ETSI TS 123 280 V18.13.0 (2025-09)

TECHNICAL SPECIFICATION

LTE;
Common functional architecture to support mission critical services;
Stage 2
(3GPP TS 23.280 version 18.13.0 Release 18)

Reference
RTS/TSGS-0623280vid0

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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

© ETSI 2025.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

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

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

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

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 16
1 Scope 17
2 References 17
3 Definitions, symbols and abbreviations 18
3.1 Definitions 18
3.2 Symbols 21
3.3 Abbreviations 21
4 Introduction 22
5 Assumptions and architectural requirements 23
5.1 Assumptions 23
5.1.1 Service continuity 23
5.1.2 Trust domain 23
5.2 Architectural requirements 23
5.2.1 General architectural requirements 23
5.2.2 PLMN change requirements 24
5.2.3 UE-to-network relay MC service requirements 24
5.2.4 MC service user profile requirements 24
5.2.5 MC service group affiliation and MC service group de-affiliation 24
5.2.6 GCS AS requirements for the MC services 25
5.2.7 Bearer management 26
5.2.7.0 General 26
5.2.7.1 MBMS bearer management 26
5.2.7.2 EPS bearer considerations 27
5.2.8 External applications access to services in a MC system 27
5.2.9 Migration 27
5.2.9.1 General 27
5.2.9.2 PLMN utilisation 28
5.2.9.3 SIP core / IMS utilisation 28
5.2.10 Interconnection 29
5.2.10.1 General 29
5.2.10.2 Connectivity 29
5.2.10.3 Migration 29
5.2.10.4 Private calls 29
5.2.10.5 Group calls 29
5.2.10.6 Group configuration 30
5.2.10.7 MC system topology hiding 30
5.2.11 Use of priorities 30
5.2.11.1 Requested priority 30
6 Involved business relationships 30
7 Functional model 33
7.1 General 33
7.2 Description of the planes 33
7.3 Functional model description 33
7.3.1 On-network functional model 33
7.3.2 Off-network functional model 37
7.4 Functional entities description 37
7.4.1 General 37
7.4.2 Application plane 37
7.4.2.1 General 37

7.4.2.2 Common services core 38
7.4.2.2.1 Configuration management client 38
7.4.2.2.2 Configuration management server (CMS) 38
7.4.2.2.3 Group management client 38
7.4.2.2.4 Group management server (GMS) 38
7.4.2.2.5 Identity management client 38
7.4.2.2.6 Identity management server (IdMS) 38
7.4.2.2.7 Key management client 39
7.4.2.2.8 Key management server (KMS) 39
7.4.2.2.9 Location management client 39
7.4.2.2.10 Location management server (LMS) 39
7.4.2.2.11 Void 39
7.4.2.2.12 Functional alias management client 39
7.4.2.2.13 Functional alias management server 39
7.4.2.3 MC service 39
7.4.2.3.1 MC service client 39
7.4.2.3.2 MC service server 39
7.4.2.3.3 MC service user database 40
7.4.2.3.4 MC gateway server 40
7.4.3 Signalling control plane 40
7.4.3.1 SIP entities 40
7.4.3.1.1 Signalling user agent 40
7.4.3.1.2 SIP AS 40
7.4.3.1.3 SIP core 40
7.4.3.1.3.1 General 40
7.4.3.1.3.2 Local inbound / outbound proxy 41
7.4.3.1.3.3 Registrar finder 41
7.4.3.1.3.4 Registrar / application service selection 41
7.4.3.1.4 Diameter proxy 42
7.4.3.2 SIP database 42
7.4.3.2.1 General 42
7.4.3.2.2 SIP database logical functions 43
7.4.3.3 HTTP entities 43
7.4.3.3.1 HTTP client 43
7.4.3.3.2 HTTP proxy 43
7.4.3.3.3 HTTP server 44
7.5 Reference points 44
7.5.1 General reference point principle 44
7.5.2 Application plane 44
7.5.2.1 General 44
7.5.2.2 Reference point CSC-1 (between the identity management client and the identity management server) 44
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) 44
7.5.2.4 Reference point CSC-3 (between the MC service server and the group management server) 44
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) 45
7.5.2.6 Reference point CSC-5 (between the MC service server and the configuration management server) 45
7.5.2.7 Reference point CSC-7 (between the group management servers) 45
7.5.2.8 Reference point CSC-8 (between the key management server and the key management client) 45
7.5.2.9 Reference point CSC-9 (between the key management server and the MC service server) 45
7.5.2.10 Reference point CSC-10 (between the key management server and the group management server) 46
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) 46
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) 46
7.5.2.13 Reference point CSC-13 (between the configuration management server and the MC service user database) 46
7.5.2.14 Reference point CSC-14 (between the location management client and the location management server) 46

7.5.2.15 Reference point CSC-15 (between the location management server and the MC service server) 46
7.5.2.16 Reference point CSC-16 (between group management servers in different MC systems) 47
7.5.2.17 Reference point CSC-17 (between configuration management servers in different MC systems) 47
7.5.2.18 Void.....47
7.5.2.19 Reference point MCX-1 (between MC service servers) 47
7.5.2.20 Reference point CSC-19 (between group management server and MC gateway server).....47
7.5.2.21 Reference point CSC-20 (between configuration management server and MC gateway server) 47
7.5.2.22 Reference point CSC-21 (between MC gateway servers in different MC systems).....48
7.5.2.23 Reference point CSC-22 (between location management servers in different MC systems).....48
7.5.2.24 Reference point CSC-23 (between location management server and MC gateway server).....48
7.5.2.25 Reference point CSC-24 (between the Location management server and the configuration management server).....48
7.5.3 Signalling control plane.....48
7.5.3.1 General.....48
7.5.3.2 Reference point SIP-1(between the signalling user agent and the SIP core).....48
7.5.3.3 Reference point SIP-2 (between the SIP core and the SIP AS).....49
7.5.3.4 Reference point SIP-3 (between the SIP core and SIP core).....49
7.5.3.5 Reference point HTTP-1 (between the HTTP client and the HTTP proxy).....49
7.5.3.6 Reference point HTTP-2 (between the HTTP proxy and the HTTP server).....49
7.5.3.7 Reference point HTTP-3 (between the HTTP proxy and HTTP proxy) 49
7.5.3.8 Reference point AAA-1 (between the SIP database and the SIP core).....50
7.5.3.9 Reference point AAA-2 (between the SIP core and Diameter proxy) 50

8 Identities.....50
8.1 Application plane 50
8.1.1 Mission Critical user identity (MC ID).....50
8.1.2 MC service user identity (MC service ID).....50
8.1.3 MC service group identity (MC service group ID).....51
8.1.3.1 General.....51
8.1.3.2 MC service group ID management (off-network operation).....51
8.1.4 MC system identity (MC system ID).....52
8.1.5 Functional Alias.....52
8.1.6 MC service UE label.....52
8.1.7 Void 53
8.2 SIP signalling control plane.....53
8.3 Relationship between identities in different planes 53
8.3.1 Relationship between MC service ID and public user identity 53
8.3.2 Relationship between MC service group ID and public service identity 54

9 Application of functional model to deployments 54
9.1 General 54
9.2 Architecture model and deployment scenarios for on-network operations 54
9.2.1 On-network architectural model 54
9.2.1.1 On-network architectural model diagram.....54
9.2.1.2 Application services layer 55
9.2.1.2.1 Overview 55
9.2.1.2.2 Common services core 55
9.2.1.2.3 MC services.....55
9.2.1.3 SIP core.....56
9.2.1.4 EPS.....56
9.2.1.5 UE 1 56
9.2.1.6 UE 2 56
9.2.2 Deployment scenarios.....56
9.2.2.1 Administration of MC service, SIP core and EPS.....56
9.2.2.1.1 General 56
9.2.2.1.2 Common administration of all planes.....56
9.2.2.1.3 MC service provider separate from SIP core and EPS 57
9.2.2.1.4 MC service provider administers SIP core, separate from EPS.....58
9.2.2.1.5 SIP core partially administered by both PLMN operator and MC service provider.....58
9.2.2.1.6 PLMN operator administers SIP core with SIP identities administered by MC service provider 59
9.2.2.2 MC service user database, SIP database and HSS 60

9.2.2.3 Control of bearers by SIP core and MC service server 63
9.2.2.3.1 General 63
9.2.2.3.2 Control of bearers by SIP core 63
9.2.2.3.3 Control of bearers by MC service server 63
9.3 Architecture model for off-network operations 64
9.3.1 Off-network architectural model diagram 64
9.3.2 UE 3 64
9.3.3 UE 4 65
9.3.4 Offline common services server 65
9.4 Architecture model for roaming 65

10 Procedures and information flows 65
10.1 MC service configuration 65
10.1.1 General 65
10.1.1.1 MC service configuration on primary MC system 65
10.1.1.2 MC service configuration for migration to partner MC system 66
10.1.2 Information flows for MC service configuration 68
10.1.2.1 Store group configuration request 68
10.1.2.2 Store group configuration response 68
10.1.2.3 Get group configuration request 68
10.1.2.4 Get group configuration response 69
10.1.2.5 Subscribe group configuration request 69
10.1.2.5a Subscribe group policy request 69
10.1.2.6 Subscribe group configuration response 69
10.1.2.6a Subscribe group policy response 69
10.1.2.7 Notify group configuration request 70
10.1.2.7a Notify group policy request 70
10.1.2.8 Notify group configuration response 70
10.1.2.8a Notify group policy response 70
10.1.2.9 Get functional alias configuration request 71
10.1.2.10 Get functional alias configuration response 71
10.1.2.11 Subscribe functional alias configuration request 71
10.1.2.12 Subscribe functional alias configuration response 71
10.1.2.13 Notify functional alias configuration request 71
10.1.2.14 Notify functional alias configuration response 72
10.1.2.15 Void 72
10.1.2.16 Void 72
10.1.2.17 Void 72
10.1.2.18 Void 72
10.1.2.19 Void 72
10.1.2.20 Void 72
10.1.2.21 Void 72
10.1.2.22 Void 72
10.1.2.23 Void 72
10.1.2.24 Void 72
10.1.2.25 Void 72
10.1.3 MC service UE configuration data 72
10.1.3.1 General 72
10.1.3.2 Procedures 72
10.1.3.3 Structure of UE configuration data 73
10.1.4 MC service user profile 73
10.1.4.1 General 73
10.1.4.2 Information flows for MC service user profile 74
10.1.4.2.1 Get MC service user profile request 74
10.1.4.2.2 Get MC service user profile response 75
10.1.4.2.3 Notification for MC service user profile data update 75
10.1.4.2.4 Get updated MC service user profile data request 75
10.1.4.2.5 Get updated MC service user profile data response 75
10.1.4.2.6 Update MC service user profile data request 75
10.1.4.2.7 Update MC service user profile data response 76
10.1.4.2.8 Update pre-selected MC service user profile request 76
10.1.4.2.9 Update pre-selected MC service user profile response 76

10.1.4.2.10 Update selected MC service user profile request 76
10.1.4.2.11 Update selected MC service user profile response 77
10.1.4.3 MC service user obtains the MC service user profile(s) from the network 77
10.1.4.3.1 MC service user receiving MC service in primary MC system 77
10.1.4.3.2 MC service user receiving MC service from a partner MC system 78
10.1.4.4 MC service user receives updated MC service user profile data from the network 79
10.1.4.5 MC service user updates MC service user profile data to the network 80
10.1.4.6 Updating the pre-selected MC service user profile 81
10.1.4.7 Updating the selected MC service user profile for an MC service 82
10.1.5 MC service group configuration management 83
10.1.5.1 Store group configurations at the group management server 83
10.1.5.2 Retrieve group configurations at the group management client 84
10.1.5.3 Subscription and notification for group configuration data at group management client 84
10.1.5.3a Subscription and notification for group policy at MC service server 85
10.1.5.4 Structure of group configuration data 86
10.1.5.5 Dynamic data associated with a group 86
10.1.5.5.1 Dynamic data associated with a group in MC service server 86
10.1.5.5.2 Dynamic data associated with a group in group management server 87
10.1.5.6 Subscription and notification for dynamic data associated with a group 88
10.1.5.6.0 General 88
10.1.5.6.1 Information flows for subscription and notification for dynamic data associated with a group 88
10.1.5.6.1.1 Subscribe group dynamic data request 88
10.1.5.6.1.2 Subscribe group dynamic data response 88
10.1.5.6.1.3 Notify group dynamic data request 89
10.1.5.6.1.4 Notify group dynamic data response 89
10.1.5.6.2 Procedure for subscription and notification for dynamic data associated with a group by the MC service client 89
10.1.5.6.3 Procedure for subscription and notification for dynamic data associated with a group by the group management server 90
10.1.6 MC service UE migration 91
10.1.6.1 MC service UE obtains migration connectivity information of partner MC system 91
10.1.6.2 Void 91
10.1.7 Functional alias configuration management 91
10.1.7.1 Retrieve functional alias configurations from the functional alias management server 91
10.1.7.2 Subscription and notification for functional alias configuration data 92
10.1.7.3 Dynamic data associated with a functional alias 93
10.1.7.3.1 Dynamic data associated with a functional alias in MC service server 93
10.2 Group management (on-network) 93
10.2.1 General 93
10.2.2 Information flows for group management 94
10.2.2.1 Group creation request 94
10.2.2.2 Group creation response 94
10.2.2.3 Group regroup request (group management client – group management server) 94
10.2.2.4 Group regroup response (group management server – group management client) 95
10.2.2.5 Group regroup teardown request 95
10.2.2.6 Group regroup teardown response 95
10.2.2.7 Group creation notify 95
10.2.2.8 Group regroup notify 96
10.2.2.9 Group regroup teardown notify 96
10.2.2.10 Group regroup teardown notification 96
10.2.2.11 Group regroup teardown notification response 96
10.2.2.12 Group regroup request (group management server – group management server) 97
10.2.2.13 Group regroup response (group management server – group management server) 97
10.2.2.14 Group regroup notification 97
10.2.2.15 Group regroup notification response 97
10.2.2.16 Group information query request 98
10.2.2.17 Group information query response 98
10.2.2.18 Group membership update request 98
10.2.2.19 Group membership update response 98
10.2.2.20 Group membership notification 99
10.2.2.21 Group deletion request 99
10.2.2.22 Group deletion response 99

10.2.2.23 Group deletion notification 99
10.2.2.24 Group information provision request 100
10.2.2.25 Group information provision response 100
10.2.2.26 Group information request 100
10.2.2.27 Group information response 100
10.2.2.28 Group information subscribe request 101
10.2.2.29 Group information subscribe response 101
10.2.2.30 Group information notify request 101
10.2.2.31 Group information notify response 101
10.2.3 Group creation 102
10.2.4 Group regrouping 103
10.2.4.1 Temporary group formation - group regrouping within an MC system 103
10.2.4.2 Temporary group formation involving multiple MC systems 105
10.2.4.2a Temporary group tear down within an MC system 107
10.2.4.3 Temporary group tear down involving multiple group host servers 108
10.2.4.4 Group regroup rules 109
10.2.5 Membership and affiliation list query 110
10.2.5.1 General 110
10.2.5.2 Procedure 110
10.2.6 Group membership 110
10.2.6.1 Group membership notification 110
10.2.6.2 Group membership update by authorized user 111
10.2.7 Group configuration for interconnection 112
10.2.7.1 Overview 112
10.2.7.2 Primary MC system provides group configuration to the partner MC system 113
10.2.7.3 Partner MC system requests group configuration from the primary MC system 114
10.2.7.4 Partner MC system subscribes to group configuration 115
10.2.7.5 Primary MC system notifies group configuration 116
10.2.8 Group deletion 117
10.3 Pre-established session (on-network) 118
10.3.1 General 118
10.3.2 Procedures 118
10.3.2.1 General 118
10.3.2.2 Pre-established session establishment 118
10.3.2.3 Pre-established session modification 119
10.3.2.4 Pre-established session release 121
10.4 Simultaneous session (on-network) 122
10.4.1 General 122
10.5 Use of UE-to-network relay 122
10.5.1 UE-to-network relay service authorization 122
10.5.2 UE-to-network relay MC service 122
10.6 General user authentication and authorization for MC services 122
10.6.1 Primary MC system 122
10.6.2 Interconnection partner MC system 123
10.6.3 Migration to partner MC system 123
10.6.3.1 General 123
10.6.3.2 Information flows 124
10.6.3.2.1 Migration service authorization request 124
10.6.3.2.2 Migration service authorization response 124
10.6.3.2.3 Migration service de-authorization notification 124
10.6.3.2.4 MC service authorization notification 125
10.6.3.3 Procedures 125
10.6.3.3.1 Migration service authorization procedure 125
10.6.3.3.2 Migration service de-authorization procedure initiated by MC service server 127
10.6.3.3.2.1 Migrated MC service user returns back to its primary MC system 127
10.6.3.3.2.2 Migrated MC service user migrate to another partner MC system 128
10.7 Use of MBMS transmission 129
10.7.1 General 129
10.7.2 Information flows for MBMS transmission 129
10.7.2.1 MBMS bearer announcement 129
10.7.2.2 MBMS listening status report 130
10.7.2.3 MBMS suspension reporting instruction 130

10.7.2.4 Discover bearer request 131
10.7.2.5 Discover bearer response 131
10.7.2.6 Media distribution request 131
10.7.2.7 Media distribution response 132
10.7.2.8 Identify multicast participants request 132
10.7.2.9 Remove call from bearer request 132
10.7.2.10 Media distribution release 132
10.7.2.11 Media broadcasting notification 132
10.7.2.12 Group status notification 132
10.7.2.13 MBMS suspension report 133
10.7.3 Procedures for MBMS usage 133
10.7.3.1 Use of pre-established MBMS bearers 133
10.7.3.1.1 General 133
10.7.3.1.2 Procedure 133
10.7.3.2 Use of dynamic MBMS bearer establishment 135
10.7.3.3 Switching from MBMS bearer to unicast bearer 136
10.7.3.4 Use of MBMS bearer for application level control signalling 137
10.7.3.4.1 Description 137
10.7.3.4.2 Procedure 137
10.7.3.5 MBMS bearer announcement over MBMS bearer 138
10.7.3.5.1 Description 138
10.7.3.5.2 Procedure 138
10.7.3.6 MBMS bearer quality detection 140
10.7.3.6.1 Description 140
10.7.3.6.2 Procedure 140
10.7.3.7 Service continuity in MBMS scenarios 141
10.7.3.7.1 General 141
10.7.3.7.2 Service continuity when moving from one MBSFN to another 141
10.7.3.7.3 Service continuity with a UE-to-Network relay 144
10.7.3.8 MBMS suspension notification 146
10.7.3.8.1 Description 146
10.7.3.8.2 Procedure 146
10.7.3.9 Multi-server bearer coordination 147
10.7.3.9.1 General 147
10.7.3.9.2 Procedures 147
10.7.3.9.2.1 MBMS bearer coordination independent on broadcasted media 147
10.7.3.9.2.2 MBMS bearer coordination within one group call 149
10.7.3.10 MBMS bearer event notification 151
10.7.3.10.1 General 151
10.7.3.10.2 Procedure 152
10.7.3.11 Use of FEC to protect MBMS transmissions 152
10.7.3.11.1 General 152
10.7.3.11.2 FEC encoding by the BM-SC 153
10.7.3.11.3 FEC encoding by the MC service server 154
10.7.3.12 Header compression over MBMS with ROHC 155
10.7.3.12.1 General 155
10.7.3.12.2 Header compression by the MC service server 155
10.7.3.12.3 Header compression by the BM-SC 155
10.7.3.13 Use of MBMS bearer for group status 157
10.8 Affiliation and de-affiliation to/from MC service group(s) 158
10.8.1 General 158
10.8.2 Information flows 158
10.8.2.1 MC service group affiliation request 158
10.8.2.2 MC service group affiliation request (MC service server – MC service server) 158
10.8.2.3 MC service group affiliation response 158
10.8.2.4 MC service group affiliation response (MC service server – MC service server) 159
10.8.2.5 Void 159
10.8.2.6 MC service group de-affiliation request 159
10.8.2.7 MC service group de-affiliation request (MC service server – MC service server) 159
10.8.2.8 MC service group de-affiliation response 159
10.8.2.9 MC service group de-affiliation response (MC service server – MC service server) 160
10.8.2.10 Void 160

10.8.2.11 MC service group affiliation change request....160
10.8.2.12 MC service group affiliation change response....160
10.8.2.13 MC service group de-affiliation notification....161
10.8.2.14 Notify group dynamic data request....161
10.8.3 Affiliation....161
10.8.3.1 MC service group affiliation procedure....161
10.8.3.2 Affiliation to MC service group(s) defined in partner MC system without topology hiding....162
10.8.3.2.1 Functional description....162
10.8.3.2.2 Procedure....163
10.8.3.2a Affiliation to MC service group(s) defined in partner MC system using topology hiding....164
10.8.3.2a.1 Functional description....164
10.8.3.2a.2 Procedure....164
10.8.4 De-affiliation from MC service group(s)....166
10.8.4.1 General....166
10.8.4.2 MC service group de-affiliation procedure....166
10.8.4.3 De-affiliation from MC service group(s) defined in partner MC system....167
10.8.4.4 MC server initiated group de-affiliation procedure....169
10.8.4.5 MC server initiated group de-affiliation from group defined in partner MC system....169
10.8.5 Remote change of affiliation....171
10.8.5.1 Remote change of affiliation for groups defined in primary MC system....171
10.8.5.1.1 Authorized user remotely changes another MC service user's affiliated MC service group(s) – mandatory mode....171
10.8.5.1.2 Authorized user remotely changes another MC service user's affiliated MC service group(s) – negotiated mode....172
10.8.5.2 Remote change of affiliation for groups defined in partner MC system....174
10.8.5.2.1 Authorized user remotely changes another MC service user's affiliated MC service group(s) defined in partner MC system – mandatory mode....174
10.9 Location management (on-network)....176
10.9.1 General....176
10.9.2 Information flows for location information....176
10.9.2.1 Location reporting configuration....176
10.9.2.2 Location information report....177
10.9.2.3 Location information request....178
10.9.2.4 Location reporting trigger....179
10.9.2.5 Location information subscription request....180
10.9.2.6 Location information subscription response....181
10.9.2.7 Location information notification....181
10.9.2.10 Location report response....184
10.9.2.11 Location information history status request....184
10.9.2.12 Location information history status report....185
10.9.2.13 Location information history request....186
10.9.2.14 Location information history report....188
10.9.2.15 Location information history cancel request....189
10.9.2.16 Location information history cancel response....190
10.9.2.17 Location reporting temporary configuration request....190
10.9.2.18 Location reporting temporary configuration response....191
10.9.2.19 Restrict location information dissemination request....191
10.9.2.20 Restrict location information dissemination response....192
10.9.2.21 Restrict location information dissemination notification....192
10.9.3 Procedure....193
10.9.3.1 Event-triggered location reporting procedure....193
10.9.3.2 On-demand location reporting procedure....194
10.9.3.3 Client-triggered location reporting procedure....195
10.9.3.4 Location reporting cancel procedure....196
10.9.3.5 Location information subscription procedure....197
10.9.3.6 Usage of location information procedure....197
10.9.3.6.1 Event-trigger location information notification procedure....197
10.9.3.6.2 On-demand usage of location information procedure....198
10.9.3.8 Location management using functional alias....200
10.9.3.8.1 Client-triggered one-time location information report....200
10.9.3.8.2 Client-triggered periodic location information report....201
10.9.3.9 Usage of location history reporting procedure....202

10.9.3.9.1 General 202
10.9.3.9.2 Report location history procedure 202
10.9.3.9.2.1 On-demand report location history procedure (LMC – LMS) 202
10.9.3.9.2.2 On-demand report location history procedure 203
10.9.3.9.3 Usage of status location history reporting procedure 204
10.9.3.9.3.1 Status location history reporting procedure (LMC – LMS) 204
10.9.3.9.3.2 On-demand status location history reporting procedure (LMS – LMC) 205
10.9.3.9.3.3 On-demand status location history reporting procedure 205
10.9.3.9.4 Usage of cancel location history reporting procedure 206
10.9.3.9.4.1 General 206
10.9.3.9.4.2 Cancel location history reporting procedure (LMS – LMC) 206
10.9.3.9.4.3 Cancel location history reporting procedure 207
10.9.3.10 Usage of location information across MC systems procedure 208
10.9.3.10.1 General 208
10.9.3.10.2 On-demand request of location information procedure 208
10.9.3.10.3 Event-triggered location information notification procedure 209
10.9.3.10.4 Location information subscription procedure 210
10.9.3.10.5 Location information cancel subscription procedure 212
10.9.3.10.6 Location reporting temporary configuration procedure 213
10.9.3.11 Restrict location information dissemination procedure 215
10.10 Emergency Alert 216
10.10.1 On-network emergency alert 216
10.10.1.1 General 216
10.10.1.1A Information flows 216
10.10.1.1A.1 MC service emergency alert request 216
10.10.1.1A.2 MC service emergency alert response 217
10.10.1.1A.3 MC service emergency alert cancel request 217
10.10.1.1A.4 MC service emergency alert cancel response 217
10.10.1.1A.5 MC service emergency alert area notification 218
10.10.1.2 MC service emergency alert 218
10.10.1.2.1 MC service emergency alert initiation 218
10.10.1.2.1.1 General 218
10.10.1.2.1.3 MC service individual emergency alert initiation 220
10.10.1.2.2 MC service emergency alert cancel 222
10.10.1.2.2.1 General 222
10.10.1.2.2.2 MC service group emergency alert cancel 222
10.10.1.2.2.3 MC service individual emergency alert cancel 223
10.10.1.2.3 Entering MC service emergency alert area 224
10.10.1.2.4 Leaving MC service emergency alert area 225
10.10.2 Off-network emergency alert 226
10.10.2.1 General 226
10.10.2.1A Information flows 227
10.10.2.1A.1 MC service emergency alert announcement 227
10.10.2.1A.2 MC service emergency alert cancel announcement 227
10.10.2.2 MC service emergency alert 227
10.10.2.2.1 Emergency alert initiation 227
10.10.2.2.2 Emergency alert cancel 228
10.10.3 Ad hoc group emergency alert 230
10.10.3.1 General 230
10.10.3.2 Information flows 230
10.10.3.2.1 Ad hoc group emergency alert request (MC service client – MC service server) 230
10.10.3.2.2 Ad hoc group emergency alert request (MC service server – MC service client) 230
10.10.3.2.2a Ad hoc group emergency alert request return 231
10.10.3.2.3 Ad hoc group emergency alert response 231
10.10.3.2.4 Ad hoc group emergency alert cancel request 231
10.10.3.2.4a Ad hoc group emergency alert cancel request return 232
10.10.3.2.5 Ad hoc group emergency alert cancel response 232
10.10.3.2.6 Ad hoc group emergency alert participants list notification 232
10.10.3.2.7 Ad hoc group emergency alert get userlist request 233
10.10.3.2.8 Ad hoc group emergency alert get userlist response 233
10.10.3.2.9 Ad hoc group emergency alert user add notification 234
10.10.3.2.10 Ad hoc group emergency alert user remove notification 234

10.10.3.2.11 Ad hoc group emergency alert notify 234
10.10.3.3 Procedures within single MC system 235
10.10.3.3.1 Ad hoc group emergency alert initiation 235
10.10.3.3.2 Ad hoc group emergency alert cancel 236
10.10.3.3.3 Entering an ongoing ad hoc group emergency alert 238
10.10.3.3.4 Leaving an ad hoc group emergency alert 239
10.10.3.4 Procedures within multiple MC systems 240
10.10.3.4.1 Ad hoc group emergency alert initiation 240
10.10.3.4.2 Updating the participant list of an ongoing ad hoc group emergency alert 241
10.10.3.4.3 Ad hoc group emergency alert cancel 243
10.11 MC service resource management (on-network) 244
10.11.1 General 244
10.11.2 Request for unicast resources at session establishment 244
10.11.2a Request for unicast resources at session establishment from MC service server 245
10.11.2a.1 General 245
10.11.2a.2 Procedure 246
10.11.3 Request for modification of unicast resources 246
10.11.4 Management of multicast media bearers 248
10.11.5 Request for resources with shared priority 248
10.11.5.1 General 248
10.11.5.2 Procedure 248
10.11.6 Request for media resources from MC service server 249
10.11.6.1 General 249
10.11.6.2 Procedure 249
10.12 Priority Management 250
10.12.1 General 250
10.12.2 Information flows 251
10.12.2.1 MC priority request 251
10.12.3 Procedure for priority coordination between multiple MC service servers 251
10.13 Functional alias management (on-network) 253
10.13.1 General 253
10.13.2 Information flows for functional alias management 253
10.13.2.1 Active functional alias information user query request 253
10.13.2.1a Active functional alias information usage query request 253
10.13.2.2 Active functional alias information user query response 253
10.13.2.2a Active functional alias information usage query response 254
10.13.2.3 Functional alias activation request 254
10.13.2.4 Functional alias activation response 254
10.13.2.5 Functional alias de-activation request 255
10.13.2.6 Functional alias de-activation response 255
10.13.2.7 Functional alias status notification 255
10.13.2.8 Functional alias take over request 255
10.13.2.9 Functional alias take over response 256
10.13.2.10 Functional alias revoke notification 256
10.13.2.11 Subscribe functional alias request 256
10.13.2.12 Subscribe functional alias response 256
10.13.2.13 Notify functional alias request 257
10.13.2.14 Notify functional alias response 257
10.13.2.15 Unsubscribe functional alias request 257
10.13.2.16 Unsubscribe functional alias response 257
10.13.2.17 Functional alias to group binding request 257
10.13.2.18 Functional alias to group binding response 258
10.13.2.19 Functional alias to group unbinding request 258
10.13.2.20 Functional alias to group unbinding response 258
10.13.3 Authorised MC service user retrieves active functional alias(es) for certain MC service user(s) 258
10.13.4 MC service user activates functional alias(es) within an MC system 259
10.13.5 MC service user de-activates functional alias(es) within an MC system 260
10.13.6 Authorised MC service user takes over functional alias(es) within an MC system 261
10.13.7 Authorised MC service user retrieves MC service user(s) for certain active functional alias(es) 262
10.13.10 Subscription and notification for functional alias 265
10.13.10.1 General 265
10.13.11 Functional alias to group binding 267

10.13.11.1 General 267
10.13.11.2 Functional alias to group binding 267
10.13.11.3 Functional alias to group unbinding 267
10.14 Generic procedures for interconnection 268
10.14.1 General 268
10.14.2 Generic call procedure with topology hiding 268
10.14.2.1 General 268
10.14.2.2 Procedure for calls with topology hiding 268
10.14.3 Generic call procedure for enforcement of local MC service group configuration 270
10.14.3.1 General 270
10.14.3.2 MC service group call initiated in the partner MC system of the MC service group 270
10.14.3.3 MC service group call request received from the primary MC system of the MC service group 271
10.14.4 Generic call procedure for media replication in participating MC system in MC service group calls 272
10.14.4.1 General 272
10.14.4.2 Media replication in the partner MC system of the MC service group 272
10.15 Preconfigured regrouping 273
10.15.1 General 273
10.15.2 Information flows for preconfigured regrouping 274
10.15.2.1 Preconfigured regroup request (MC service client – MC service server) 274
10.15.2.2 Preconfigured regroup request (MC service server – MC service client) 274
10.15.2.3 Preconfigured regroup request (MC service server – MC service server) 275
10.15.2.4 Preconfigured regroup response (MC service client – MC service server) 275
10.15.2.5 Preconfigured regroup response (MC service server – MC service client) 275
10.15.2.6 Preconfigured regroup response (MC service server – MC service server) 275
10.15.2.7 Preconfigured regroup cancel request (MC service client – MC service server) 276
10.15.2.8 Preconfigured regroup cancel request (MC service server – MC service client) 276
10.15.2.9 Preconfigured regroup cancel request (MC service server – MC service server) 276
10.15.2.10 Preconfigured regroup cancel response (MC service client – MC service server) 276
10.15.2.11 Preconfigured regroup cancel response (MC service server – MC service client) 277
10.15.2.12 Preconfigured regroup cancel response (MC service server – MC service server) 277
10.15.2.13 Preconfigured regroup reject (MC service server – MC service client) 277
10.15.2.14 Preconfigured regroup reject (MC service server – MC service server) 278
10.15.2.15 Preconfigured user regroup remove request (MC service server – MC service client) 278
10.15.2.16 Preconfigured user regroup remove response (MC service client – MC service server) 278
10.15.3 Regroup with preconfigured group 278
10.15.3.1 General 278
10.15.3.2 Preconfigured regroup procedures in a single MC system 279
10.15.3.2.1 Preconfigured Group Regroup formation in a single MC system 279
10.15.3.2.2 Preconfigured User Regroup formation in a single MC system 281
10.15.3.2.3 Preconfigured regroup cancellation in a single MC system 283
10.15.3.3 Preconfigured regroup procedures in multiple MC systems 284
10.15.3.3.1 Preconfigured Group Regroup formation in multiple MC systems 284
10.15.3.3.2 Preconfigured User Regroup formation in multiple MC systems 286
10.15.3.3.3 Preconfigured regroup cancellation in multiple MC systems 288
10.15.3.3.4 Preconfigured group regroup rejection in multiple MC systems 289
10.15.3.4 Other preconfigured regroup procedures 290
10.15.3.4.1 Adding newly affiliated user to preconfigured group regroup 290
10.15.3.4.2 Updating the MC service ID list in a preconfigured regroup group based on user regroup 291
10.16 Generic procedures for migration 293
10.16.1 General 293
10.16.2 Migration during an ongoing group communication 293
10.16.2.1 General 293
10.16.2.2 Procedure 293
10.16.2.3 Void 294
10.16.2.3.1 Void 294
10.16.3 Private call using functional alias towards a partner MC system 294
10.16.3.1 General 294
10.16.3.2 Information flows 294
10.16.3.2.1 MC service functional alias resolution request 294
10.16.3.2.2 MC service functional alias resolution response 295
10.16.3.3 Procedure 295
10.16.4 Migration during an onging private communication 297

10.16.4.1 General 297
10.16.4.2 Procedure 297
10.16.5 Generic private call procedure towards a migrated MC service user 299
10.16.5.1 General 299
10.16.5.2 Private call redirection 299
10.16.5.3 Procedure 299

11 MC gateway UE 301
11.1 General 301
11.2 Functional Model 301
11.2.0 General 301
11.2.1 Functional model 303
11.2.2.1 General 305
11.2.2.2 Void 305
11.2.2.3 Void 305
11.2.2.4 Reference points MCX-n, CSC-n, SIP-1 and HTTP-1 305
11.2.3 Void 305
11.3 Using identities behind the MC gateway UE 305
11.3.1 General 305
11.3.2 When using separate IMS subscriptions 305
11.3.3 When sharing MC gateway UE's IMS subscription 305
11.4 Void 306
11.5 Procedures and information flows 306
11.5.1 Void 306
11.5.2 Void 306
11.5.3 Void 306
11.5.4 Void 306

Annex A (normative): Configuration data for MC services 307
A.1 General 307
A.2 MC service UE configuration data 308
A.3 MC service user profile configuration data 308
A.4 Group configuration data 308
A.5 MC service configuration data 313
A.6 Initial MC service UE configuration data 313
A.7 Void 315
A.8 Location user profile configuration data 315

Annex B (informative): Service continuity for MC service 317
B.1 Service continuity between on-network MC service and UE-to-network relay MC service 317

Annex C (informative): Application Priority 320
C.1 Use of application priorities 320

Annex D (informative): Considerations for MC gateway UE selection 322
D.1 General 322
D.2 Potential operating conditions 322

Annex E (informative): MC gateway UE routing capabilities 323
E.1 General 323
E.2 MC client IP address association 323
E.3 IP address association using the MC gateway UE 323

Annex F (informative): Change history 325
History 333

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); Stage 1".

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

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

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

[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] Void

[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".

[26] IETF RFC 6733 (October 2012): "Diameter Base Protocol".

[27] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[28] 3GPP TS 22.011: "Service accessibility".

[29] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".

[30] 3GPP TS 25.305: "Stage 2 functional specification of User Equipment (UE) positioning in UTRAN".

[31] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[32] IETF RFC 2865 (June 2000): "Remote Authentication Dial In User Service (RADIUS)".

[33] IETF RFC 3162 (August 2001): "RADIUS and IPv6".

[34] 3GPP TS 25.501: "System architecture for the 5G System (5GS)".

[35] IETF RFC 1541 (October 1993): "Dynamic host configuration protocol".

[36] IETF RFC 8415 (November 2018): "Dynamic host configuration protocol for IPv6 (DHCPv6)".

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]. Not all definitions are used in this document.

Accuracy: Reflects the uncertainty of the location at the moment of location measurement, e.g. see 3GPP TS 25.305 [30] and 3GPP TS 23.032 [31].

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.

Ad hoc Group Communication: The combining of a multiplicity of MC service users into a group for the duration of a communication. When the communication is released, the group no longer exists. If the communication is associated with an alert, then the group continues to exist until the alert is also cancelled.

Ad hoc Group emergency alert: The combining of a multiplicity of MC service users into a group for sending an emergency alert. When the alert is cancelled, the group no longer exists. If the alert is associated with a communication, then the group continues to exist until the communication is also cancelled.

Altitude: Third dimension for the geographical coordinates at the moment of location measurement, e.g. see 3GPP TS 25.305 [30] and 3GPP TS 23.032 [31].

Bearing: Direction at the moment of location measurement, e.g. see 3GPP TS 25.305 [30].

Chat group: An MC service group that is pre-defined with MC service group ID and member list in the group management server. Group members must join the pre-established group call to participate.

ECGI: E-UTRAN Cell Global Identifier, which is used to identify cells globally, where the ECGI is constructed from the Mobile Country Code (MCC), Mobile Network Code (MNC) and the E-UTRAN Cell Identifier (ECI).

Interconnection: A means of communication between MC systems whereby MC service users obtaining MC service from one MC system can communicate with MC service users who are obtaining MC service from one or more other MC systems.

Interconnection group: An MC service group that is configured to allow inclusion of MC service group members who are MC service users from partner MC system(s).

LCS network: The 3GPP network that provides location service as defined in 3GPP TS 23.271 [29].

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

MBMS SAI: Multimedia Broadcast Multicast Service Area Identity which is mapped to the MBMS service area.

MC gateway server: A server providing topology hiding for MC service interconnection with a partner MC system, where that partner MC system is in a different trust domain.

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 MC system where the MC service group is defined.

MC service group host MC service server: The MC service server within an MC 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 service UE label: A generic name for identification of a specific MC service UE.

MC 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.

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

Migration: A means for an MC Service user to obtain MC service directly from a partner MC system.

Partner MC system: Allied MC system that provides MC services to an MC service user based on the MC service user profiles that are defined in the primary MC system of that MC service user.

Preconfigured MC service group: an MC service group used only for regrouping that has been configured in advance of a group or user regrouping operation to serve as the source of regroup group configuration.

Pre-arranged group: An MC service group that is pre-defined with MC service group ID and member list in the group management server. Affiliated group members are invited when the group communication is setup.

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.

Primary MC system: MC system where the MC service user profiles of an MC service user are defined.

Requested Priority: A value for use in a MC service group or MC private communication that, if accepted, is used by the MCX service server to temporarily replace the priority level that is predefined in the MC service group or MC service user profile. This value is used in combination with other factors to determine the application priority for the requested communication.

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.

Serving MC service server: The MC service server which is providing MC service to an MC service client.

NOTE 1: There is one serving MC service server for each MC service, which can be the primary MC service server of the MC service user of the MC service client, or can be a partner MC service server to which the MC service user has migrated.

Serving MC system: The MC system which is providing MC service to an MC user.

NOTE 2: The MC system can be the primary MC system of the MC service user, or can be a partner MC system to which the MC service user has migrated.

Speed: Movement at the moment of location measurement, e.g. see 3GPP TS 25.305 [30] and 3GPP TS 23.032 [31].

Time of measurement: Date and time expressed with a certain precision to reflect the moment of the location measurement.

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
Functional alias

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

Multi-talker control
Group-broadcast group

For the purposes of the present document, the following terms related to a MC gateway UE function apply

MC gateway UE: A UE with functionality that enables access to the MC service for non-3GPP devices.

MC client: Aggregates a set of clients (i.e. Group management client, Configuration management client, Identity management client, Key management client, Location management client and MC service client).

MC server: Aggregates a set of servers (i.e. Group management server, Configuration management server, Identity management server, Key management server, Location management server and MC service server) which serves the MC client accordingly.

Non-3GPP device: A device that enables connectivity towards an MC gateway UE using an access method not specified by 3GPP. A subset of these devices can host an MC client specified by 3GPP.

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
CMS	Configuration Management Server
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
FEC	Forward Error Correction
GBR	Guaranteed Bit Rate
GCS AS	Group Communication Service Application Server
GCSE_LTE	Group Communication Service Enabler over LTE
GMS	Group Management Server
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
IdMS	Identity Management Server
IM CN	IP Multimedia Core Network
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia PUblic identity
IMS	IP Multimedia Subsystem
KMS	Key Management Server
LCS	Location Services
LMC	Location Management Client
LMS	Location Management Server
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
ROHC	RObust Header Compression
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. It also deals with the functional architecture of the MC gateway UE to enable access to the MC system from MC clients residing on non-3GPP devices. A subset of these devices can host an MC client specified by 3GPP.

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 PLMN change requirements

The MC applications can provide MC services to users in various PLMNs. An MC service UE may connect to PLMNs using EPC-level roaming, IMS-level roaming or local subscription.

For EPC-level roaming, in order to prioritize for network selection PLMNs that allow migration to partner MC systems, the MC service UE's User Preferred PLMN Selector list (see 3GPP TS 22.011 [28]) may be configured with a list of PLMNs that can be used to migrate to one or more partner MC systems (see subclause 5.2.9.2).

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.

NOTE 1: A combined affiliation to multiple MC services for a single MC service group is not specified in the current document.

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 2: 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. When the MC service user is logged off from the MC service, all affiliations shall be revoked in the MC service server even if no explicit de-affiliation signalling is sent.

NOTE 3: The interaction of logoff and de-affiliation when moving to off network mode of operation is out of scope of the present document.

NOTE 4: When the MC service user next performs successful service authorization, re-affiliation occurs in the MC service server without explicit affiliation signalling for all MC service groups that are configured for implicit affiliation after service authorization.

NOTE 5: The MC service client may also store MC service groups to which the MC service user was affiliated prior to that user logging off, and may re-affiliate through an explicit affiliation to these groups following the next service authorization. Such a function is outside the scope of the present document.

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:

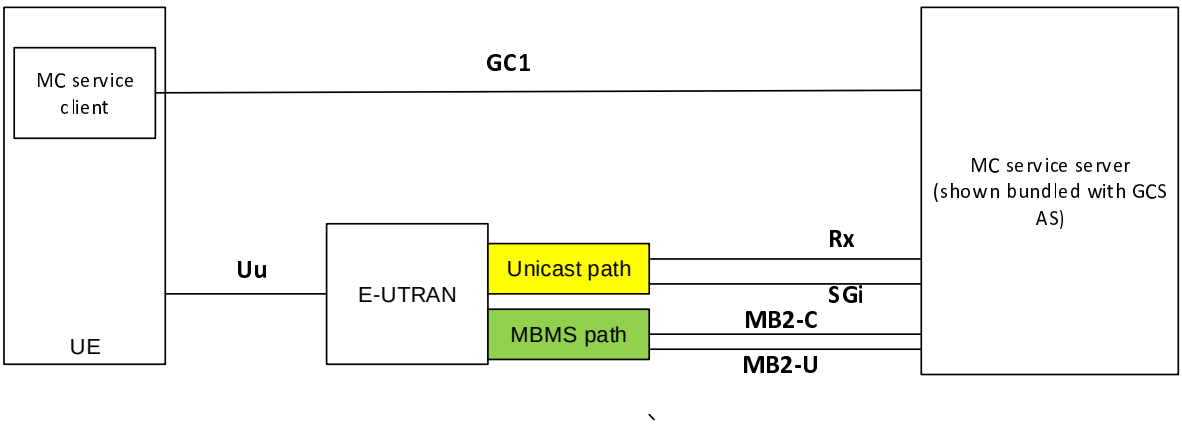

Figure 5.2.6-1: MC service on-network architecture showing MBMS

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 MC gateway UE establishes a PDN connection to the MC service APN and utilizes this connection for MC service clients host on non-3GPP devices behind it.

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. If QCI value 8 is not used for HTTP-1 transport, then caution should be used that a higher priority bearer (that is used for signalling or media) is not compromised by combining HTTP-1 traffic on this bearer.

5.2.8 External applications access to services in a MC system

The support for external applications to access MC services is out of scope of this document.

5.2.9 Migration

5.2.9.1 General

Migration provides means for the MC service user to obtain MC services from a partner MC system. As the MC service client receives one or multiple user profiles for the MC service user from its primary MC system (as described in clause 10.1.4.3). Each user profile contains a list of partner MC systems that the user is permitted to migrate to, along with necessary access information to facilitate service authentication, hence, facilitate migration to the partner MC system.

MC service interconnection needs to be provided between MC systems that wish to provide migration of their MC service users.

Migration of MC service users between any two MC systems can be on a bilateral or unilateral basis.

NOTE: Whether migration is bilateral or unilateral between any two MC systems is left to business agreements between the two MC service providers, and is outside the scope of the present document.

Migration may be triggered by the primary MC system or may be requested by the MC service client due to its geographical changes.

Upon a successful service authorization for migration, i.e., once the MC service user is authorized to migrate to a partner MC system, its primary MC system marks the user as migrated, is informed of the target partner MC system, and records the corresponding MC service ID of the migrated user provided by the partner MC system. Further details are described in clause 10.6.3.

The functional alias of a migrated MC service user at a partner MC system, which is defined in the partner MC system, can be utilized as a target address in private communication as described in clause 10.16.3.

During migration of an MC service user to a partner MC system, media of the MC service user's calls may need to be routed to the MC service user's primary MC system e.g. for logging purposes.

5.2.9.2 PLMN utilisation

Migrated MC service users should utilize the PLMN used by the partner MC system to access MC services in the partner MC system, however, utilizing the PLMN used by the primary MC system is not precluded.

NOTE 1: The above recommendation ensures the security policy of the partner MC system is not compromised, the expected QCIs are used on the RAN, and ensures service-level delay requirements are consistently met (which are especially at risk when the HPLMN of the primary MC system and HPLMN of the partner MC system are far apart from a geographical point of view).

NOTE 2: Whether the PLMN used by the partner MC systems or the PLMN used by the primary MC system is used to access MC services in partner MC systems is left to business agreements between MC service providers and is outside the scope of the present document.

MC service users enabled for migration shall be provisioned with configuration that specifies which PLMNs may be used to migrate to other MC systems.

If the PLMN used by a partner MC system is different from the PLMN used by the primary MC system (i.e. migrating MC service user starts using the PLMN used by the partner MC system), then:

- EPC-level roaming (see subclause 5.2.2) is needed between the PLMN used by the primary MC system and PLMN used by the partner MC system; and
- the PLMN used by the partner MC system needs to enable local break-out for the APNs specified in subclause 5.2.7 that identify the PDNs of the partner MC system; and
- the EPS subscriptions of the PLMN used by the primary MC system utilized by the MC service users who are allowed to migrate to the partner MC system need to be provisioned with, and local break-out enabled for, the APNs specified in subclause 5.2.7 that identify the PDNs of the partner MC system.

If the PLMN used by the partner MC system and the PLMN used by the primary MC system are the same (i.e. migrating MC service user continues to use the PLMN used by the primary MC system), then:

- the EPS subscriptions of the PLMN used by the primary MC system utilized by the MC service users who are allowed to migrate to the partner MC system need to be provisioned with the APNs specified in subclause 5.2.7 that identify the PDNs of the partner MC system.

NOTE 3: Provisioning of APNs in all of the above includes provisioning of any needed access credentials e.g. PAP, CHAP.

5.2.9.3 SIP core / IMS utilisation

Migrated MC service users should utilise the SIP core / IMS of the partner MC system.

NOTE 1: The above recommendation ensures the security policy of the partner MC system is not compromised and ensures service-level delay requirements are consistently met (which are especially at risk when the SIP core / IMS of the primary MC system and the SIP core / IMS of the partner MC system are far apart from a geographical point of view).

Where connectivity and security policies allow, the same SIP core / IMS can be utilised to connect to the primary MC system and one or more partner MC systems.

NOTE 2: Whether the same SIP core / IMS can be utilised to connect to the primary MC system and a partner MC system is left to business agreements between MC service providers, and is outside the scope of the present document.

For each partner MC system, MC service UEs of MC service users enabled for migration shall be provisioned with:

- configuration that controls whether the MC service UE shall connect to the SIP core / IMS of the primary MC system or a different SIP core / IMS (i.e. SIP core / IMS of the partner MC system); and
- where a different SIP core / IMS to the primary MC system's SIP core / IMS is to be connected to then the MC service UE shall also be configured with:
  - configuration required for the MC service UE to access the SIP core / IMS; and
  - credentials required for the MC service UE to register with the SIP core / IMS.

NOTE 3: How the MC service UE connects to the SIP core / IMS of the partner MC system to access MC services in the partner MC system is out of scope of the present document.

5.2.10 Interconnection

5.2.10.1 General

MC service interconnection allows a first set of MC service users who are receiving MC service from a first MC system to take part in communications with a second set of MC service users, where this second set of MC service users are receiving MC service from a second MC system, and where the second MC system is in a different trust domain to the first MC system.

NOTE: Assumptions for trust domains are described in subclause 5.1.2 of the present document.

5.2.10.2 Connectivity

The MC service clients of the MC service users receiving MC service(s) from a first MC system and using MC service interconnection to take part in communication with MC service users in a second MC system require connectivity to only the identity management server in the second MC system.

IP connectivity is required between MC systems wishing to interconnect. The IP connectivity is used to carry the signalling and application plane protocols needed to provide MC service.

NOTE 1: The IP connectivity between interconnecting MC systems needs to provide appropriate performance (e.g. low packet latency) in order to meet MC service user performance requirements for the MC service.

NOTE 2: If IP connectivity between interconnecting MC systems is carried outside the trust domain of both MC systems, then there will need to be appropriate security measures applied. Such security measures are outside the scope of the present document.

5.2.10.3 Migration

Interconnection may be used by a migrated MC service user who is receiving service from a partner MC system to take part in communication with MC service users in the primary MC system of that migrated MC service user.

5.2.10.4 Private calls

Where private calls take place using interconnection between MC service users who are receiving MC service in different MC systems, the MC system providing MC service to the calling MC service user will provide the controlling function for the private call.

5.2.10.5 Group calls

Where MC service users in a partner MC system of the group home MC system of an MC service group take part in group calls in that group, the group home MC system of the MC service group will provide the controlling function for the group call.

5.2.10.6 Group configuration

A partner MC system may apply local configuration to an MC service group configuration received from the primary MC system (i.e. the group home MC system).

5.2.10.7 MC system topology hiding

If an MC system requires internal network topology hiding, then this shall be achieved in the MC system by use of the following:

- proxies for signalling plane functions; and
- gateway MC service servers for application plane functions.

5.2.11 Use of priorities

5.2.11.1 Requested priority

The MC system may allow the MC service client to request the priority of a communication by selecting the corresponding priority level. The MC service server can enforce the selected priority level in determining the application priority for resource allocation during communication establishment.

The use of the requested priority may vary depending on MC service provider's policy.

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.

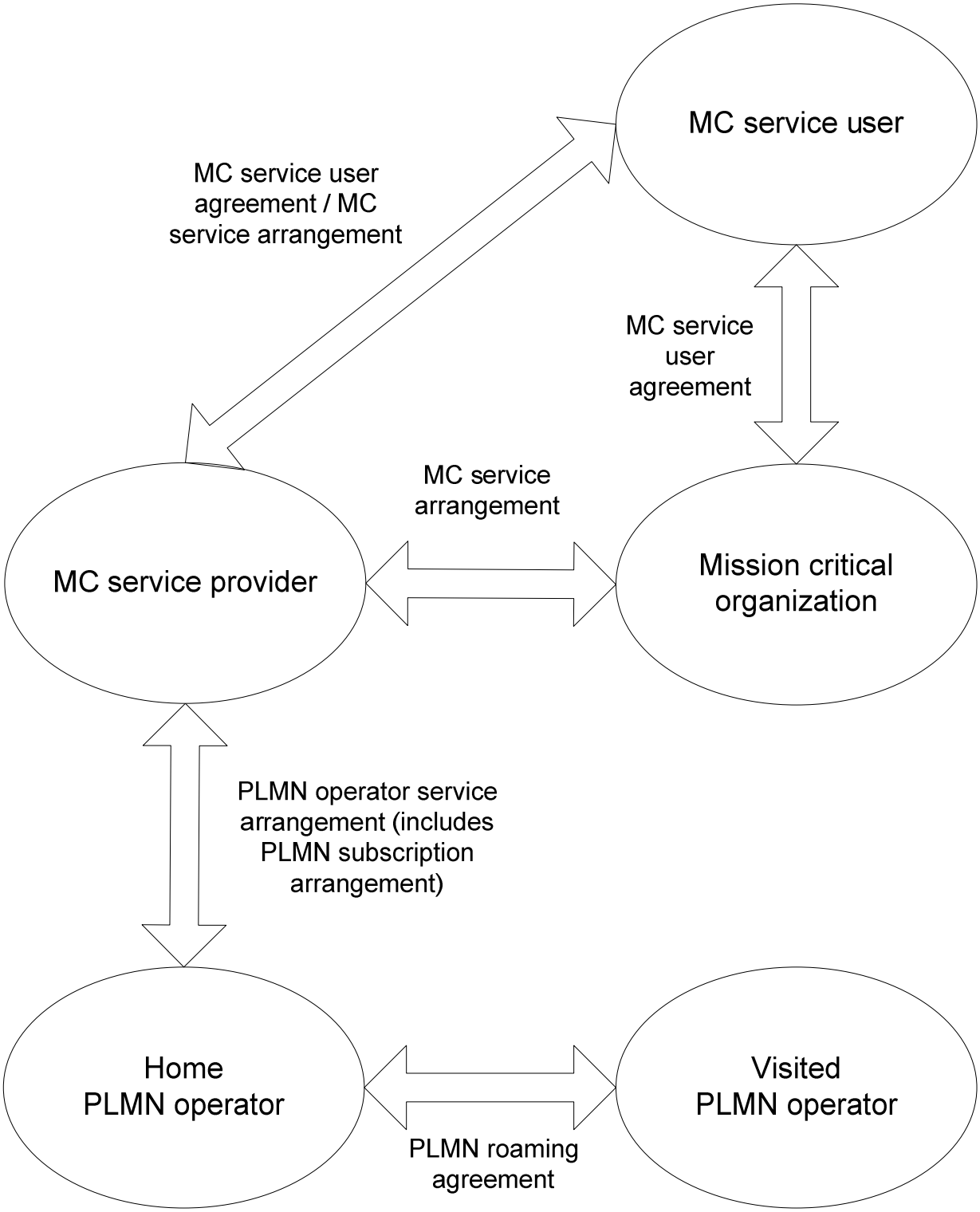

Figure 6-1: Business relationships for MC services

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.

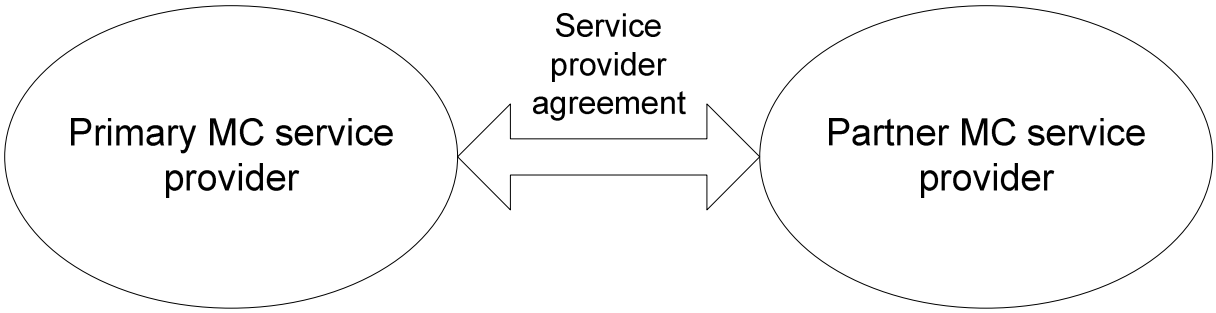

Figure 6-2: Additional business relationships for mutual aid

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.

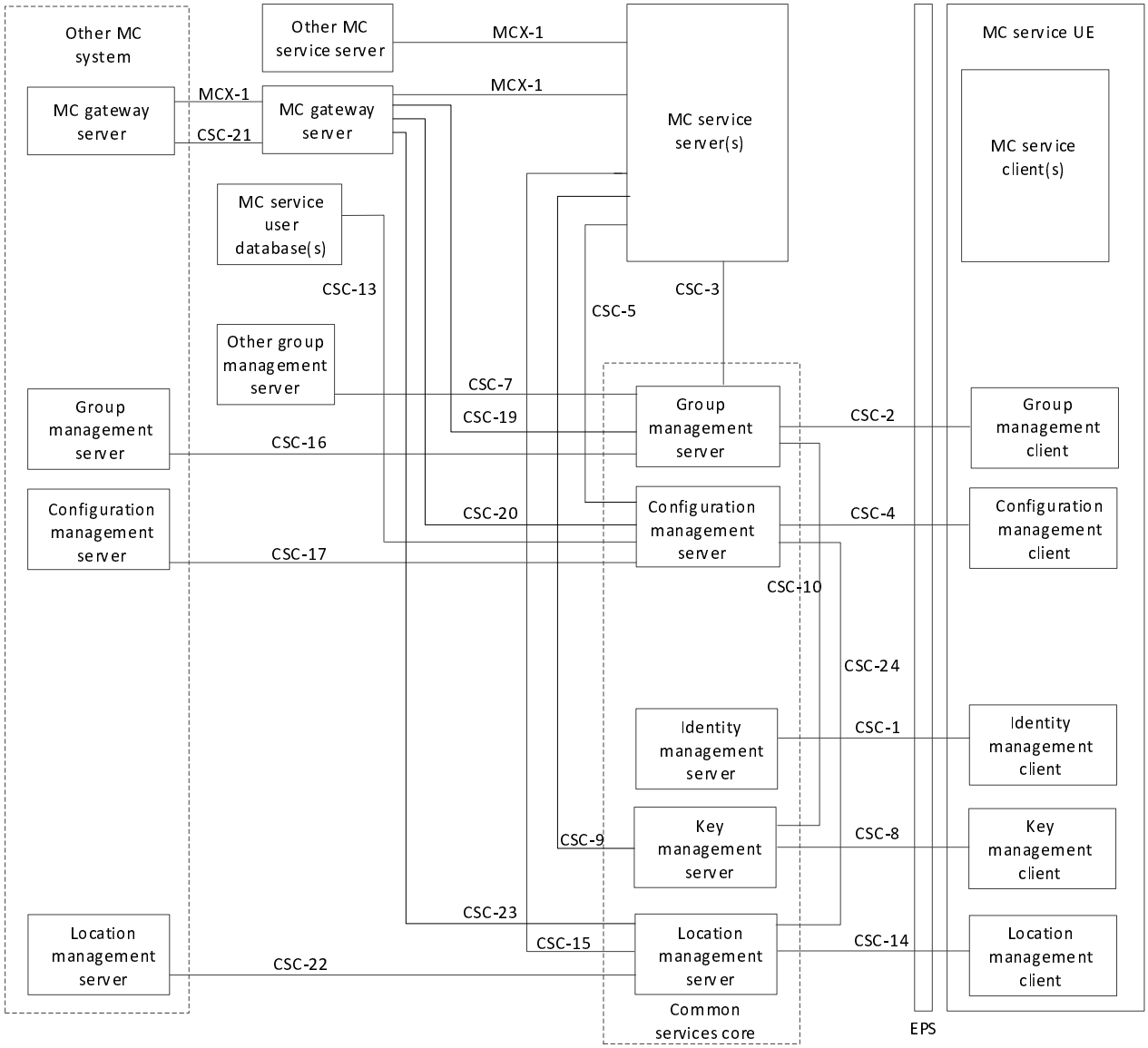

Figure 7.3.1-1: Functional model for application plane for an MC system

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].
- The functional alias management client is an integrated functional entity of the configuration management client. The functional alias management client is described in subclause 7.4.2.2.12.
- The functional alias management server is an integrated functional entity of the configuration management server. The functional alias management server is described in subclause 7.4.2.2.13.

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

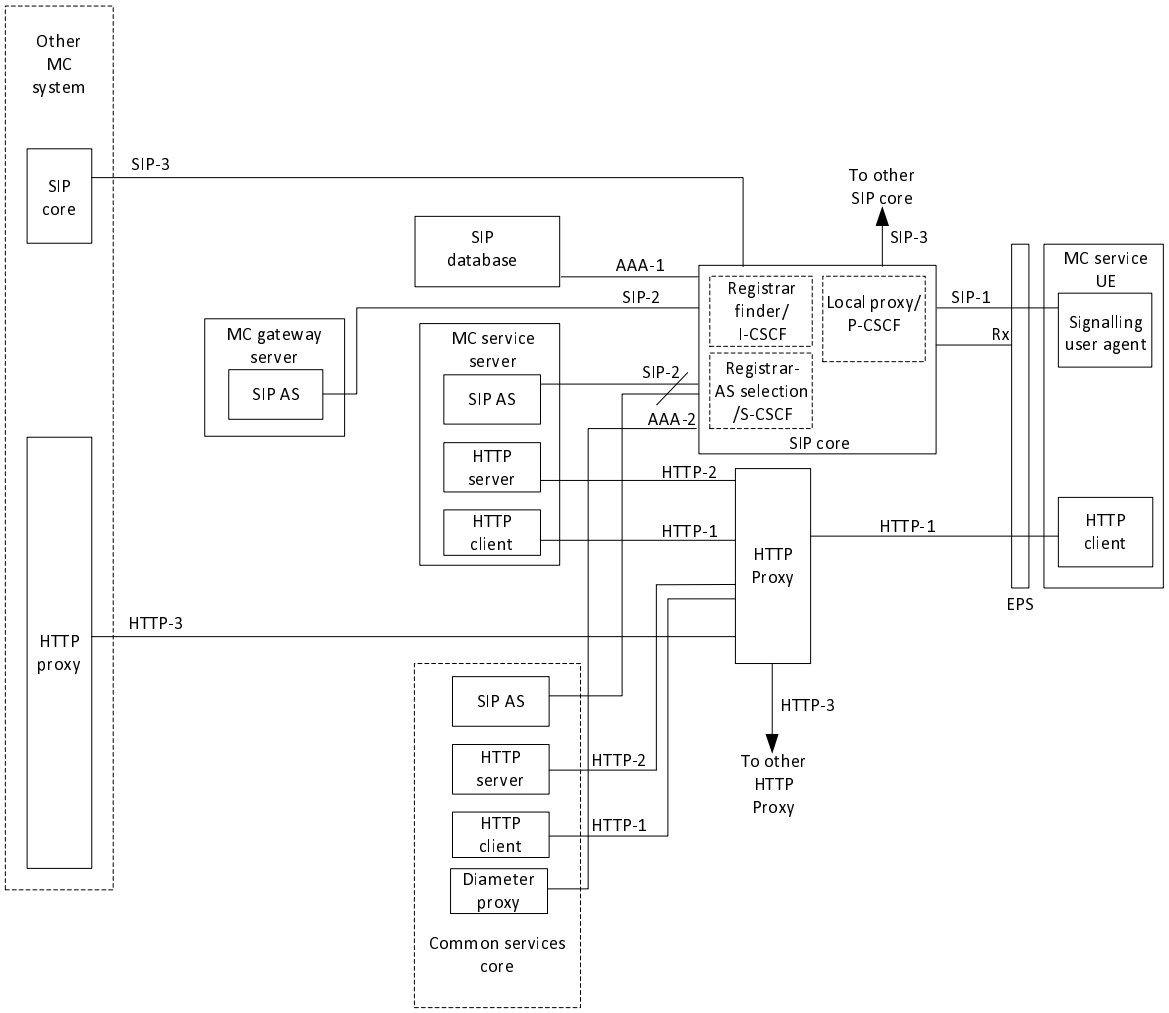

Figure 7.3.1-2: Functional model for signalling control plane

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.

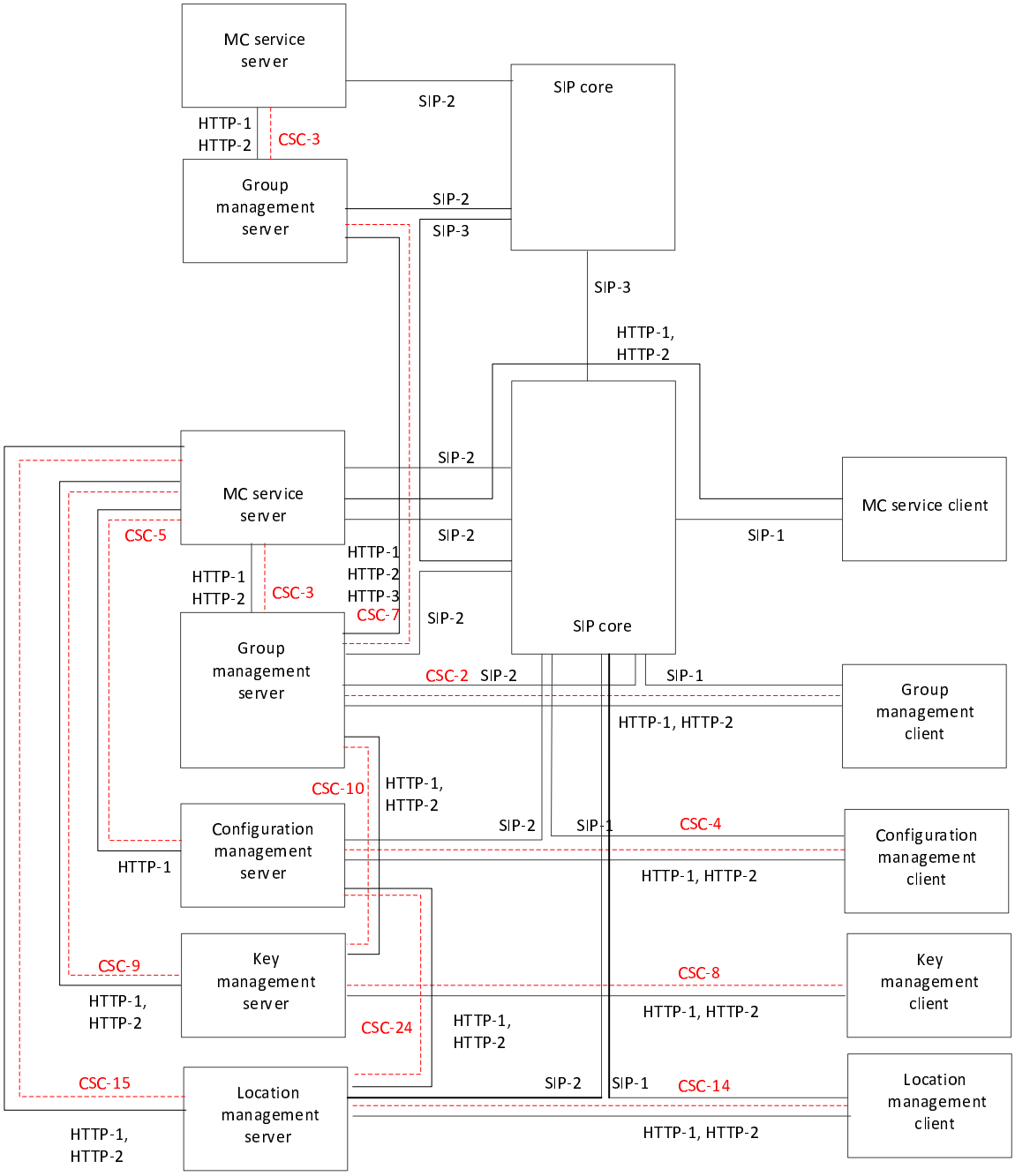

Figure 7.3.1-3: Relationships between reference points of MC service application plane and signalling control planes

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.

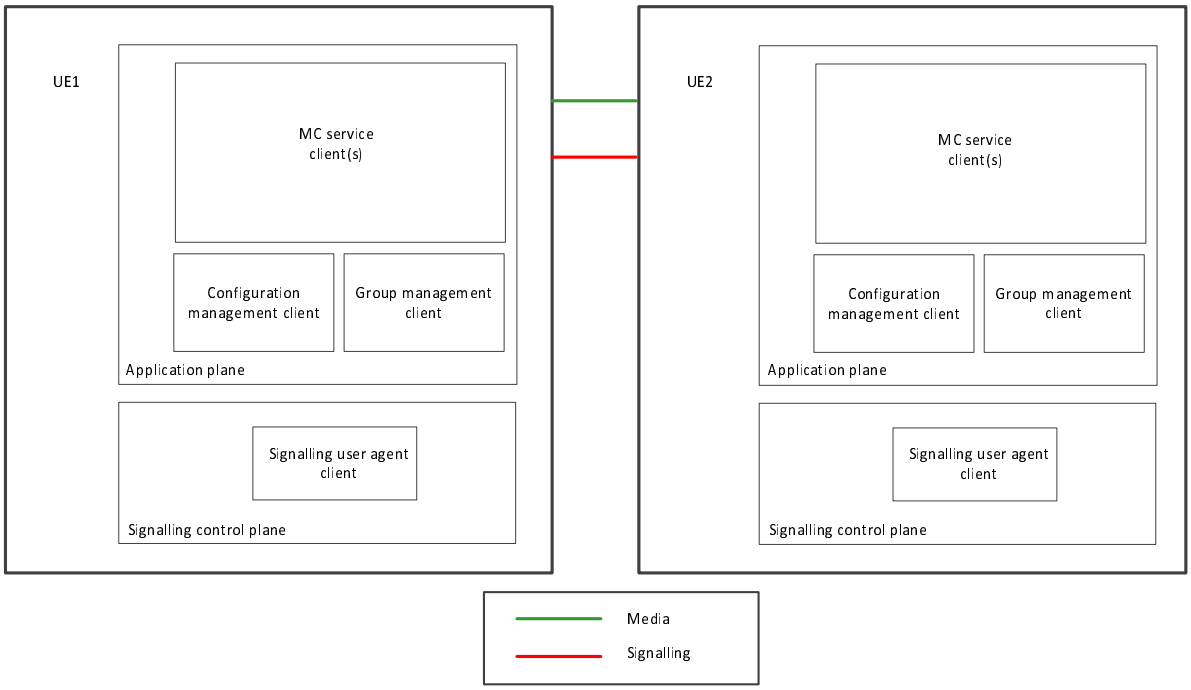

Figure 7.3.2-1: Functional model for MC service off-network operation

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.

The configuration management client provides the functional alias management client functionality as described in subclause 7.4.2.2.12.

7.4.2.2.2 Configuration management server (CMS)

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.

The configuration management server provides the functional alias management server functionality as described in subclause 7.4.2.2.13.

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 (GMS)

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 (IdMS)

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 33.180 [25].

7.4.2.2.8 Key management server (KMS)

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 33.180 [25].

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 (LMS)

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 (e.g. LCS network).

NOTE: The reference point and procedures to acquire location information from the PLMN operator are out of scope of the present document.

7.4.2.2.11 Void

7.4.2.2.12 Functional alias management client

The functional alias management client functional entity acts as the application user agent for management of functional aliases. The functional alias management client interacts with the functional alias management server.

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

7.4.2.2.13 Functional alias management server

The functional alias management server functional entity provides the configuration management of functional alias(es).

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

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 performs the functional alias controlling role for functional alias management including functional alias activation, deactivation, take over and interrogation. For a single functional alias, only one MC service server is specified as the functional alias controlling role. The detailed description of the functional alias controlling role assumed by the different MC service servers are contained in 3GPP TS 23.379 [16], 3GPP TS 23.281 [12] and 3GPP TS 23.282 [13].

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.

7.4.2.3.4 MC gateway server

The MC gateway server provides support for interconnection between a primary MC system and a partner MC system in a different trust domain whilst providing topology hiding. It acts as a proxy for one or more MC service servers in the partner MC system without needing to expose the MC service servers in the primary MC system outside the trusted domain of the primary MC system. It may be a role of an MC service server described in subclause 7.4.2.3.2 of the present document.

The MC gateway server is responsible for relaying signalling control messages and media between MC service servers in the interconnected MC systems.

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].

7.4.3.1.4 Diameter proxy

This functional entity acts as a proxy agent for Diameter messaging as specified in IETF RFC 6733 [26].

The Diameter proxy, when used on the AAA-2 interface may also be present in the SIP core / IMS.

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

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 terminates the HTTP-3 reference point that lies between different HTTP proxies. It may provide a topology hiding function from HTTP entities outside the trust domain of the MC system.

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 33.180 [25].

According to 3GPP TS 33.180 [25], 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 33.180 [25].

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 and SIP-3 reference points for transport and routing of subscription/notification related signalling. The SIP-3 reference point is used when a MC service server and the group management server, are served by different SIP cores.

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 and SIP-3 reference points for transport and routing of subscription/notification related signalling. The SIP-3 reference point is used when a MC service server and the configuration management server, are served by different SIP cores.

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 the same security domain. 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. The SIP-3 reference point is used when a pair of group management servers, are served by different SIP cores.

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 33.180 [25].

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 33.180 [25].

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 33.180 [25].

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.

7.5.2.16 Reference point CSC-16 (between group management servers in different MC systems)

The CSC-16 reference point, which exists between two group management servers in different MC systems in different security domains, is used by the group management servers to share group configuration information for MC service groups that can take part in interconnected MC service group calls.

The CSC-16 reference point uses the HTTP-1, HTTP-2 and HTTP-3 reference points for transport and routing of non-subscription/notification related signalling. The CSC-16 reference point uses SIP-2 and SIP-3 reference points for transport and routing of subscription/notification related signalling.

7.5.2.17 Reference point CSC-17 (between configuration management servers in different MC systems)

The CSC-17 reference point, which exists between configuration management servers in different MC systems in different security domains, is used by the configuration management servers to share user configuration information for MC service users who are permitted to migrate between the MC systems.

The CSC-17 reference point uses the HTTP-1, HTTP-2 and HTTP-3 reference points for transport and routing of non-subscription/notification related signalling.

7.5.2.18 Void

7.5.2.19 Reference point MCX-1 (between MC service servers)

The MCX-1 reference point is defined between MC service servers, between MC service servers and MC gateway servers and between MC gateway servers. The MC service servers and MC gateway servers may be located within one MC system or in separate MC systems. Furthermore, the MC service servers may be of the same type or different types.

This MCX-1 reference point is used by MC service servers' coordination procedures (e.g. priority coordination). This reference point is not part of the common service core functionality.

NOTE: The relation between MCX-1 and MCPTT-3 (see reference 3GPP TS 23.379 [16]), MCVideo-3 (see reference 3GPP TS 23.281 [4]) and MCData-3 (see reference 3GPP TS 23.282 [5]) is out of scope of the present document.

7.5.2.20 Reference point CSC-19 (between group management server and MC gateway server)

The CSC-19 reference point, which exists between the group management server and MC gateway server is used by the group management server for subscription and notification signalling related to group configuration information that is shared between MC systems to permit interconnection of MC service group calls.

The CSC-19 reference point uses the SIP-2 and SIP-3 reference points for transport and routing of subscription/notification related signalling. The SIP-3 reference point is used when a group management server and an MC gateway server, are served by different SIP cores.

7.5.2.21 Reference point CSC-20 (between configuration management server and MC gateway server)

The CSC-20 reference point, which exists between configuration management server and MC gateway server is used by the configuration management server for subscription and notification signalling related to user configuration information that is shared between MC systems to permit migration between MC systems.

The CSC-20 reference point uses the SIP-2 and SIP-3 reference points for transport and routing of subscription/notification related signalling. The SIP-3 reference point is used when a configuration management server and an MC gateway server, are served by different SIP cores.

7.5.2.22 Reference point CSC-21 (between MC gateway servers in different MC systems)

The CSC-21 reference point, which exists between MC gateway servers in different MC systems in different security domains, is used to share subscription and notification related signalling for group configuration, user configuration management and location management to permit interconnection and migration between MC systems.

The CSC-21 reference point uses the SIP-3 reference point for transport and routing of subscription/notification related signalling.

7.5.2.23 Reference point CSC-22 (between location management servers in different MC systems)

The CSC-22 reference point, which exists between location management servers in different MC systems, is used to share location information related signalling for location management for interconnected MC systems.

The CSC-22 reference point uses the HTTP-1, HTTP-2 and HTTP-3 reference points for transport and routing of non-subscription/notification related signalling.

The CSC-22 reference point uses the SIP-2 and SIP-3 reference points for transport and routing of subscription/notification and request/response related signalling.

7.5.2.24 Reference point CSC-23 (between location management server and MC gateway server)

The CSC-23 reference point, which exists between location management server and MC gateway server, is used to handle location management related signalling.

The CSC-23 reference point uses SIP-2 and SIP-3 reference points for transport and routing of subscription/notification and request/response related signalling.

The CSC-23 reference point uses the HTTP-1, HTTP-2 and HTTP-3 reference points for transport and routing of non-subscription/notification related signalling.

7.5.2.25 Reference point CSC-24 (between the Location management server and the configuration management server)

The CSC-24 reference point, which exists between the location management server and the configuration management server, to allow the location management server to obtain non-group configuration related information for location service (e.g. policy information). The CSC-24 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-24 reference point shall use SIP-2 reference point for transport and routing of 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.

7.5.3.9 Reference point AAA-2 (between the SIP core and Diameter proxy)

The AAA-2 reference point, which exists between the SIP core / IMS and Diameter proxy for SIP registration during migration, shall use the Cx reference point as defined in 3GPP TS 23.002 [6]. The AAA-2 reference point is used for:

- authentication and security to the service layer for migration;

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 33.180 [25].

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.

For the purposes of this document, an MC service administrator, MC service dispatcher, or MC service authorized user is an MC service user that has been granted special privileges within the context of the client function being performed (e.g. MC service client, group management client, configuration management client, key management client). For

example, the MC service ID of a group management client of an MC service administrator can be authorized within the group management server to create new groups and add members to groups (i.e. administrative function), but is not authorized to dynamically create group or user regroups (i.e. operational function). Alternatively, for example, the MC service ID of a dispatcher will typically be authorized to dynamically create group and user regroups, but is not authorized to create new groups or add/delete members to groups. The MC service authorization framework is defined in TS 33.180 [25].

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.

In 3GPP TS 23.379 [16], the MCPTT group ID is an MC service group ID.

In 3GPP TS 23.281 [12], the MCVideo group ID is an MC service group ID.

In 3GPP TS 23.282 [13], the MCData group ID is an MC service group ID.

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.

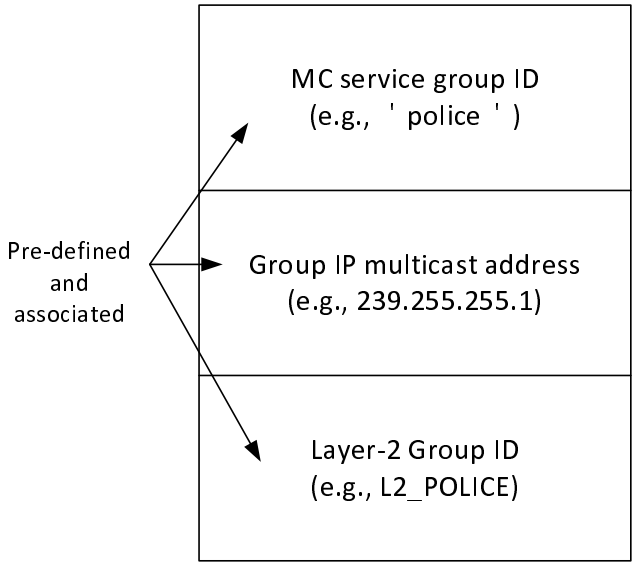

Figure 8.1.3.2-1: MC service group ID management in off-network operation

8.1.4 MC system identity (MC system ID)

The MC system ID is a globally unique identifier representing an MC system. The MC system ID shall be a URI.

8.1.5 Functional Alias

Functional alias provides a complementary, role-based user identification scheme which can be used by MC service users for operational purposes in the form of meaningful elements such as the function, the order number or vehicle identifications that can be used within any form of MC service communication. Functional alias takes a form of a URI where the host part of the URI shall identify the home MC system MC service functional alias controlling server. The application addressing remains in its form and forms the foundation for the association with the corresponding functional alias. An MC service user can simultaneously activate several functional aliases but only one can be associated to a certain communication.

Each functional alias is subject to the uniqueness principle within an organization and can be shared simultaneously by several MC service users, depending on the assignment. In this case, all assigned MC service users sharing a functional alias can be included in a communication.

An MC service user uses a different set of functional aliases when migrating towards another service organization to allow the MC service user to be reachable by functional aliases within that organization.

The use of a functional alias always requires an association with the MC service ID. The MC service ID needs to be used to provide the security context for a communication.

8.1.6 MC service UE label

The optional MC service UE label allows to distinguish between different MC service UEs in use by the same MC service ID. The MC service UE label may be added to location information reports.

The non-routable MC service UE label may include human readable information, such as an incident or MC service user specific ID, manufacturer name, brand, model, serial number, etc.

NOTE: The MC service UE label may be provided during initial MC service UE configuration, see clause A.6.

8.1.7 Void

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.

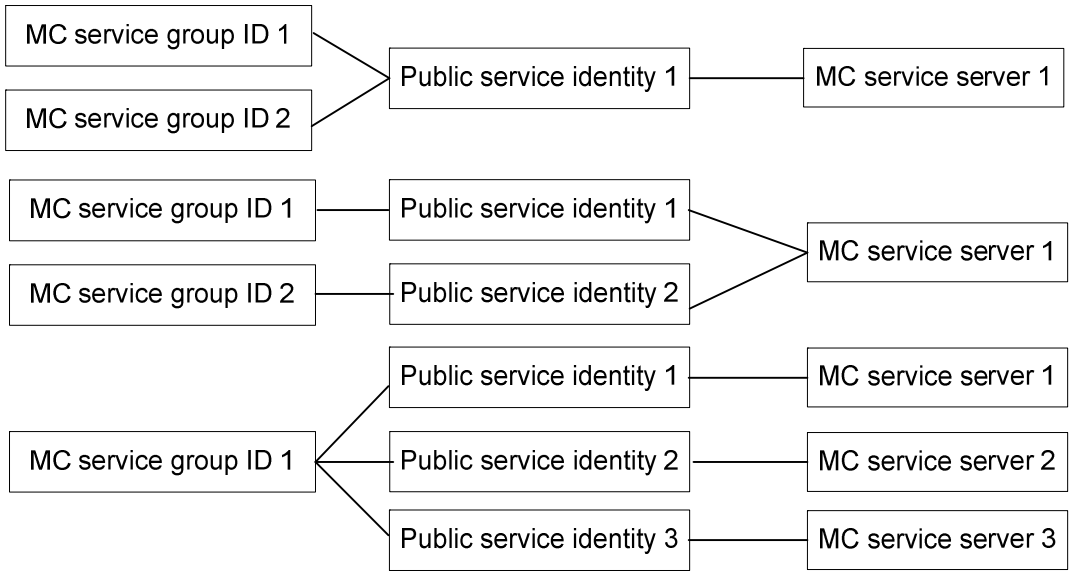

Figure 8.3.2-1: The relationship of MC service group IDs, PSIs and MC service servers

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.

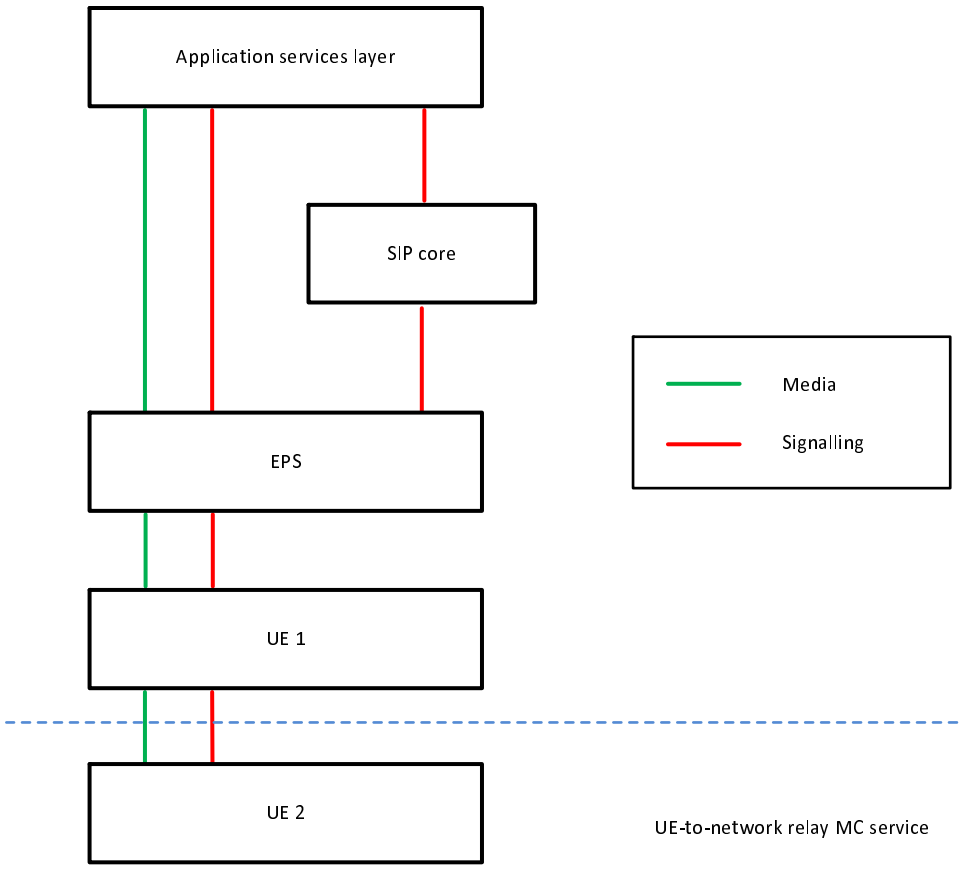

Figure 9.2.1.1-1: On-network architectural model

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.

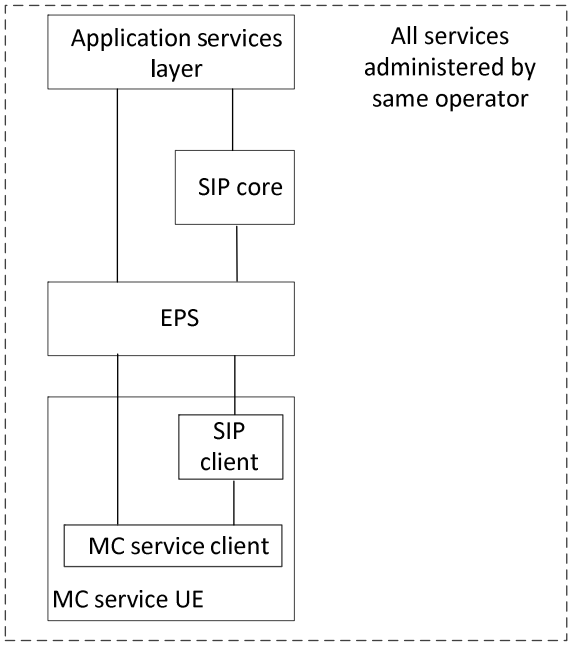

Figure 9.2.2.1.2-1: Common administration of all services by one operator

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.

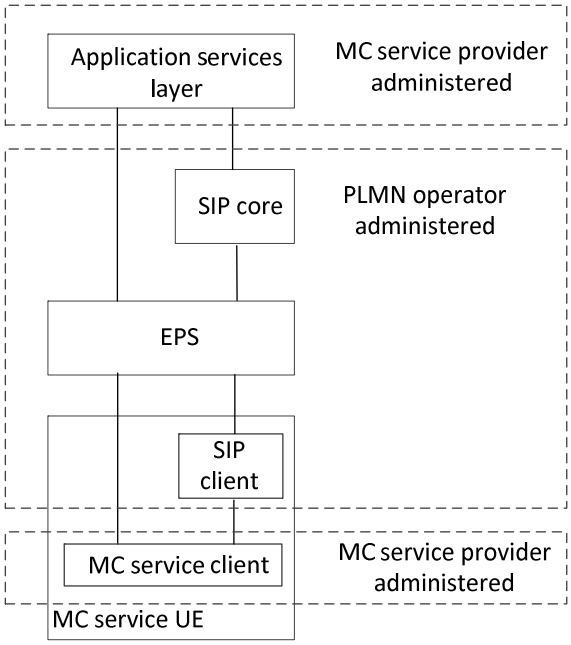

Figure 9.2.2.1.3-1: MC service provider administers MC service separately from SIP core and EPS

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.

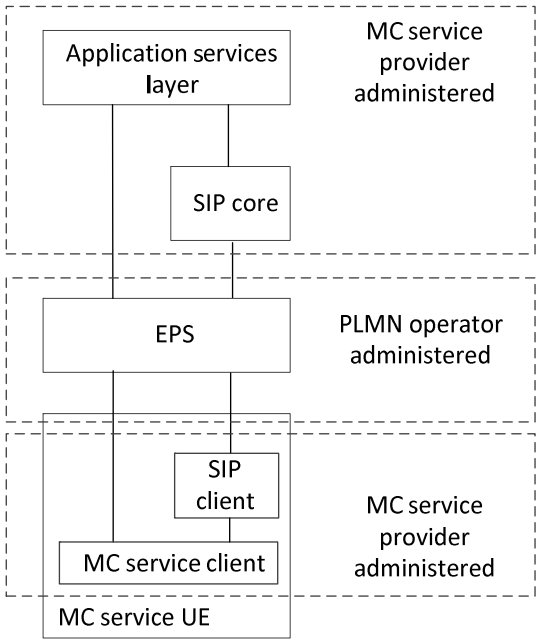

Figure 9.2.2.1.4-1: MC service provider provision of SIP core, separate domain from EPS

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.

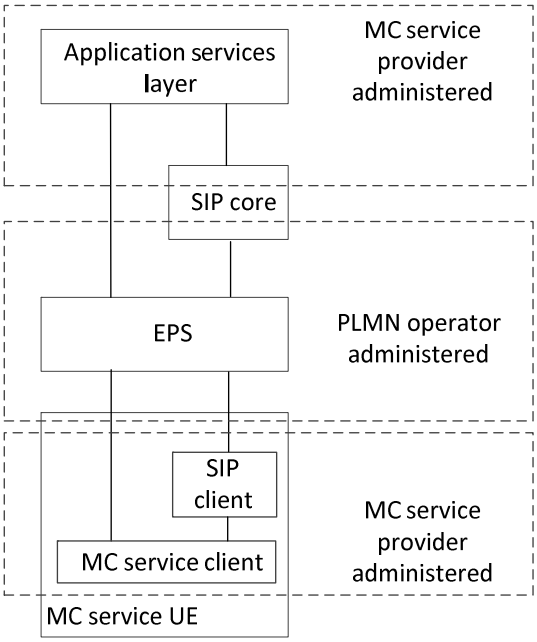

Figure 9.2.2.1.5-1: MC service provider partial provision of SIP core, separate domain from EPS

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.

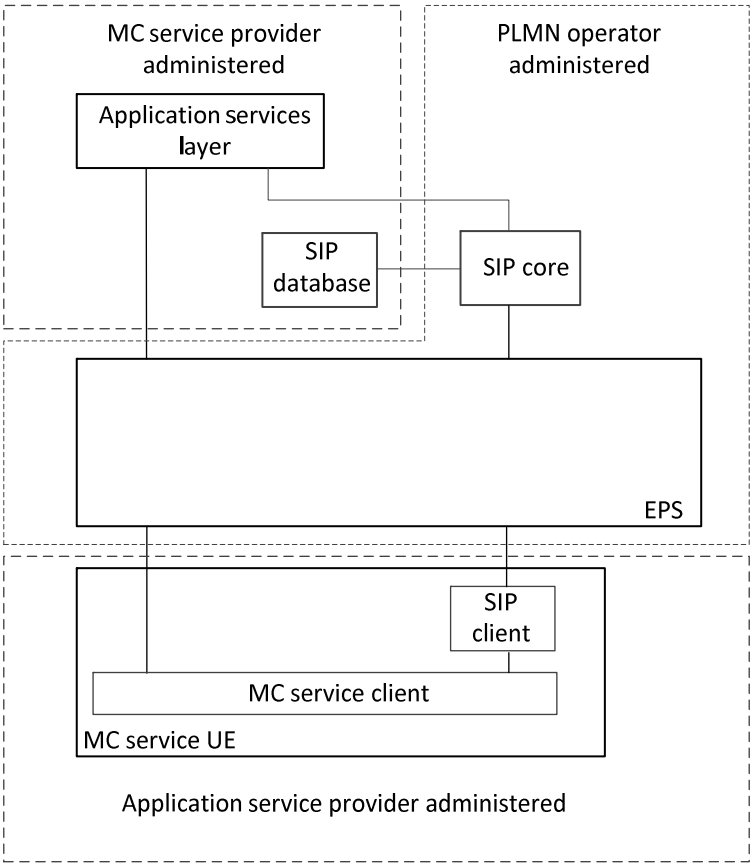

Figure 9.2.2.1.6-1: MC service provider provides identities to PLMN operator SIP core

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.

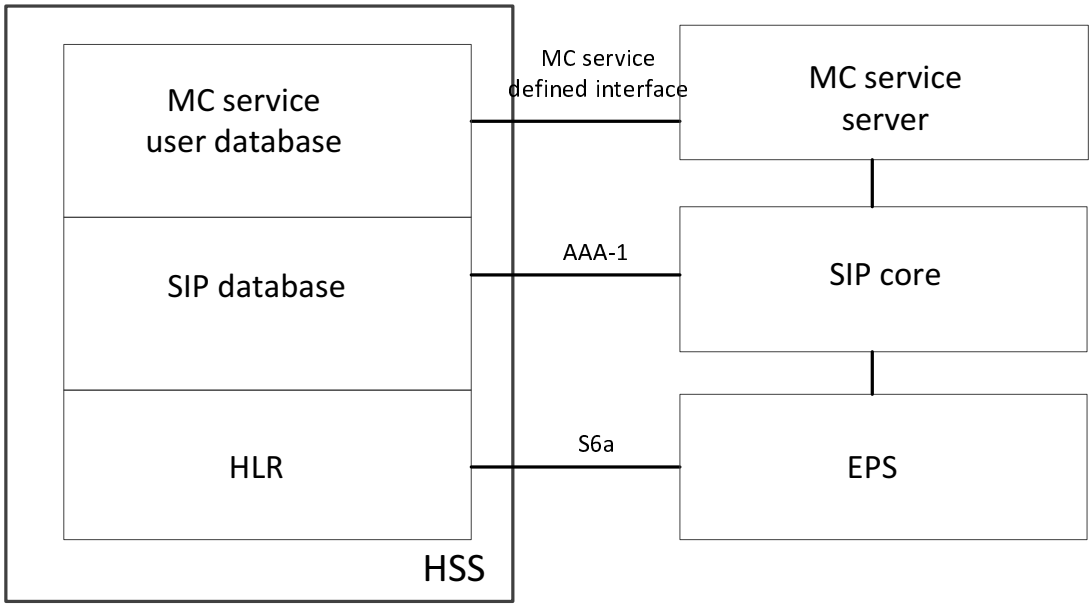

Figure 9.2.2.2-1: Collocation of MC service user database and SIP database with HSS

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.

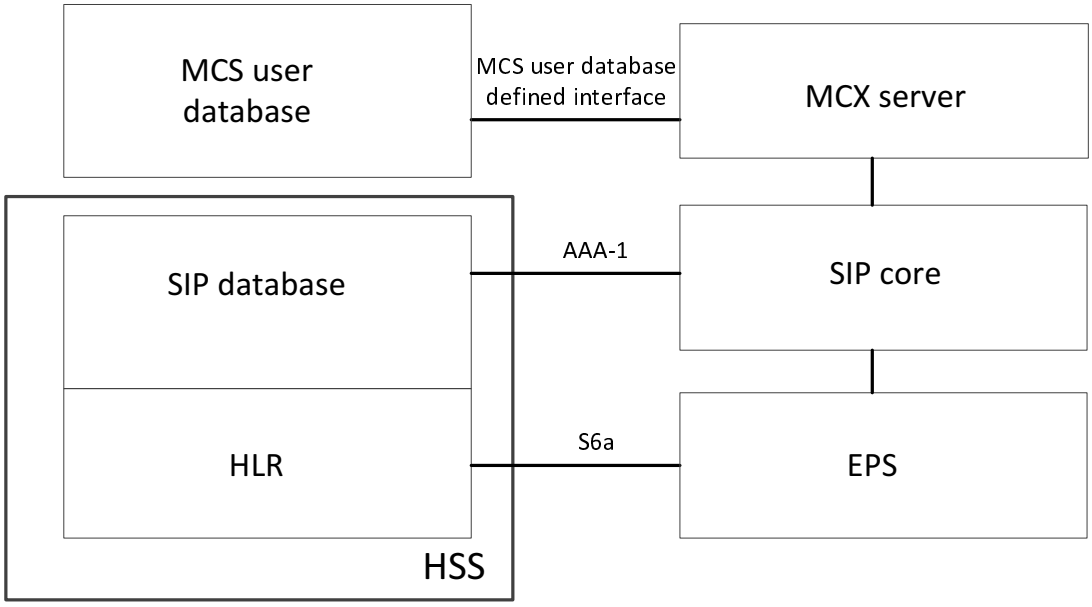

Figure 9.2.2.2-2: Shared PLMN operator and MC service provider based deployment of MC service - SIP database collocated with HSS with separate MC service user database

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.

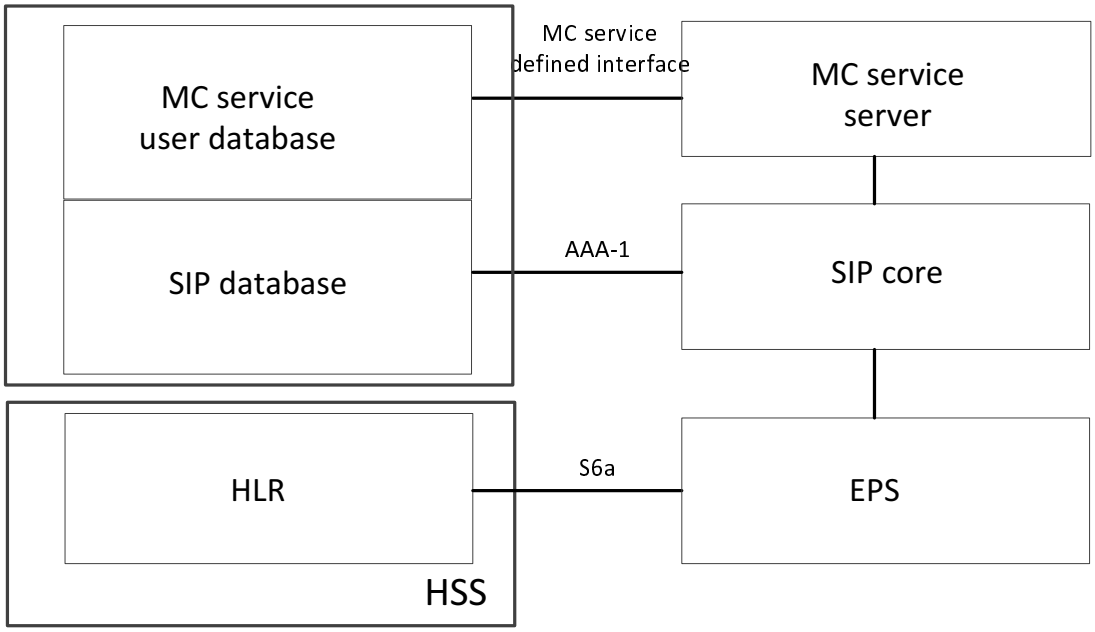

Figure 9.2.2.2-3: Shared PLMN operator and MC service provider based deployment of MC service - MC service user database and SIP database deployed together, with separate HSS

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.

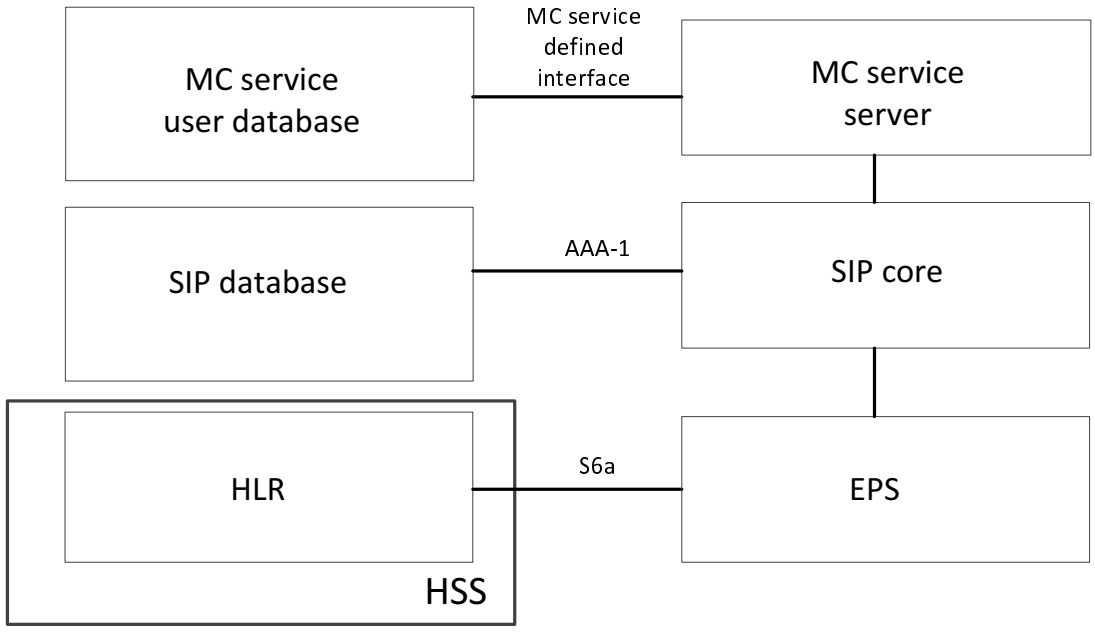

Figure 9.2.2.2-4: Shared PLMN operator and MC service provider based deployment of MC service - separate HSS, MC service user database and SIP database

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.

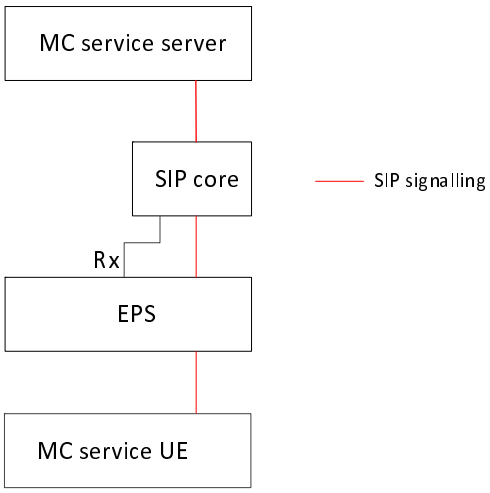

Figure 9.2.2.3.2-1: Bearer control by SIP core

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.

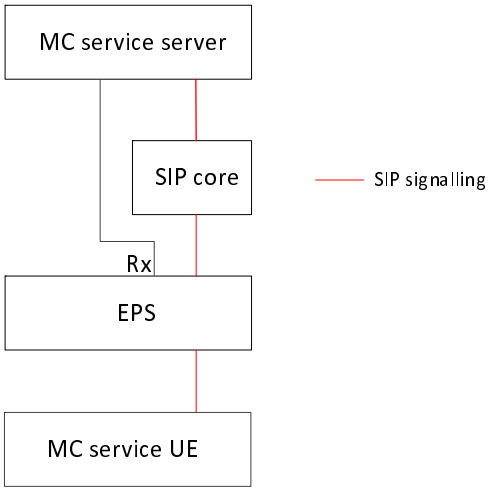

Figure 9.2.2.3.3-1: Bearer control by MC service server

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.

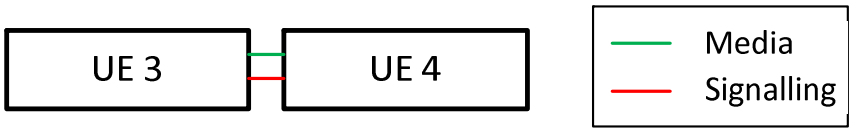

Figure 9.3.1-1: Off-network architectural model for inter-UE communication where no relay function is used

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

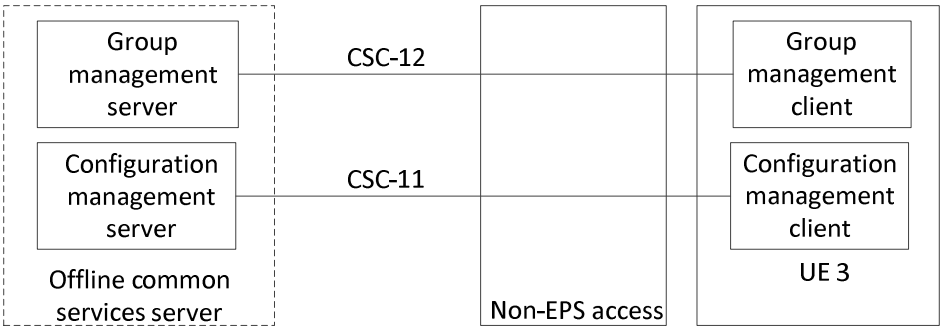

Figure 9.3.1-2: Off-network architectural model for configuration management and group management

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

10.1.1.1 MC service configuration on primary MC system

Depicted in figure 10.1.1.1-1 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.

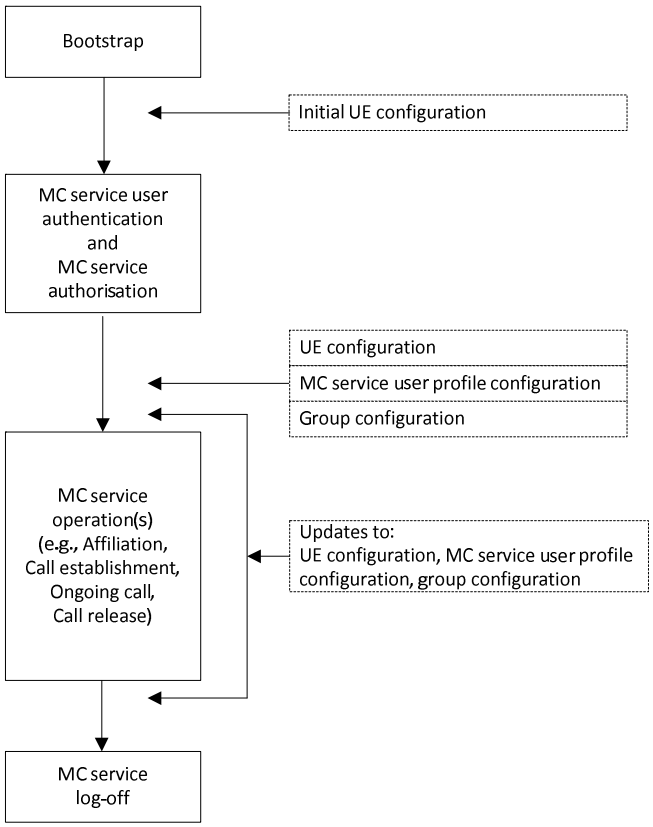

Figure 10.1.1.1-1 MC service UE configuration time sequence and associated configuration data

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, functional alias 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. When this happens, the MC service UE shall apply these updates and use them for further operations. 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 after 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 10.1.1.1-1) which the MC service enforces during the entire phase of MC service UE using the MC service.

NOTE: The extent of MC services available to an MC service UE with an unauthenticated MC user or unauthorized MC service user is described as 'limited services' in 3GPP TS 33.180 [25] is out of scope of the present document.

10.1.1.2 MC service configuration for migration to partner MC system

Figure 10.1.1.2-1 depicts a general MC service configuration time sequence of the data related to MC service, representing the general lifecycle of MC service UE which obtains MC service when migrated to a partner MC system. The MC service user can only receive MC service from one MC system at a time.

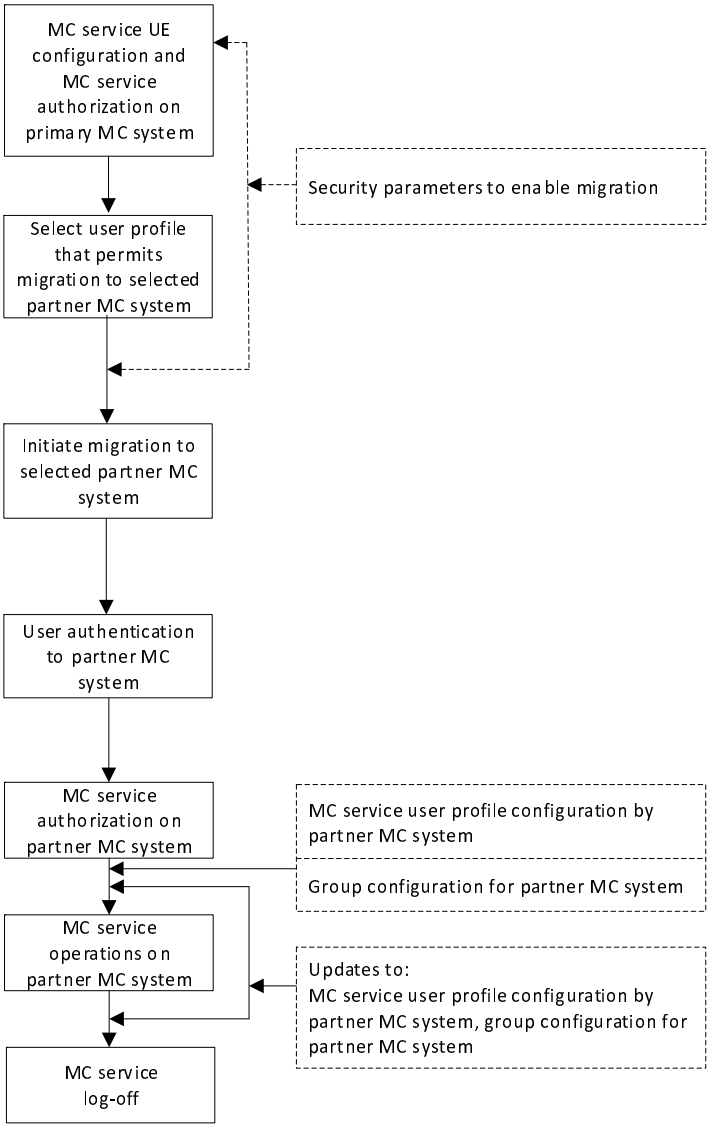

Figure 10.1.1.2-1 MC service UE configuration sequence for migration

The MC service user and MC service UE first follow the MC service UE configuration and MC service user authorization steps described in subclause 10.1.1.1 to obtain one or more MC service user profiles from the primary MC system. Each user profile received from the primary MC system contains a list of partner MC systems to which migration is permitted using that user profile, together with the access information needed to communicate with the application plane servers of the partner MC system. See Annex A.3 for more information. The MC service user also obtains the necessary security parameters needed to authenticate and become service authorized on the partner MC system; the process for this is specified in 3GPP TS 33.180 [25]. At this point, the MC UE is configured sufficiently for the partner system so that the MC service user is capable of utilizing "limited services" as described in 3GPP TS 33.180 [25].

NOTE 1: The above steps which enable migration to take place may be carried out some time in advance of migration. The MC service user could repeatedly obtain migrated MC service, e.g. on successive days while located in the area of the partner MC system, without needing to obtain the initial configuration afresh in advance of each period of migrated MC service. The user profile from the primary MC system must be retained to provide the access information to permit this.

To initiate migration, the desired partner system from those listed in the chosen user profile is selected, and the access information provided in the user profile is used to initiate communication with the partner MC system.

NOTE 2: Selection of the relevant partner MC system could be performed as a result of a manual action by the user or automatically by an application in the MC service UE, e.g. according to the current location of the MC service UE or according to the serving PLMN of the MC service UE.

The MC service user performs user authentication to the partner MC system as specified in 3GPP TS 33.180 [25].

The user profile or profiles for that MC service user which are to be used for service when migrated to the partner MC system are then downloaded to the configuration management client in the MC service UE by the partner MC system, and these downloaded profile or profiles are used by the MC service user during the ensuing period of MC service on the partner MC system.

NOTE 3: The user profile obtained from the primary MC system is simply used to provide access information for the partner MC system and is not otherwise used by the MC service client during migrated MC service.

Group configuration for the MC service groups listed in the user profile are then obtained by the group management client in the MC service UE. After these configuration steps, the MC service user obtains service authorization on the partner MC system.

Once service authorized, further configuration changes may be provided by the partner MC system during the period of operational MC service, in accordance with subclause 10.1.1.1. The partner MC system enforces the use of the user profiles and group configuration that have been provided by the configuration process described in this subclause.

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		

10.1.2.5a Subscribe group policy request

Table 10.1.2.5a-1 describes the information flow subscribe group policy request from the MC service server to the group management server.

Table 10.1.2.5a-1: Subscribe group policy 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: The 'MC services requested' is the same service that requesting MC service server supports.		

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

10.1.2.6a Subscribe group policy response

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

Table 10.1.2.6a-1: Subscribe group policy 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 (see NOTE)	O	Reference to information stored relating to the MC service group
Group related key material (see NOTE)	O	Key material for use with the MC service group
NOTE: At least one of these information elements shall be present.		

10.1.2.7a Notify group policy request

Table 10.1.2.7a-1 describes the information flow notify group policy request from the group management server to the MC service server.

Table 10.1.2.7a-1: Notify group policy 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

10.1.2.8 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

10.1.2.8a Notify group policy response

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

Table 10.1.2.8a-1: Notify group policy 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

10.1.2.9 Get functional alias configuration request

Table 10.1.2.9-1 describes the information flow get functional alias configuration request from the functional alias management client or the MC service server to the functional alias management server.

Table 10.1.2.9-1: Get functional alias configuration request

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

10.1.2.10 Get functional alias configuration response

Table 10.1.2.10-1 describes the information flow get configuration response from the functional alias management server to the functional alias management client or the MC service server.

Table 10.1.2.10-1: Get functional alias configuration response

Information element	Status	Description
Functional alias	M	URI of the functional alias
Functional alias configuration data	M	Functional alias configuration data

10.1.2.11 Subscribe functional alias configuration request

Table 10.1.2.11-1 describes the information flow subscribe functional alias configuration request from the functional alias management client or the MC service server to the functional alias management server.

Table 10.1.2.11-1: Subscribe functional alias configuration request

Information element	Status	Description
Functional alias	M	URI of the functional alias
MC services requested (see NOTE)	O	Service(s) for which functional alias configuration is requested; one or more of MCPTT, MCVideo, MCData
NOTE: If 'MC services requested' is not present, functional alias configuration is requested for all services defined for the functional alias.		

10.1.2.12 Subscribe functional alias configuration response

Table 10.1.2.12-1 describes the information flow subscribe functional alias configuration response from the functional alias management server to the functional management client or the MC service server.

Table 10.1.2.12-1: Subscribe functional alias configuration response

Information element	Status	Description
Functional alias	M	URI of the functional alias
Result	M	Indicates the success or failure for the result

10.1.2.13 Notify functional alias configuration request

Table 10.1.2.13-1 describes the information flow notify functional alias configuration request from the functional alias management server to the functional alias management client or the MC service server.

Table 10.1.2.13-1: Notify functional alias configuration request

Information element	Status	Description
Functional alias	M	URI of the functional alias
Functional alias information reference	M	Reference to information stored relating to the functional alias

10.1.2.14 Notify functional alias configuration response

Table 10.1.2.14-1 describes the information flow notify functional alias configuration response from the functional alias management client or the MC service server to the functional alias management server.

Table 10.1.2.14-1: Notify functional alias configuration response

Information element	Status	Description
Functional alias	M	URI of the functional alias
Result	M	Indicates the success or failure for the result

10.1.2.15 Void

10.1.2.16 Void

10.1.2.17 Void

10.1.2.18 Void

10.1.2.19 Void

10.1.2.20 Void

10.1.2.21 Void

10.1.2.22 Void

10.1.2.23 Void

10.1.2.24 Void

10.1.2.25 Void

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.

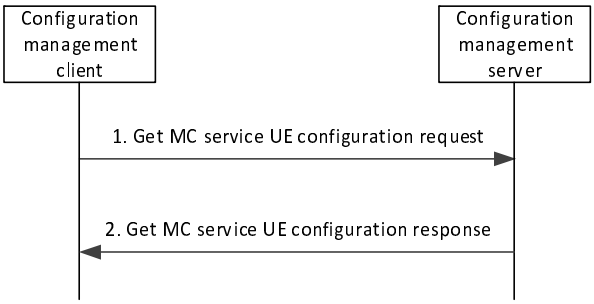

Figure 10.1.3.2-1: MC service UE obtains the configuration data

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.

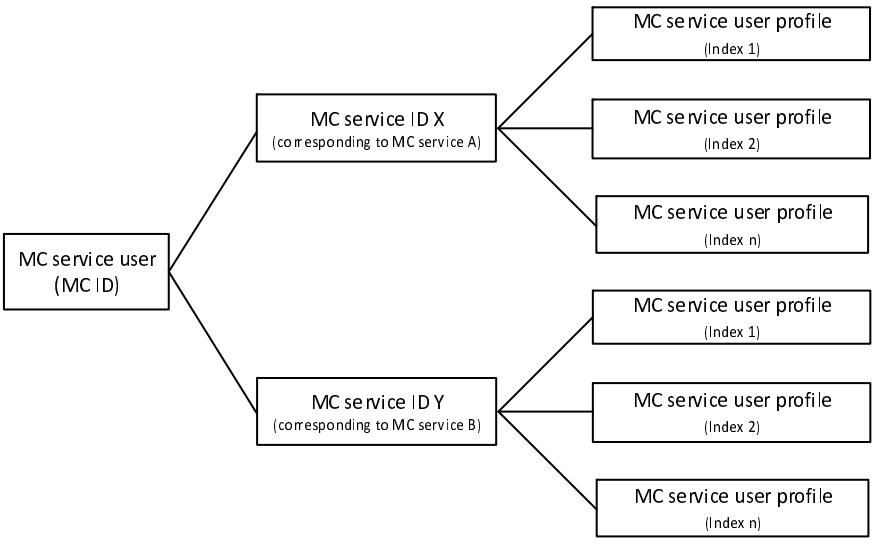

Figure 10.1.4.1-1: The relationship of MC service user, MC service IDs, MC service user profile and MC services

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. The MC service user may have one or more specific MC service user profiles defined for use in migration cases, whereby there may be more than one MC service user profiles defined for migration for that MC service user e.g. so that different MC service user profiles can be applied in different partner MC systems. The appropriate MC service user profile for migration for the relevant partner MC system will be provided to the partner MC system by the procedure. For both the cases of MC service on the primary MC system of the MC service user, and MC service when migrating to a partner MC system, 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 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).

When an MC service user is receiving MC service in its primary MC system, 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). For a migrating MC service user, the MC service user profile provisioning in the UE is initiated when the MC service user attempts to migrate to a partner MC system, and requests the MC service user profile from a nominated configuration management server in the partner MC system, prior to requesting service authorization from a partner MC service server.

The partner MC system may require that the MC service user profiles for migrating MC service users have parameters imposed by that partner MC system according to its operating and security policies. For example, there may be limitations in the locations at which migrating MC users can receive service, specific priority levels for migrating MC service users or certain groups to which the migrating MC service users require access. The partner MC system applies any necessary modifications to the MC service user profile received from the primary MC system of the MC service user in accordance with its local requirements. This local profile will be stored, and will be provided to the configuration management server in the partner MC system in order to distribute it to the configuration management client of the migrating MC service user. This modified profile may be sent to the primary MC system of the migrating MC service user so that the primary MC system can validate the modified profile before it is provided to the migrating MC service UE. The modified MC service user profile will subsequently be provided to the MC service server in the partner MC system when the migrating MC user attempts service authorization.

NOTE: Configuration tables in Annex A to indicate where the local configuration policy can be configured are out of scope of the present document.

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. This information flow is sent individually addressed on unicast or multicast.

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

10.1.4.3.1 MC service user receiving MC service in primary MC system

The procedure for the MC service user obtaining MC service user profiles in the primary MC system of that MC service user is illustrated in figure 10.1.4.3.1-1.

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.

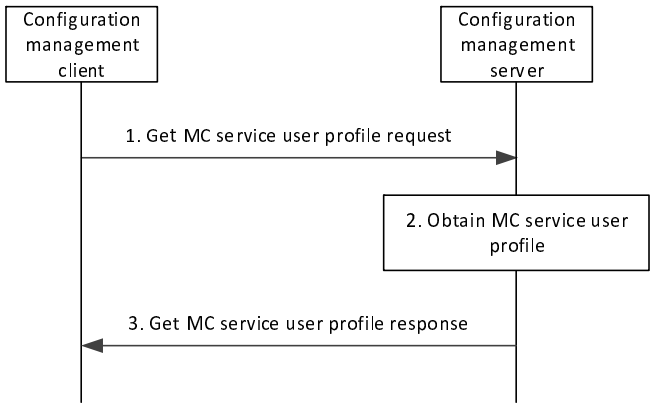

Figure 10.1.4.3.1-1: MC service user obtains the MC service user profile(s) from the network

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.

10.1.4.3.2 MC service user receiving MC service from a partner MC system

Figure 10.1.4.3.2-1 below illustrates mechanism for the configuration management client to retrieve the MC service user profile for the migrating MC service user from the partner MC system.

NOTE: Any proxy servers at the edges of the primary and partner MC systems which are used to hide the topology of the MC systems from external entities are not shown in this procedure.

Preconditions

- The MC service user is permitted to migrate to the partner MC system, and the relevant authorizations are configured in both the primary and partner MC systems of that MC service user
- The MC service user has performed MC service user authentication in the partner MC system, and has received the necessary credentials to retrieve configuration information and to request service authorization.
- The MC service UE has been provided with addressing information to allow the configuration management client in the MC service UE to access the configuration management server in the partner MC system.

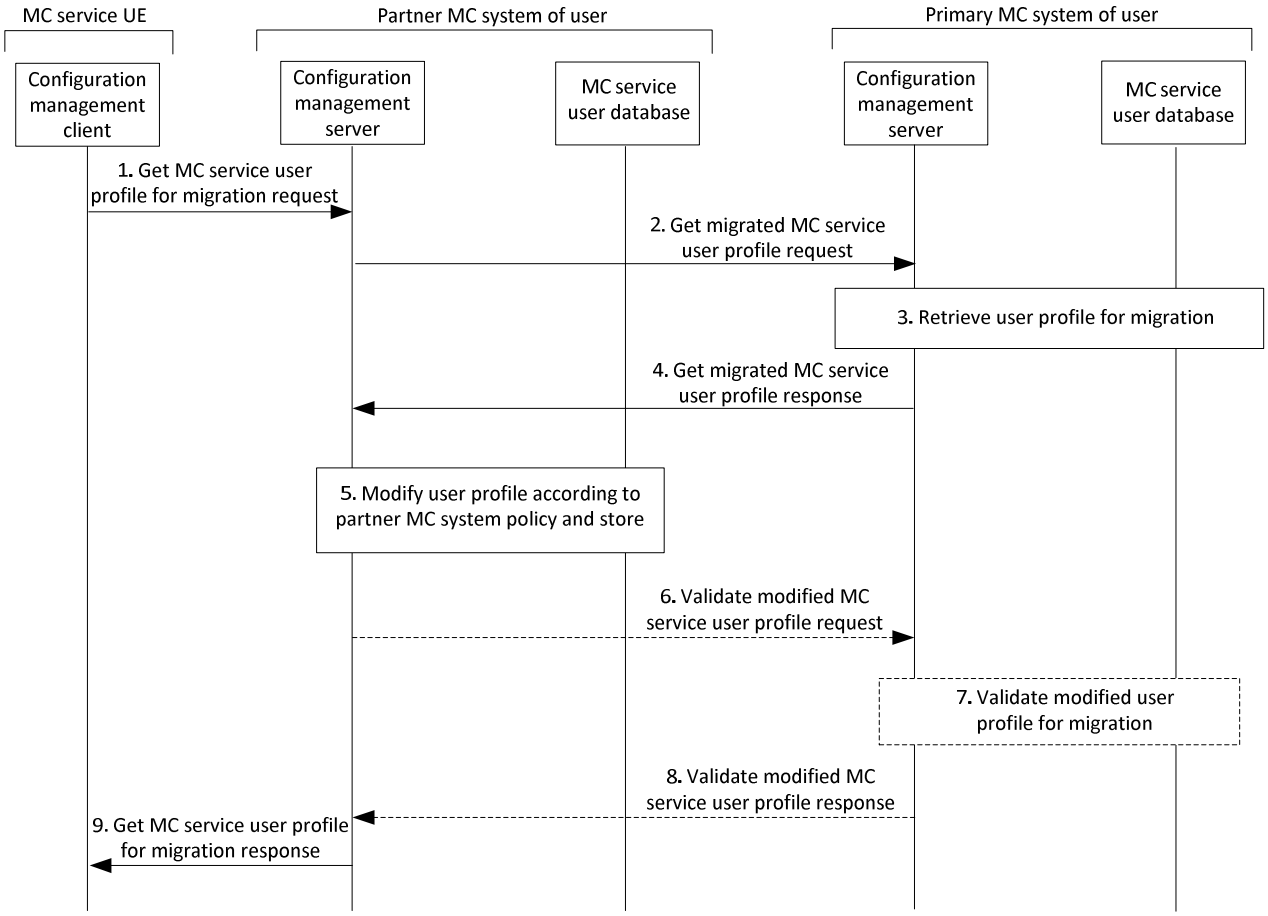

Figure 10.1.4.3.2-1: Retrieval of user profile in partner MC system

1. The configuration management client in the MC service UE of the migrating MC service user requests the MC service user profile for migration from the configuration management server in the partner MC system.
2. The configuration management server in the partner MC system requests the MC service user profile from the configuration management server in the primary MC system of the MC service user.
3. The configuration management server in the primary MC system of the MC service user retrieves the MC service user profile from the MC service user database in that primary MC system. The identification of the partner MC system to which the MC service user is attempting to migrate is used to determine which MC service user profile is retrieved for that MC service user for migration to that partner MC system.

4. The configuration management server in the primary MC system provides the MC service user profile to the configuration management server in the partner MC system of the MC service user, optionally requesting validation of the modified MC service user profile.

5. The partner MC system of the MC service user modifies the MC service user profile according to local configuration information and stores the modified MC service user profile in the MC service user database in the partner MC system.

6. If the primary MC system requested validation of the MC service user profile in step 4, the configuration management server in the partner MC system of the migrating MC service user may send the modified MC service user profile to the configuration management server of the primary MC system of the MC service user to allow the primary MC system of the MC service user to validate the modified MC service user profile.

7. The primary MC system of the migrated MC service user validates the modified MC service profile of the migrated MC service user.

8. The primary MC system of the migrated MC service user responds to the partner MC system with the results of the validation process.

9. The configuration management server in the partner MC system provides the MC service user profile to the configuration management client of the migrating MC service user,

NOTE: Step 9 is not followed if the validation process fails.

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.

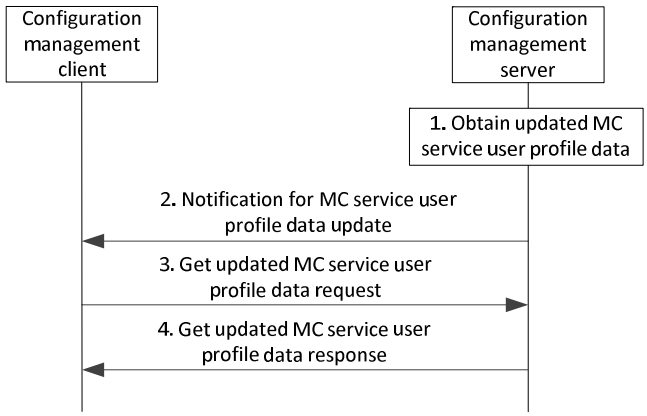

Figure 10.1.4.4-1: MC service user receives updated MC service user profile data from the network

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.

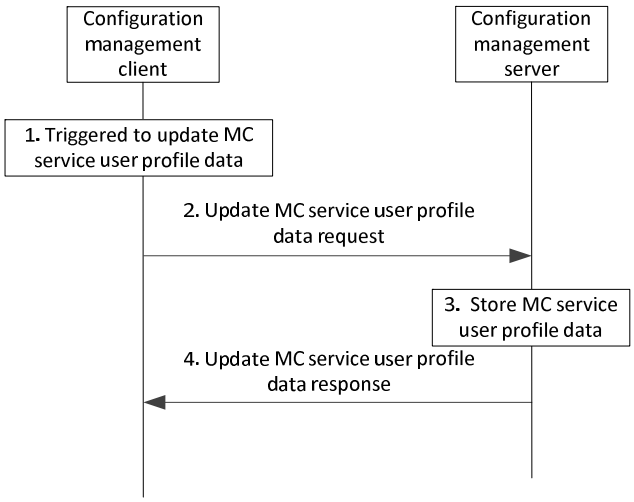

Figure 10.1.4.5-1: MC service user updates MC service user profile data to the network

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.

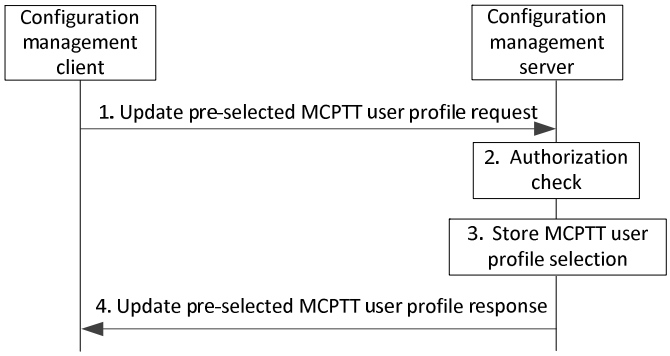

Figure 10.1.4.6-1: MC service user updates the pre-selected MC service user profile

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 1: 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.

NOTE 2: Specifying a pre-selected MC service user profile specific to each UE associated with an MC service user is out of scope of the present document.

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.

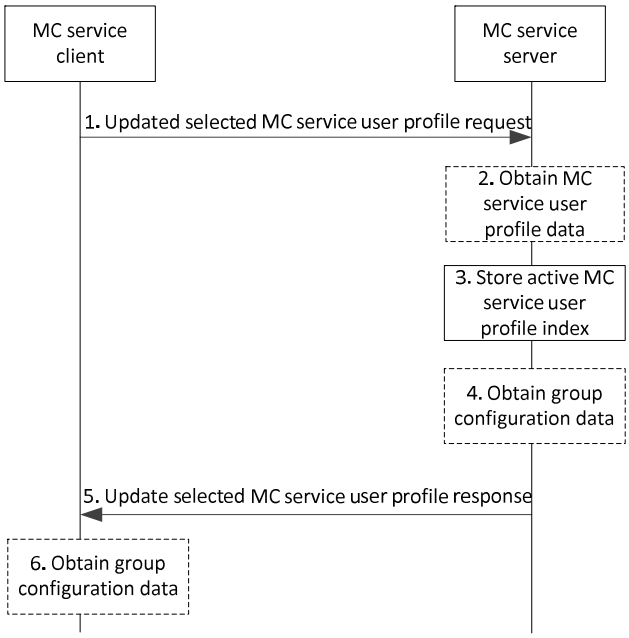

Figure 10.1.4.7-1: MC service user updates the selected MC service user profile

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;

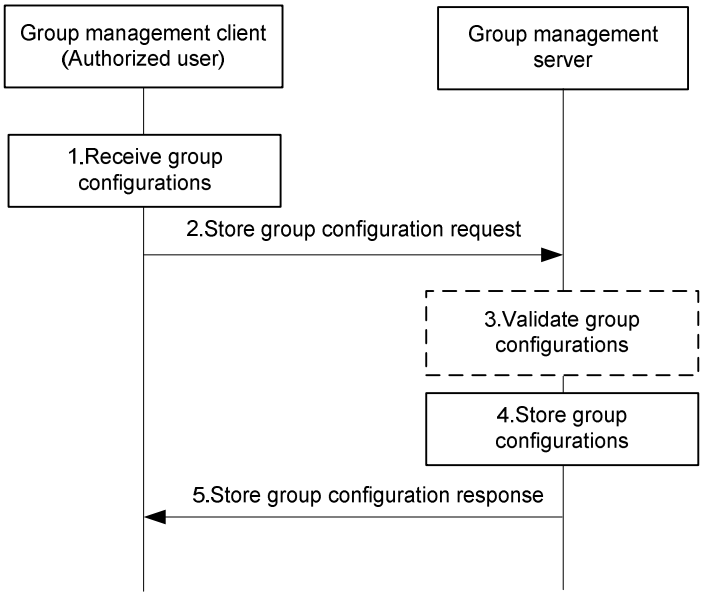

Figure 10.1.5.1-1: Store group configurations at group management server

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.

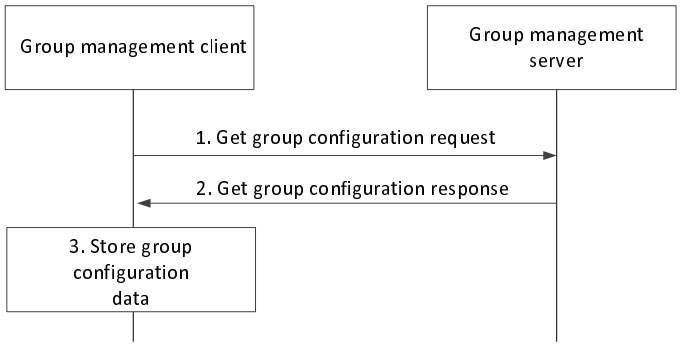

Figure 10.1.5.2-1: Retrieve group configurations at group management client

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 at group management client

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.

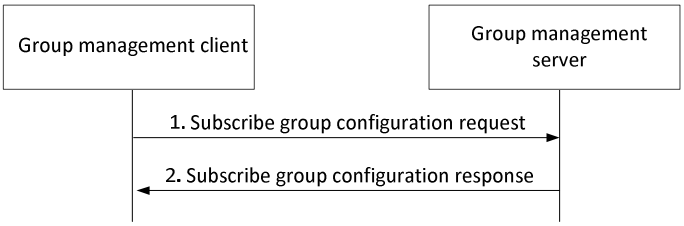

Figure 10.1.5.3-1: Subscription for group configurations at group management client

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.

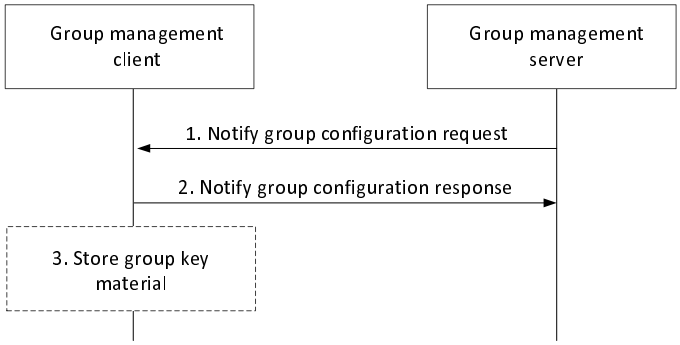

Figure 10.1.5.3-2: Notification of group configurations to group management client

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.

10.1.5.3a Subscription and notification for group policy at MC service server

The procedure for subscription for group configuration data as described in figure 10.1.5.3a-1 is used by the MC service server 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.

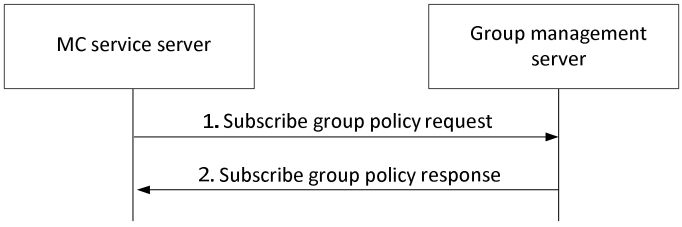

Figure 10.1.5.3a-1: Subscription for group policy at MC service server

1. The MC service server subscribes to the group policy from the group configuration stored at the group management server using the subscribe group policy request.

2. The group management server provides a subscribe group policy response to the MC service server indicating success or failure of the request.

The procedure for notification of group policy as described in figure 10.1.5.3a-2 is used by the group management server to inform the MC service server that new group policy is available.

Pre-conditions:

- The MC service server has subscribed to the group policy information from group management server.

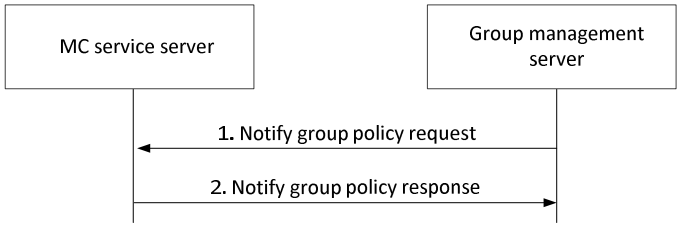

Figure 10.1.5.3a-2: Notification of group policy to MC service server

1. The group management server provides the notification to the MC service server, who previously subscribed for the group policy from the group configuration.

2. The MC service server provides a notify group policy response to the group management server.

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

10.1.5.5.1 Dynamic data associated with a group in MC service server

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 10.1.5.5.1-1: 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.
Regroup status of group where regrouping using a preconfigured group is used, e.g. whether group is regrouped, MC service group identity of regroup group.
Functional alias binding information for each user within the group.

10.1.5.5.2 Dynamic data associated with a group in group management server

The group management server may require (e.g., for regrouping) subscribe to a subset of dynamic data including affiliation status, regroup status and emergency status in the MC service server listed in table 10.1.5.5.1-1.

The affiliation status in the form of a list of MC service IDs of affiliated group members corresponding to the MC service for that group is available in group management server. The group management server can subscribe to this information from the MC service server in Table 10.1.5.5.1-1. Table 10.1.5.5.2-1 describes the affiliation status contained in the group management server.

Table 10.1.5.5.2-1: Affiliation status in group management server

Parameter description
MC service group ID
List of affiliated group members
> MCPTT
>> MCPTT ID
> MCVideo
>> MCVideo ID
> MCData
>> MCData ID

NOTE: The support for affiliation status in the group management server of an MC service user logged into multiple UEs is out of scope of the present document.

The regroup status of a group in the form of a list of MC service group IDs of the group being regrouped is available in group management server. The group management server can subscribe to this information from the MC service server in Table 10.1.5.5.1-1. Table 10.1.5.5.2-2 describes the regroup status contained in the group management server.

Table 10.1.5.5.2-2: Regroup status in group management server

Parameter description
List of MC service groups being regrouped into a new group
> MC service group ID (Constituent MC service group)
> Corresponding regrouped group information
>> MC service group ID

The emergency status of a group in the form of a list of MC service group IDs of the group in emergency state is available in group management server. The group management server can subscribe to this information from the MC service server in Table 10.1.5.5.1-1. Table 10.1.5.5.2-3 describes the emergency status contained in the group management server.

Table 10.1.5.5.2-3: Emergency status in group management server

Parameter description
List of MC service groups in emergency state
> MC service group ID

10.1.5.6 Subscription and notification for dynamic data associated with a group

10.1.5.6.0 General

An authorized user can request the current dynamic data for an MC service group on request. The dynamic data is described in subclause 10.1.5.5.1.

The group management server can subscribe for affiliation status, regroup status and emergency status associated with a group at the MC service server. The affiliation status, regroup status and emergency status in the group management server is described in subclause 10.1.5.5.2.

10.1.5.6.1 Information flows for subscription and notification for dynamic data associated with a group

10.1.5.6.1.1 Subscribe group dynamic data request

Table 10.1.5.6.1.1-1 describes the information flow subscribe group dynamic data request from the MC service client to the MC service server and from the group management server to the MC service server.

Table 10.1.5.6.1-1: Subscribe group dynamic data request

Information element	Status	Description
MC service group ID	M	The MC service group ID for which dynamic data is requested.
List of group dynamic data type (see NOTE)	O	The type of group dynamic data requested, e.g., affiliated status, regroup status, emergency status
NOTE: If the Group dynamic data type IE is not present, all types of group dynamic data is requested. This IE shall be present from when the request is sent from the group management sever.		

10.1.5.6.1.2 Subscribe group dynamic data response

Table 10.1.5.6.1.2-1 describes the information flow subscribe group dynamic data response from the MC service server to the MC service client and from the MC service server to the group management server. This information flow from the MC service server to the MC service client is sent individually addressed on unicast or multicast.

Table 10.1.5.6.1.2-1: Subscribe group dynamic data response

Information element	Status	Description
MC service group ID	M	The MC service group ID for which dynamic data is requested.
Status	M	Success or failure of the request

10.1.5.6.1.3 Notify group dynamic data request

Table 10.1.5.6.1.3-1 describes the information flow notify group dynamic data response from the MC service server to the MC service client and from the MC service server to the group management server. This information flow from the MC service server to the MC service client may be sent individually addressed or group addressed on unicast or multicast (see subclause 10.7.3.4.1).

Table 10.1.5.6.1.3-1: Notify group dynamic data request

Information element	Status	Description
MC service group ID	M	The MC service group ID for which dynamic data is requested.
Group dynamic data	M	Dynamic data associated with the group as per the requested group dynamic data type(s)

10.1.5.6.1.4 Notify group dynamic data response

Table 10.1.5.6.1.4-1 describes the information flow notify group dynamic data response from the MC service client to the MC service server and from the group management server to the MC service server.

Table 10.1.5.6.1.4-1: Notify group dynamic data response

Information element	Status	Description
MC service group ID	M	The MC service group ID for which dynamic data was received

10.1.5.6.2 Procedure for subscription and notification for dynamic data associated with a group by the MC service client

The procedure for subscription for dynamic data associated with an MC service group is described in figure 10.1.5.6.2-1 and is used by the MC service client of the authorized user to obtain the dynamic data from the MC service server.

Pre-conditions:

- The MC service server holds dynamic data associated with the MC service group.
- The MC service client is authorized to request the dynamic data associated with the MC service group.

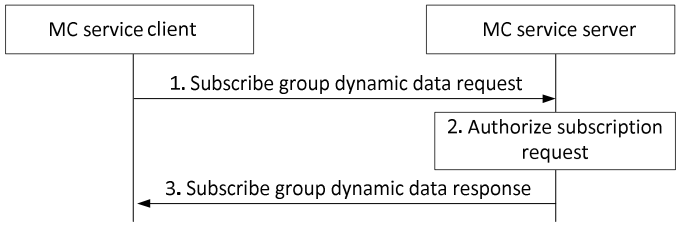

Figure 10.1.5.6.2-1: Subscription for group dynamic data

1. The MC service client subscribes to the group dynamic data stored in the MC service server using the subscribe group dynamic data request.
2. The MC service server checks that the MC service client is authorized to receive dynamic data associated with the MC service group.
3. The MC service server provides a subscribe group dynamic data response to the MC service client indicating success or failure of the request.

The procedure for notification of group dynamic data as shown in figure 10.1.5.6.2-2 is used by the MC service server to inform the MC service client about new group dynamic data.

Pre-conditions:

- The MC service client has subscribed to the group dynamic data
- The MC service server has new group dynamic data available.

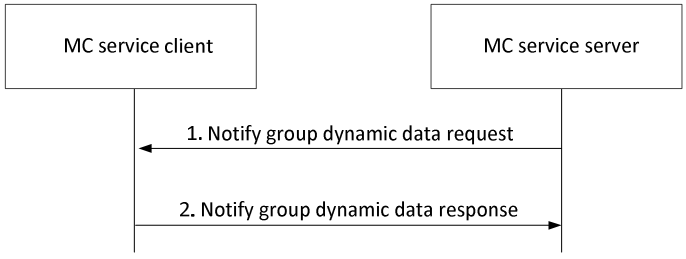

Figure 10.1.5.6.2-2: Notification of group dynamic data

1. The MC service server provides the notification to the MC service client, who previously subscribed for the group dynamic data.

2. The MC service client provides a notify group dynamic data response to the MC service server.

10.1.5.6.3 Procedure for subscription and notification for dynamic data associated with a group by the group management server

The procedure for subscription for affiliation status regroup status and emergency status associated with an MC service group by the group management server is described in figure 10.1.5.6.3-1 and is used by the group management server to obtain the affiliation status (implicit and explicit), regroup status and emergency status from the MC service server.

Pre-conditions:

- The MC service server is the MC service server within the MC system where the group is defined.

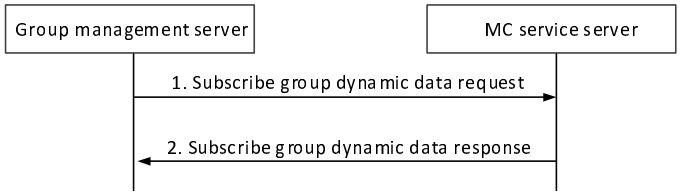

Figure 10.1.5.6.3-1: Subscription for dynamic data associated with a group

1. The group management server subscribes to the dynamic data associated with a group stored in the MC service server using the subscribe group dynamic data request.

2. The MC service server provides a subscribe group dynamic data response to the group management server indicating success or failure of the request by specifying the list of group dynamic data type. The group dynamic data type indicates the group affiliation status, regroup status or emergency status to be subscribed.

The procedure for notification of group affiliation status, regroup status or emergency status as shown in figure 10.1.5.6.3-2 is used by the MC service server to inform the group management server about the updates to the group affiliation status, regroup status or emergency status.

Pre-conditions:

- The group management server has subscribed to the affiliation status, regroup status or emergency status in the MC service server.

- The affiliation status, regroup status or emergency status associated with a group subscribed to by the group management server has been updated at the MC service server.

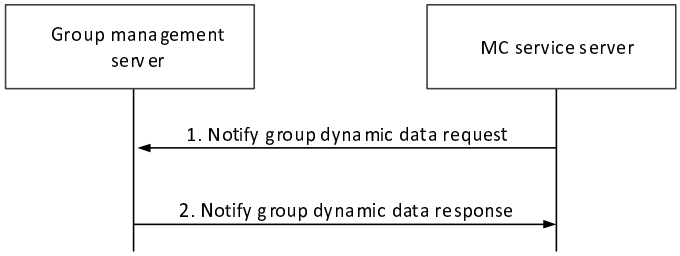

Figure 10.1.5.6.3-2: Notification of dynamic data associated with a group

1. The MC service server provides either or all of the affiliation status, regroup status and emergency status via a notification to the group management server based on the list of group dynamic data type which has subscribed.

2. The group management server provides a notify group dynamic data response to the MC service server.

10.1.6 MC service UE migration

10.1.6.1 MC service UE obtains migration connectivity information of partner MC system

Connectivity information for the partner MC system, including MC system identification and access information, is contained in the on-network user profiles for MCPTT in 3GPP TS 23.379 [16], for MCVideo in 3GPP TS 23.281 [12] and for MCData in 3GPP TS 23.282 [13].

10.1.6.2 Void

10.1.7 Functional alias configuration management

10.1.7.1 Retrieve functional alias configurations from the functional alias management server

The procedure for retrieve functional alias configurations from the functional alias management server is described in figure 10.1.7.1-1. This procedure can be used following service authorisation when the configuration management client has received the list of functional aliases and the functional alias management client needs to obtain the functional alias configurations, or following a notification from the functional alias management server that new functional alias configuration information or functional alias configuration update is available. This procedure can be also used by the MC service server under authorization to obtain the functional alias configurations (e.g. upon functional alias activation or call processing).

Pre-conditions:

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

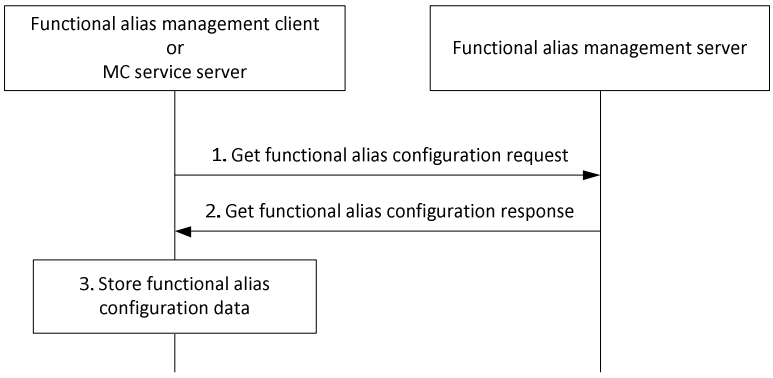

Figure 10.1.7.1-1: Retrieve functional alias configurations from the functional alias management server

1. The functional alias management client or the MC service server requests the functional alias configuration data.
2. The functional alias management server provides the functional alias configuration data to the client or MC service server.
3. The functional alias management client or MC service server stores the functional alias configuration information.

10.1.7.2 Subscription and notification for functional alias configuration data

The procedure for subscription for functional alias configuration data as described in figure 10.1.7.2-1 is used by the functional alias management client to indicate to the functional alias management server that it wishes to receive

updates of functional alias configuration data for functional aliases for which it is authorized. This procedure can be also used by the MC service server under authorization to obtain the functional alias configurations and the updates (e.g. upon functional alias activation or call processing).

Pre-conditions:

- The functional alias management server has some functional alias configurations stored.

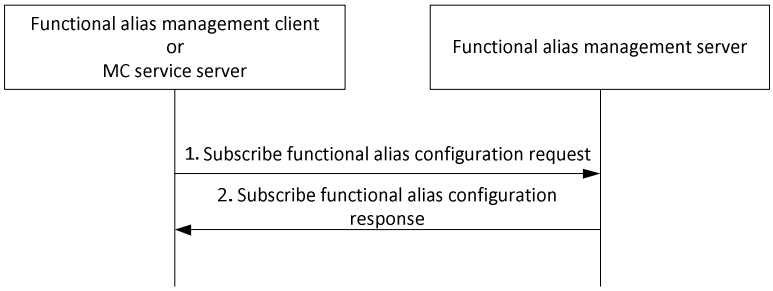

Figure 10.1.7.2-1: Subscription for functional alias configurations

1. The functional alias management client or MC service server subscribes to the functional alias configuration information stored at the functional alias management server using the subscribe functional alias configuration request.
2. The functional alias management server provides a subscribe functional alias configuration response to the functional alias management client or MC service server indicating success or failure of the request.

The procedure for notification of functional alias configuration data as described in figure 10.1.7.2-1 is used by the functional alias management server to inform the functional alias management client or MC service server that new functional alias configuration data is available.

Pre-conditions:

- The functional alias management client has subscribed to the functional alias configuration information
- The functional alias management server has received and stored new functional alias configuration information.

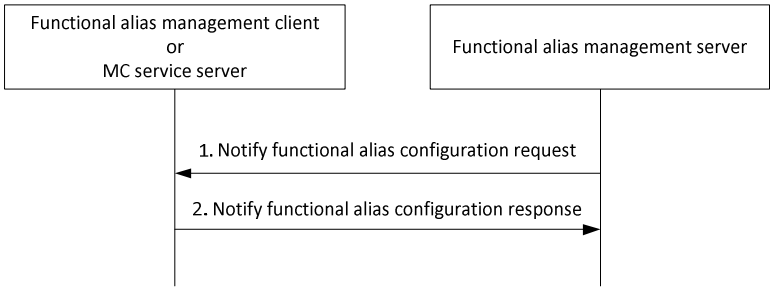

Figure 10.1.7.2-2: Notification of functional alias configurations

1. The functional alias management server provides the notification to the functional alias management client or MC service server, who previously subscribed for the functional alias configuration information.
2. The functional alias management client or MC service server provides a notify functional alias configuration response to the functional alias management server.

If the functional alias management server has notified the functional alias management client about new functional alias configuration information through this procedure, the functional alias management client may then follow the procedure described in subclause 10.1.7.1 in order to retrieve that functional alias configuration information.

10.1.7.3 Dynamic data associated with a functional alias

10.1.7.3.1 Dynamic data associated with a functional alias in MC service server

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

Table 10.1.7.3-1: Dynamic data associated with a functional alias

Parameter description
Activation status of each functional alias and the corresponding MC service ID of the user who activated that functional alias (subscription and notification procedures for functional alias are defined in clause 10.13.10)

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 (see NOTE 1)
MC service list (see NOTE 2)	O	List of MC services whose service communications are to be enabled on the group.
Proposed MC service group ID	O	MC service group ID proposed for the requested group
MC service group configuration data	O	Configuration data for the requested group (see NOTE 3)
NOTE 1: The MC service ID list can be an empty list. NOTE 2: This information element shall be included in the message for creating a group configured for multiple MC services. NOTE 3: If the MC service group configuration data is not present it can be provided later using the "Store group configuration request" (see subclause 10.1.2.1).		

10.2.2.2 Group creation response

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

Table 10.2.2.2-1: Group creation response

Information element	Status	Description
MC service group ID	M (see NOTE)	MC service group ID of the group
Result	M	Indicates success or reason for failure
NOTE: If the Result information element indicates failure then the value of MC service group ID information element has no meaning.		

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

Table 10.2.2.3-1 describes the information flow for the 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 1)	O	Required security level for the temporary group
Priority level	O	Required priority level for the temporary group
MC service list (see NOTE 2)	O	A subset of the common MC service(s) to be applied for the regrouped group
Broadcast regroup	O	Indicates that only an authorized MC service user can transmit on this temporary group.
NOTE 1: Security level refers to the configuration of media and floor control protection parameters as listed in Annex A.4, table A.4-1 NOTE 2: If this information element is not present, all the MC service(s) that are common to the groups being regrouped will be applicable for the regrouped group.		

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

Table 10.2.2.4-1 describes the information flow for the 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 (see NOTE)	MC service group ID of the temporary group
MC service list	O	List of MC services whose service communications are to be enabled on this 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
MC service list	O	List of MC services whose service communications are to be enabled on this temporary group.
Broadcast regroup	O	Indicates that only an authorized MC service user can transmit on this 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 and from the group management server to the group management client.

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 and from the group management client to the group management server.

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 and from the group management server to the group management client.

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
Broadcast regroup	O	Indicates that only an authorized MC service user can transmit on this 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 and from the group management client to the group management server.

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
Broadcast regroup	O	Indicates that only an authorized MC service user can transmit on this 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 flow 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

10.2.2.21 Group deletion request

Table 10.2.2.21-1 describes the information flow group deletion request from the group management client to the group management server.

Table 10.2.2.21-1: Group deletion request

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

10.2.2.22 Group deletion response

Table 10.2.2.22-1 describes the information flow group deletion response from the group management server to the group management client.

Table 10.2.2.22-1: Group deletion response

Information element	Status	Description
MC service group ID	M	Identity of the MC service group requested deleted
Result	M	Indicates success (group no longer exists), or failure (group deletion did not occur, eg. authorization failure).

10.2.2.23 Group deletion notification

Table 10.2.2.23-1 describes the information flow group deletion notification from the group management server to the MC service server, and from the group management server to the group management clients for MC service users which are members of the group.

Table 10.2.2.23-1: Group deletion notification

Information element	Status	Description
MC service group ID	M	MC service group ID has been deleted.

10.2.2.24 Group information provision request

Table 10.2.2.24-1 describes the information flow group information provision request from the group management server in the primary MC system of the MC service group to the group management server in the partner MC system of the MC service group.

Table 10.2.2.24-1: Group information provision request

Information element	Status	Description
MC service group ID	M	MC service group ID of the group
MC service group configuration information	M	Configuration information for the MC service group

10.2.2.25 Group information provision response

Table 10.2.2.25-1 describes the information flow group information provision response from the group management server in the partner MC system of the MC service group to the group management server in the primary MC system of the MC service group.

Table 10.2.2.25-1: Group information provision response

Information element	Status	Description
MC service group ID	M	MC service group ID of the group
Result	M	Indicates success or failure of reception, modification and storage of MC service group configuration information

10.2.2.26 Group information request

Table 10.2.2.26-1 describes the information flow group information request from the group management server in the partner MC system of the MC service group to the group management server in the primary MC system of the MC service group.

Table 10.2.2.26-1: Group information request

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

10.2.2.27 Group information response

Table 10.2.2.27-1 describes the information flow group information response from the group management server in the primary MC system of the MC service group to the group management server in the partner MC system of the MC service group.

Table 10.2.2.27-1: Group information response

Information element	Status	Description
MC service group ID	M	MC service group ID of the group
MC service group configuration information	O (see NOTE 1)	Configuration information for the MC service group
Failure reason	O (see NOTE 2)	Indicates reason for failure to provide MC service group configuration information
NOTE 1: Shall be present if the request can be fulfilled by the group management server in the primary MC system of the MC service group. NOTE 2: Shall be present if the request cannot be fulfilled by the group management server in the primary MC system of the MC service group.		

10.2.2.28 Group information subscribe request

Table 10.2.2.28-1 describes the information flow group information subscribe request from the group management server in the partner MC system of the MC service group to the group management server in the primary MC system of the MC service group.

Table 10.2.2.28-1: Group information subscribe request

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

10.2.2.29 Group information subscribe response

Table 10.2.2.29-1 describes the information flow group information subscribe response from the group management server in the primary MC system of the MC service group to the group management server in the partner MC system of the MC service group.

Table 10.2.2.29-1: Group information subscribe response

Information element	Status	Description
MC service group ID	M	MC service group ID of the group
Result	M	Inidicates success or failure of the subscribe request

10.2.2.30 Group information notify request

Table 10.2.2.30-1 describes the information flow group information notify request from the group management server in the primary MC system of the MC service group to the group management server in the partner MC system of the MC service group.

Table 10.2.2.30-1: Group information notify request

Information element	Status	Description
MC service group ID	M	MC service group ID of the group
MC service group configuration information	M	Configuration information for the MC service group

10.2.2.31 Group information notify response

Table 10.2.2.31-1 describes the information flow group information notify response from the group management server in the partner MC system of the MC service group to the group management server in the primary MC system of the MC service group.

Table 10.2.2.31-1: Group information notify response

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

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.

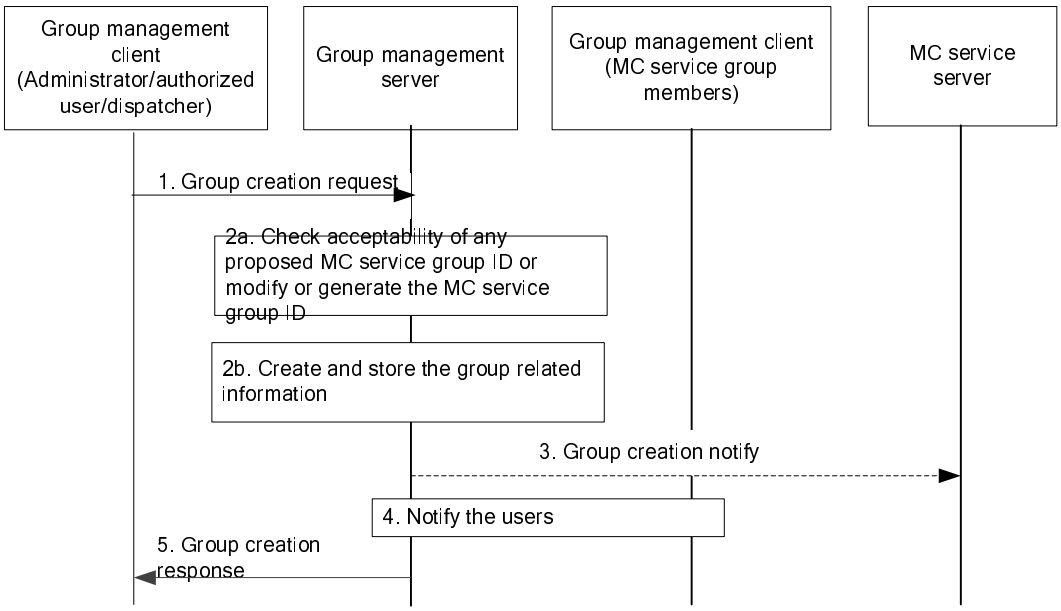

Figure 10.2.3-1: Group creation

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.

NOTE 1: The administrator/dispatcher/authorized MC service user can include a proposed MC service group ID in the group creation request. The proposed MC service group ID can be derived from a set of rules previously agreed between the administrator/dispatcher/authorized MC service user and the group management server. The method by which the the administrator/dispatcher/authorized MC service user obtains the set of rules is outside the scope of the present document.

NOTE 2: The administrator/dispatcher/authorized MC service user can include configuration data for the requested group. The method by which the administrator/dispatcher/authorized MC service user prepares the configuration data for the requested group is outside the scope of the present document, but it could, for example, be derived from pre-prepared templates available to the administrator/dispatcher/authorized MC service user.

2a. If the proposed MC service group ID information element is not present in the group creation request, the group management server generates the MC service group ID. If the proposed MC service group ID information element is present and acceptable to the group management server, the group management server uses the proposed MC service group ID for the new group. If the proposed MC service group ID information element is present but not acceptable to the group management server, the group management server modifies proposed MC service group ID or generates the MC service group ID or rejects the group creation request.

2b. During the group creation, the group management server stores or 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 (if any). 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 (if any) 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 response to the group management client of the administrator/dispatcher/authorized MC service user. The result information element indicates:

- success (using proposed MC service group ID); or
- success (MC service group ID provided by the group management server); or
- failure (proposed MC service group ID not acceptable); or
- failure for other reason.

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.

The temporary group formation is applicable only for groups configured with at least one common MC service. The temporary group formation shall be rejected if any of the requested MC services are not common to all MC service groups in the list.

The temporary group created can be a broadcast group or a non-broadcast group. The broadcast regroup is used for one-way communication where only an authorized MCX user is allowed to transmit and all other regroup members are only allowed to receive the communication (e.g. a call from a dispatcher to all regroup members). The non-broadcast regroup is used for two-way communication where all regroup members can transmit and receive (i.e, the regroup group call behaves like a normal non-broadcast group call). The broadcast regroup satisfies the temporary group-broadcast group requirements defined in 3GPP TS 22.180 [2] and is an alternative to the "Temporary group – broadcast group call" procedure (10.6.2.5.3) defined in 3GPP TS 23.379 [16].

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 group management client has retrieved the group configurations of the groups to be regrouped.

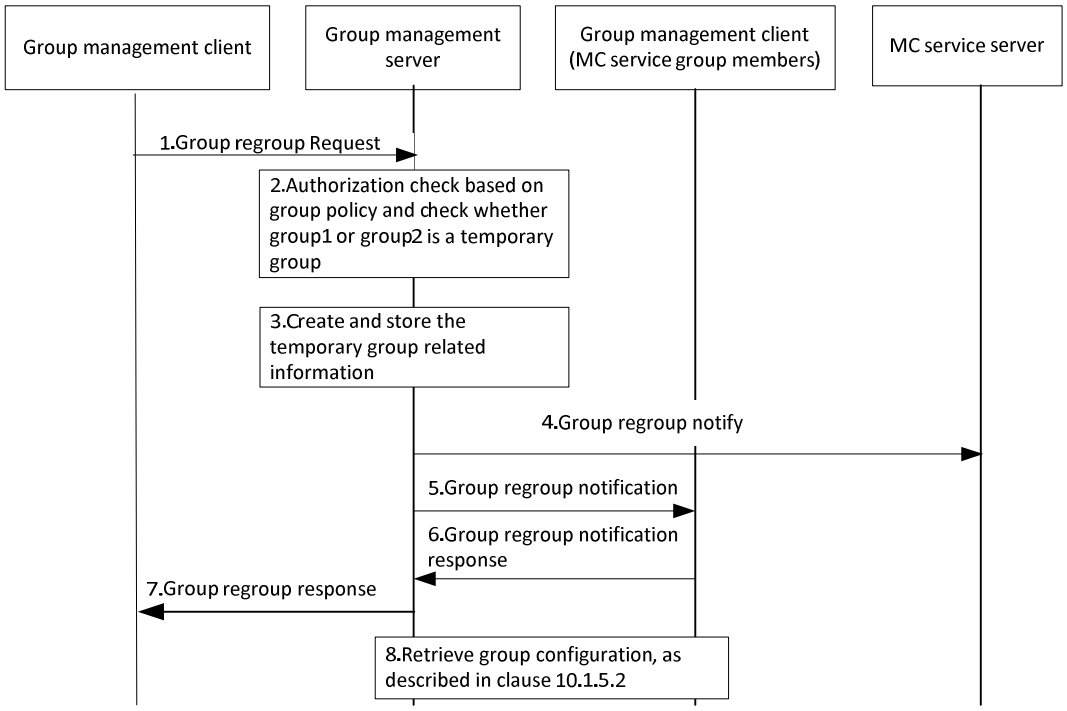

Figure 10.2.4.1-1: Group regroup for the groups within the same MC system

1. The group management client of the MC service user requests group regroup operation to the group management server, which is the group management server of one of the groups to be regrouped. 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. The group management client indicates whether the temporary group is a broadcast regroup.

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, the security level of the temporary group, and whether the temporary group is a broadcast regroup. 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. If MC service types of the groups being combined are not identical, group management server determines the overlapping part and stores the MC service list for the temporary group.

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. If MC service list is included, MC service server stores it and provides MC service types accordingly.

5. The group management server notifies the affiliated MC service group members of the constituent MC service groups by sending group regroup notification messages.

6. The affiliated MC service group members of the constituent MC service groups send individual group regroup notification response messages.

7. The group management server provides a group regroup response to the group management client of the authorized MC service user. If MC service list is included, group management client stores it and initiates MC service types accordingly.

8. The affiliated MC service group members of the constituent MC service groups individually request group configuration data from the group management server for the temporary group, as described in clause 10.1.5.2. The group configuration data includes security, priority, and other parameters.

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.

4. The group management client has retrieved the group configurations of the groups to be regrouped.

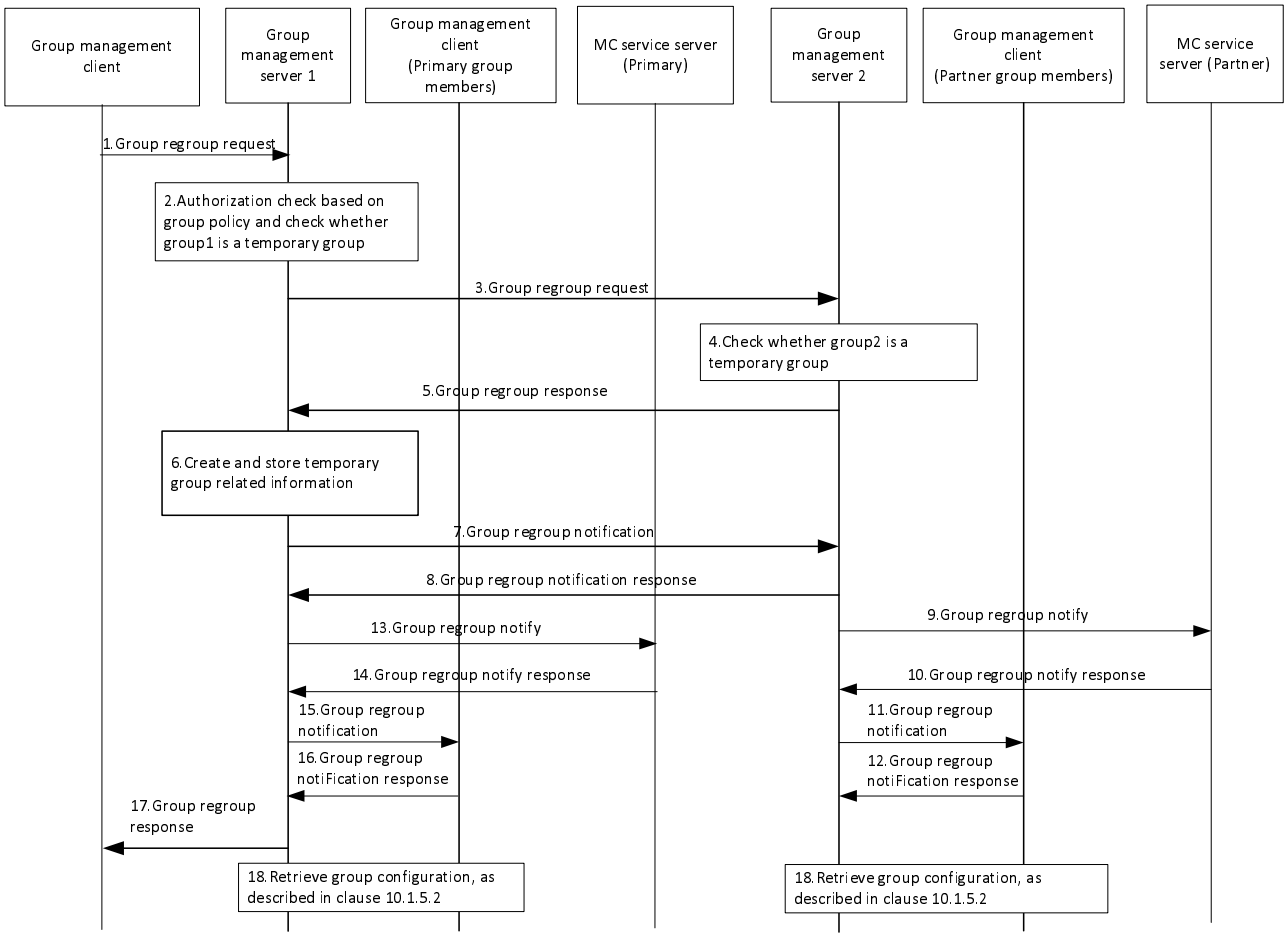

Figure 10.2.4.2-1: Temporary group formation - group regrouping involving multiple MC systems

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 one of the groups to be regrouped). 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. The group management client indicates whether the temporary group is a broadcast regroup.

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. Any regroup action that violates the rules specified in subclause 10.2.4.4 shall cause a negative response and the current procedure to proceed to step 15.

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, the security level of the temporary group, and whether the temporary group is a broadcast regroup. 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 affiliated MC service group members of the constituent MC service groups of the group management server 2 send individual group regroup notification responses to the group management server 2.

13. 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.

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

15. The group management server 1 notifies the affiliated MC service group members of the constituent MC service groups of the group management server 1 by sending group regroup notification messages.

16. The affiliated MC service group members of the constituent MC service groups of group management server 1 send individual group regroup notification responses to the group management server 1.

17. The group management server 1 provides a group regroup response to the group management client of the authorized MC service user (e.g. dispatcher).

18. The affiliated MC service group members of the constituent MC service groups of the group management servers individually request group configuration data from the group management servers for the temporary group, as described in clause 10.1.5.2. The group configuration data includes security, priority, and other parameters.

10.2.4.2a Temporary group tear down within an MC system

Figure 10.2.4.2a-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-condition:

- 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 10.2.4.1.

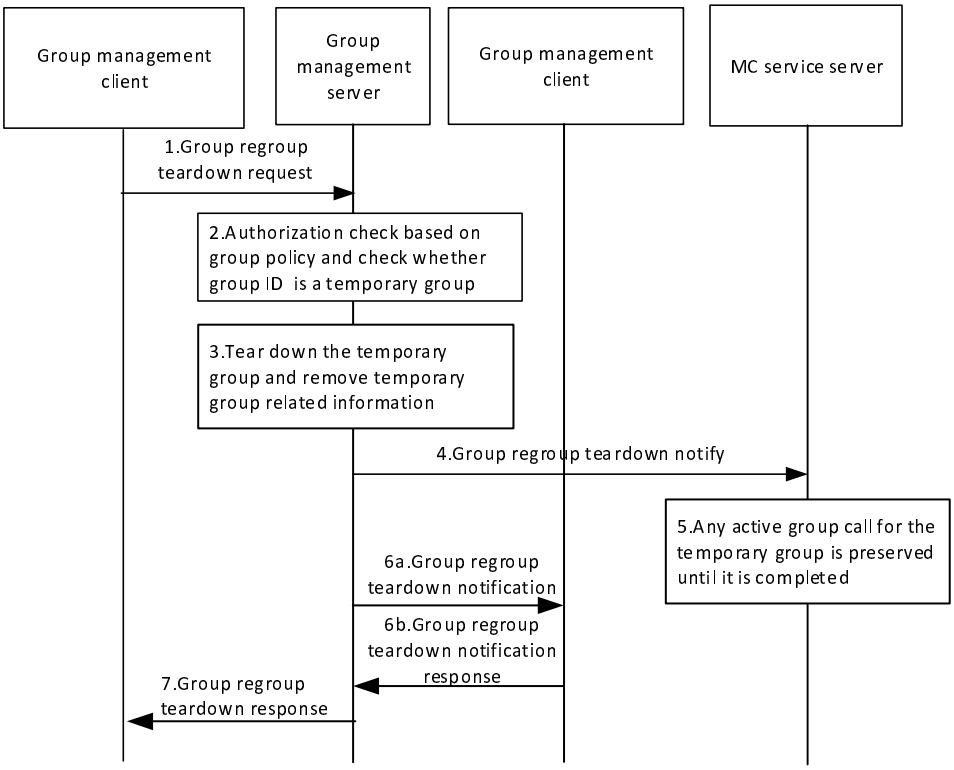

Figure 10.2.4.2a-1: Temporary group tear down within an MC system

1. The group management client of the MC service user requests group regroup teardown operation to the group management server (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 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. The group management server tears down the temporary group, i.e., remove the temporary group related information.

4. The group management server notifies the MC service server regarding the temporary group teardown.

5. Any active group call for the temporary group is preserved until it is completed.

6. The group management server notifies the affiliated MC service group members regarding the temporary group teardown by sending the group regroup teardown notification (6a) and receives a group regroup teardown notification response (6b) messages.

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

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.

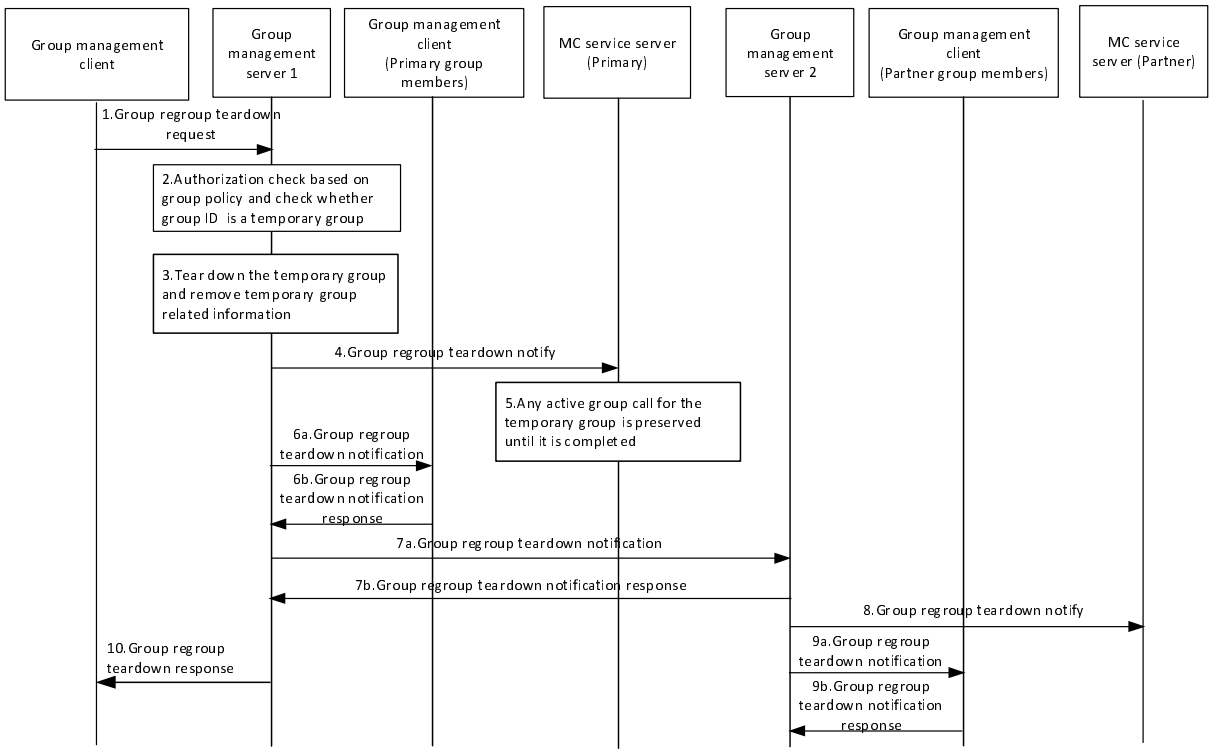

Figure 10.2.4.3-1: Temporary group tear down

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

4. The group management server 1 notifies the primary MC service server regarding the temporary group teardown.

5. Any active group call for the temporary group is preserved until it is completed.

6. The group management server 1 notifies the affiliated MC service group members regarding the temporary group teardown by sending the group regroup teardown notification (6a) and receives a group regroup teardown notification response (6b) messages.

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. The group management server 2 notifies the partner MC service server.

9. The group management server 2 notifies the affiliated MC service group members regarding the temporary group teardown by sending the group regroup teardown notification (9a) and receives a group regroup teardown notification response (9b) messages. Any active group call for the temporary group is preserved until it is completed.

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

10.2.4.4 Group regroup rules

To prevent routing issues and complexity related to group regrouping, the following rules shall be applied:

- Group regroup in either single MC system or multiple MC systems can take place if:
  - None of the groups to be regrouped are temporary groups; and
  - The groups to be regrouped are not already regrouped into another temporary group; and
  - If the policy of the MC system does not allow a temporary group to include groups that are currently in emergency state, then regrouping of groups can take place if none of the groups to be regrouped are in emergency state.
- If the policy of the MC system allows a temporary group to include groups from other MC systems, group regrouping containing groups with multiple MC systems can take place if:
  - the MC service server (controlling role) for the regrouped group is the MC service server (controlling role) for all MC service groups involved in the regrouping; or
  - the MC service server (controlling role) for the regrouped group is an MC service server (controlling role) for at least one of the MC service groups involved in the regrouping; or
  - the MC service server (controlling role) for the regrouped group is an MC service server homed by at least one of the MC service groups and the MC system of any involved MC service group allows floor control for the set of regrouped groups to be deferred to the MC service server (controlling role) of the temporary group.
- If the policy of the MC system does not allow a temporary group to include groups from other MC systems, regrouping of groups with members spanning multiple MC systems can take place if:
  - the MC service server (controlling role) for the regrouped group is the MC service server (controlling role) for all MC service groups involved in the regrouping; or

- the MC service server (controlling role) for the regrouped group is an MC service server (controlling role) for at least one of the MC service groups involved in the regrouping, and the MC service servers with the controlling roles for all of the groups that are regrouped are within the same MC system.

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.

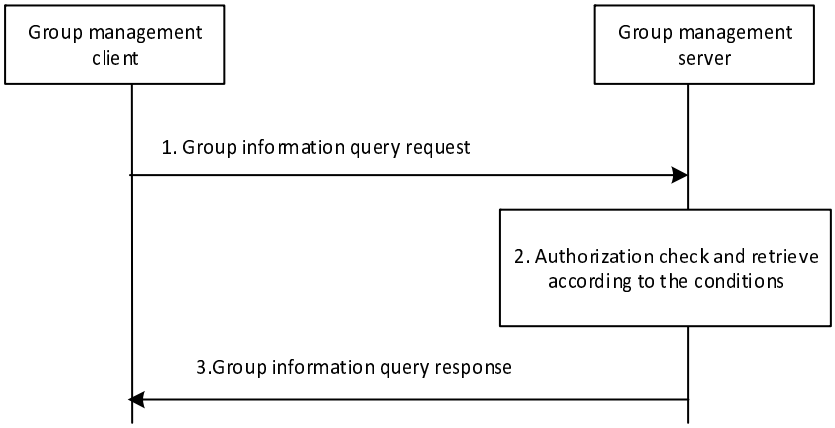

Figure 10.2.5.2-1: membership or affiliation list query

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 retrieves 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.

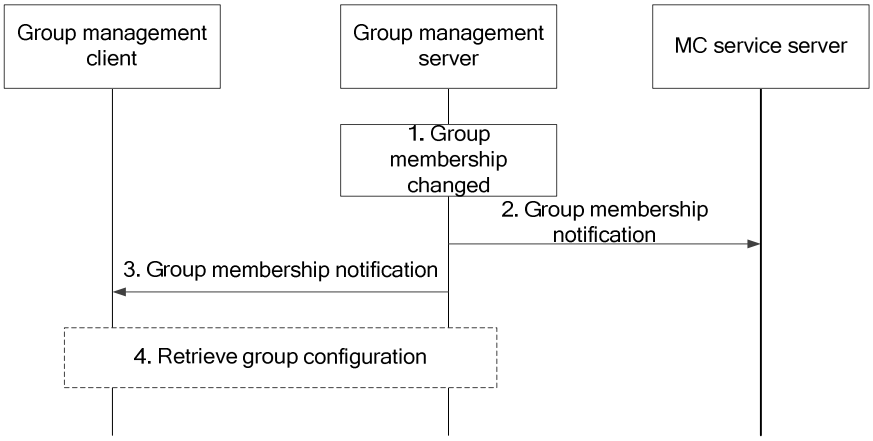

Figure 10.2.6.1-1: group membership notification

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 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.

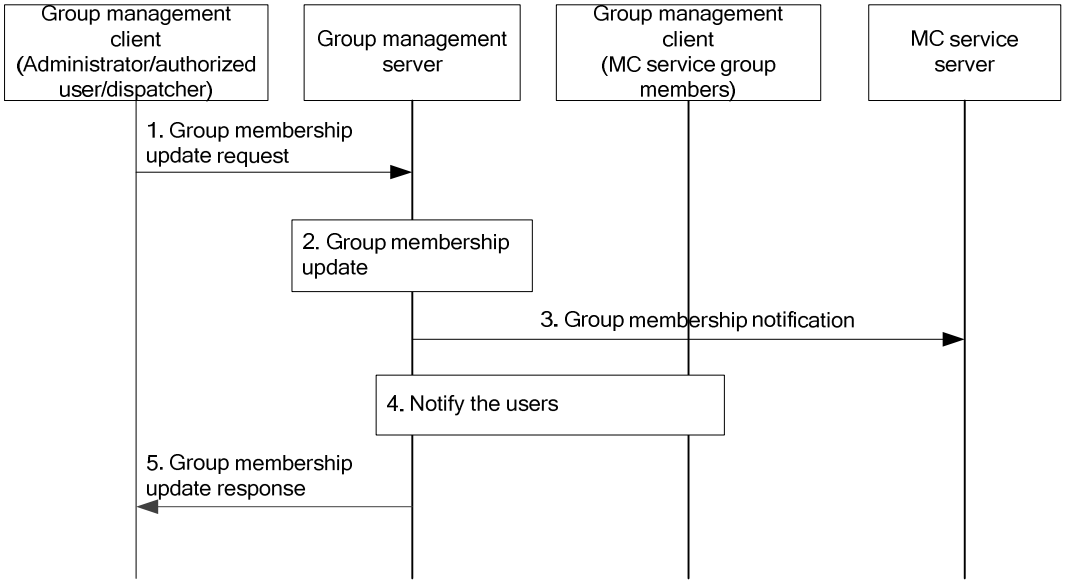

Figure 10.2.6.2-1: Group membership update by authorized user

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.

10.2.7 Group configuration for interconnection

10.2.7.1 Overview

The procedures in the following subclauses describe the process for sharing group configuration from a primary MC system of the MC service group to an interconnected partner MC system of the MC service group where MC service clients receiving MC service in the partner MC system of the MC service group need to make use of the MC service group.

The group management server in the primary MC system of the MC service group provides group configuration information to the group management server in the partner MC system of the MC service group. The group management server in the primary MC system of the MC service group may modify the configuration before providing it to that partner MC system in accordance with policies and requirements within the primary MC system (for example the list of members of the group within the primary MC system or within other partner MC systems might not be exposed to that partner system). The means by which the group management server in the primary system determines which configuration parameters are changed is outside the scope of the present document.

The group management server in the partner MC system of the MC service group may modify the configuration before storing it in accordance with policies and requirements within that MC system (for example the priority of the group within that partner MC system, or permitted locations for service within that partner MC system). The group management server in the partner MC system of the MC service group will be the source of group configuration information to the group management clients of any MC service user who is receiving MC service in the partner MC system of the MC service group and who is defined as a member of the MC service group. The list of groups in the user profile for those group members in the partner MC system of the MC service group will contain the address of this

group management server in the partner MC system of the MC service group as the address of the server from which to obtain the MC service group configuration for this MC service group.

The procedures in the following subclauses describe the cases where the provision of configuration information is initiated by the group management server in the primary MC system of the MC service group, and where the configuration is requested by the group management server in the partner MC system of the MC service group. There may be additional proxy servers in between the two group management servers on the edges of one or both MC systems so that each group management server is not aware of the network topology of the other MC system. These additional proxy servers are not shown in these procedures.

10.2.7.2 Primary MC system provides group configuration to the partner MC system

Figure 10.2.7.2-1 below illustrates the case where the primary MC system of the MC service group provides the group configuration to the partner MC system of the MC service group, e.g. due to an action by an administrator or because the primary MC system of some of the MC service group members is the partner MC system of the MC service group.

Preconditions

- The MC service group is defined in its primary MC system.
- One or more MC service group members are defined in the partner MC system.
- The primary MC system of the MC service group has been configured with addressing information for the group management server in the partner MC system of the MC service group.
- The primary MC system of the MC service group is authorized to provide group configuration information to the partner MC system of the MC service group.

NOTE 1: The primary MC system of the MC service group could be configured with an address of the group management server within the partner MC system of the MC service group which is a proxy address, and routing within the partner MC system of the MC service group determines which actual group management server is the correct server to receive the configuration information.

NOTE 2: The group management server within the partner MC system of the MC service group is responsible for providing MC service group configuration information to MC service group members for whom the partner MC system of the MC service group is their serving MC system.

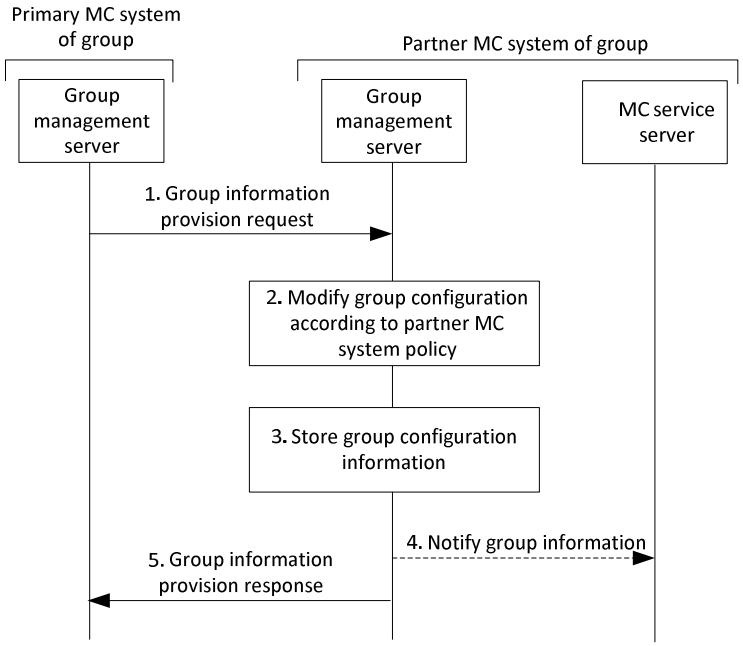

Figure 10.2.7.2-1: Primary MC system provides group configuration to partner MC system

1. The group management server in the primary MC system of the MC service group provides the configuration information related to the MC service group to the group management server in the partner MC system of the MC service group.

NOTE 3: The group management server in the primary MC system can modify the group configuration information in accordance with local policies and local requirements before it is provided to the partner MC system. Such modification is outside the scope of the present document.

2. The group management server in the partner MC system of the MC service group modifies the group configuration information received from the primary MC system of the MC service group according to the partner MC system's policies and local configuration information.

3. The group management server in the partner MC system of the MC service group stores the modified group configuration.

4. The group management server in the partner MC system may notify the MC service server(s) in the partner MC system of the MC service group of the MC service group configuration.

5. The group management server of the partner MC system of the MC service group responds to the group management server of the primary MC system of the MC service group that the configuration has been received and stored correctly.

10.2.7.3 Partner MC system requests group configuration from the primary MC system

Figure 10.2.7.3-1 below illustrates the case where the partner MC system of the MC service group requests the group configuration from the primary MC system of the MC service group, for example because an MC service user receiving service in the partner MC system of the MC service group has the group configured in the user profile.

Preconditions

- The MC service group is defined in its primary MC system.

- The MC service group is configured in the MC service user profiles of one or more MC service users in the partner MC system of the MC service group.

- At least one of the MC service users in the partner MC system of the MC service group that is listed as an MC service group member of the MC service group has become MC service authorized with the MC service server in the partner MC system of the MC service group.

- The group management server in the partner MC system of the MC service group does not have the configuration for the MC service group stored.

- The partner MC system of the MC service group has been configured with addressing information for the group management server in the primary MC system of the MC service group.

- The partner MC system of the MC service group is authorized to request group configuration information from the primary MC system of the group.

NOTE 1: The partner MC system of the MC service group could be configured with an address of the group management server within the primary MC system of the MC service group which is a proxy address, and routing within the primary MC system of the MC service group determines which actual group management server is the correct server to provide the configuration information.

NOTE 2: The group management server within the partner MC system of the MC service group is responsible for providing group configuration information to MC service group members for whom the partner MC system of the MC service group is their serving MC system.

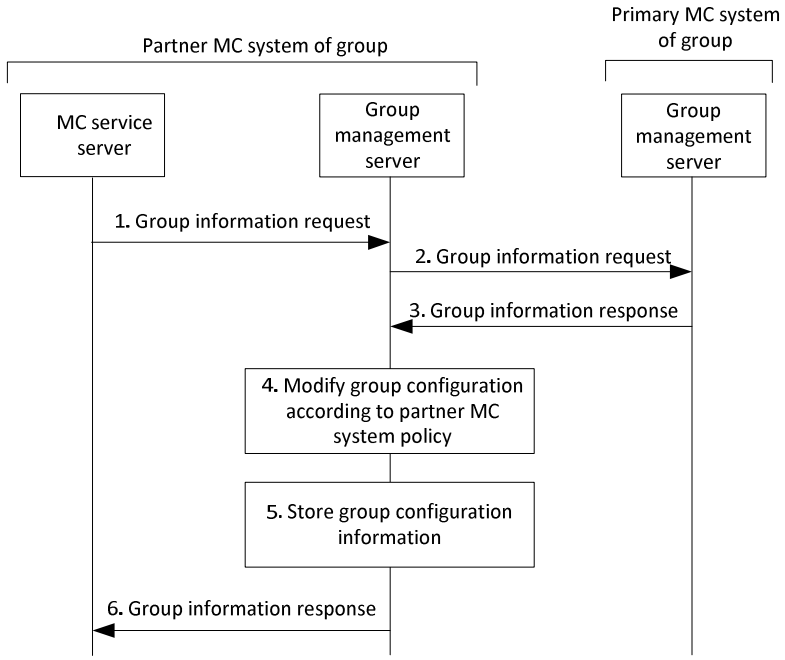

Figure 10.2.7.3-1: Partner MC system requests group configuration from primary MC system

1. The MC service server in the partner MC system of the MC service group requests the group configuration information from the group management server in the partner MC system of the MC service group.
2. The group management server in the partner MC system of the MC service group requests the group configuration from the group management server in the primary MC system of the MC service group.
3. The group management server in the primary MC system of the MC service group provides the requested group configuration information.

NOTE 3: The group management server in the primary MC system can modify the group configuration information in accordance with local policies and local requirements before it is provided to the partner MC system. Such modification is outside the scope of the present document.

4. The group management server in the partner MC system of the MC service group modifies the group configuration information received from the primary MC system of the MC service group according to the partner MC system's policies and local configuration information.
5. The group management server in the partner MC system of the MC service group stores the modified group configuration.
6. The group management server in the partner MC system notifies the MC service server(s) in the partner MC system of the MC service group of the MC service group configuration.

10.2.7.4 Partner MC system subscribes to group configuration

The procedure for subscription from the group management server in the partner system for group configuration information to the group management server in the primary MC system of the MC service group is shown in figure 10.2.7.4-1.

Pre-conditions:

- The MC service group is defined in its primary MC system.
- One or more MC service group members are defined in the partner MC system.
- The GMS in the partner MC system of the MC service group has received group configuration information from the GMS in the primary MC system of the MC service group.

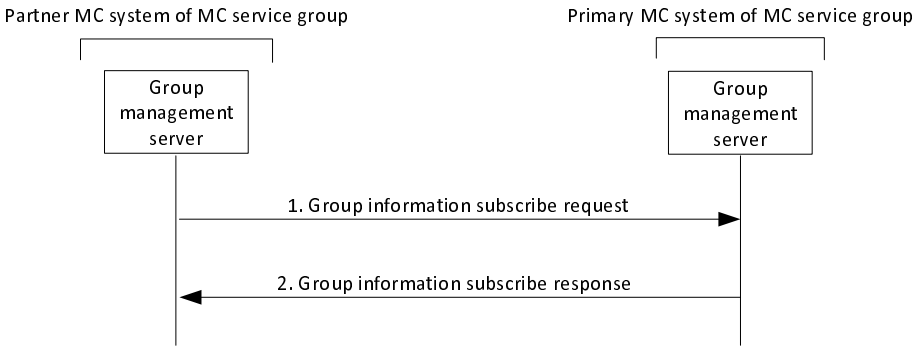

Figure 10.2.7.4-1: Subscription from partner MC system to primary MC system for MC service group configuration

1. The group management server in the partner MC system of the MC service group subscribes to the group configuration information stored in the group management server in the primary MC system of the MC service group.

2. The group management server in the primary MC system of the MC service group provides a group information subscribe response to the group management server in the partner MC system of the MC service group indicating success or failure of the request.

10.2.7.5 Primary MC system notifies group configuration

The procedure for notification of group configuration information from the group management server in the primary MC system of the MC service group to the group management server in the partner MC system of the MC service group is shown in figure 10.2.7.5-1.

Pre-conditions:

- The group management server in the partner MC system of the MC service group has subscribed to the group configuration information for the MC service group in the group management server in the primary MC system of the MC service group.

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

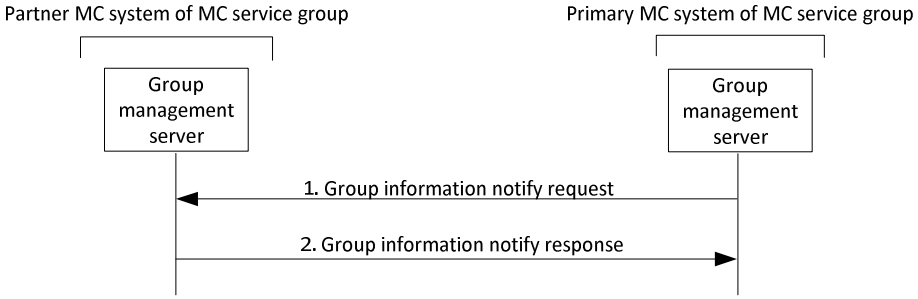

Figure 10.2.7.5-1: Notification of group configuration information to partner MC system of MC service group

1. The group management server in the primary MC system of the MC service group provides the notification to the group management server in the partner MC system of the MC service group, Optionally, the notify group configuration request may contain group related key material for the group management client.

2. The group management server in the partner MC system of the MC service group provides a notify group information notify response to the group management server in the primary MC system of the MC service group indicating the success or failure of the notification.

Following completion of the notification procedure, the group management server in the partner MC system of the MC service group stores the group configuration information and any key material provided.

10.2.8 Group deletion

Figure 10.2.8-1 below illustrates the group deletion procedure by an authorized MC service user/ MC service administrator to delete a group in the primary MC system. Any actions taken by the group management clients on the UE after receiving the group deletion notification are outside the scope of this procedure.

Pre-conditions:

1. The group management clients, the group management server, and the MC service server belong to the same MC system.
2. The group management client (originator) is for an authorized user with authorization to perform the group deletion.

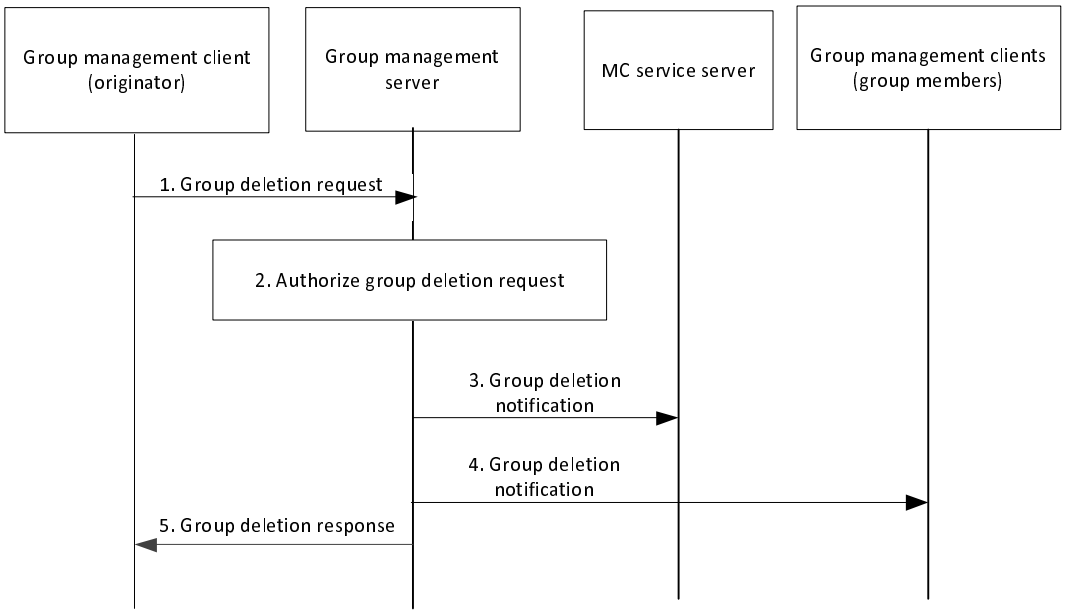

Figure 10.2.8-1: Group deletion

1. The group management client (originator) of an authorized MC service user sends a group deletion request to the group management server.2. The group management server checks whether the MC service user is authorized to perform the group deletion operation. For an authorized MC service user, the group management server will proceed to delete the group and move to step 3. If the MC service user is not authorized, then the group management server will not delete the group and move to step 5 sending a group deletion response failure.
3. The group management server sends a group deletion notification to the MC service server of the group as well as any MC service servers subscribed to the group. When a group is configured for multiple MC services, the group deletion notification is sent from the group management server to all MC service servers subscribed to the group. Affiliations to the deleted group will be removed.

NOTE 1: Any actions taken by the MC service server upon receiving the group deletion notification are not shown in this procedure. Whether ongoing calls associated with the group deletion are impacted is left to implementation.

4. The group management server sends the group deletion notification to group management clients for all group members of the deleted group. MC service client affiliations to the deleted group are removed.

NOTE 2: It is assumed in this flow that the group management client (originator) is not a member of the group, so it does not receive a group deletion notification.

5. The group management server sends a group deletion response to the group management client (originator).

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.

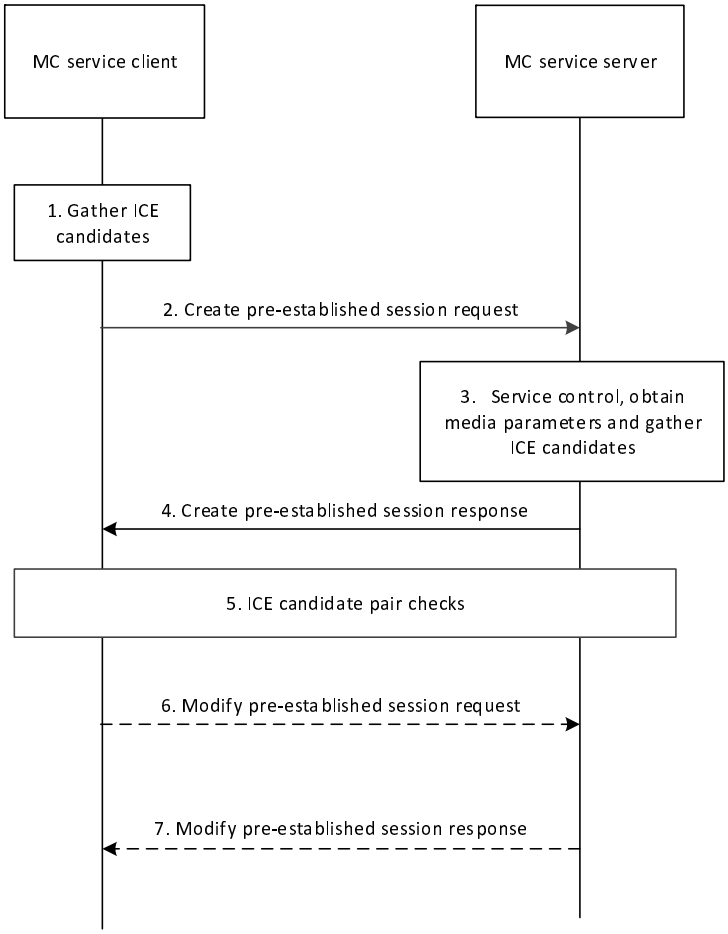

Figure 10.3.2.2-1: Pre-established session establishment

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.

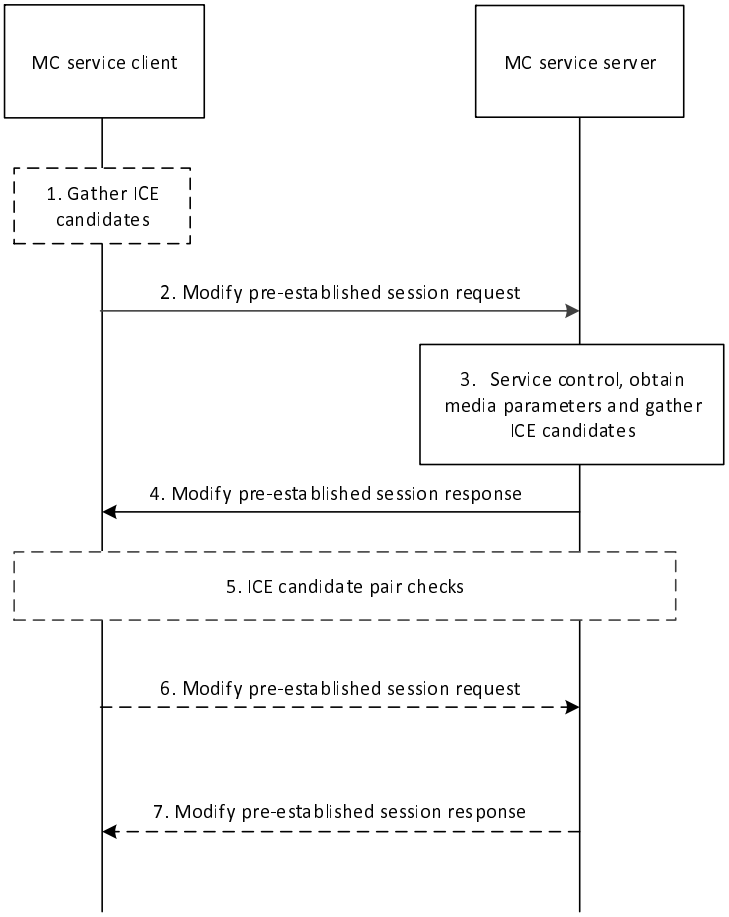

Figure 10.3.2.3-1: Pre-established session modification

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.

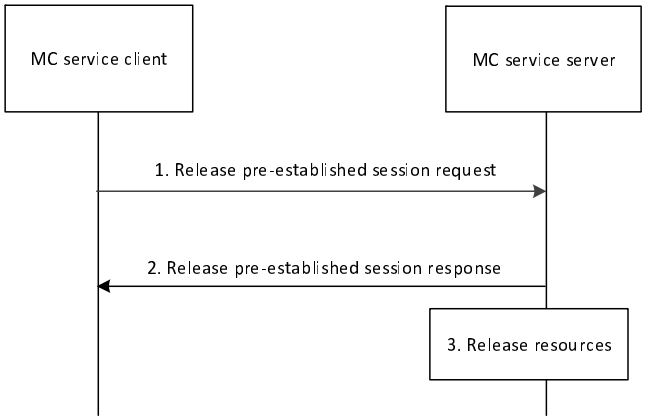

Figure 10.3.2.4-1: MC service client within the MC service UE initiated pre-established session release

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.

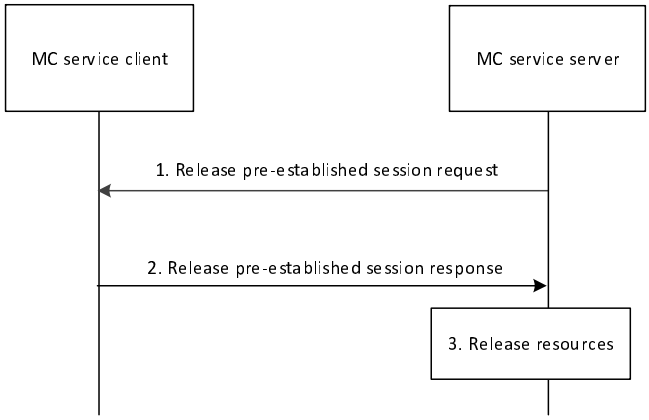

Figure 10.3.2.4-2: MC service server initiated pre-established session release

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

10.6.1 Primary MC system

NOTE: Figure 10.6.1-1 is a high level user authentication and authorization flow. 3GPP TS 33.180 [25] 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 10.6.1-1 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 10.6.1-1. Other alternatives may be possible, such as authenticating the user within the SIP registration phase.

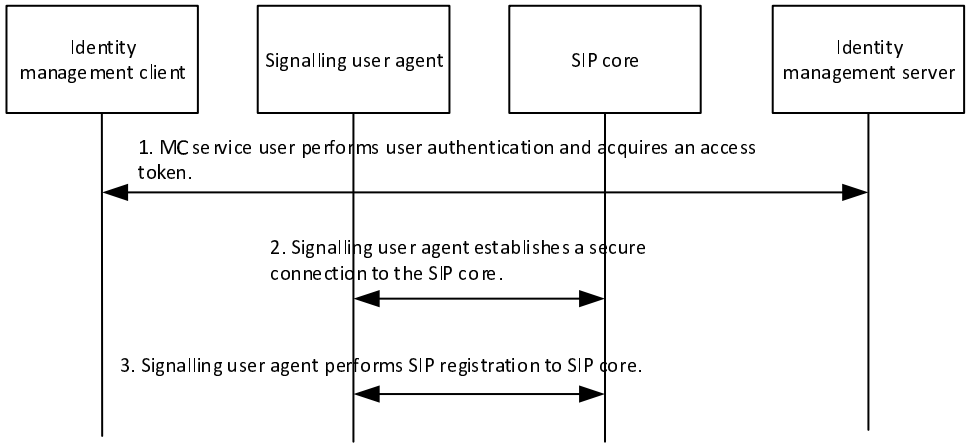

Figure 10.6.1-1: MC service user authentication and registration with Primary MC system, single domain

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.

10.6.2 Interconnection partner MC system

Where communications with a partner MC system using interconnection are required, user authorization takes place in the serving MC system of the MC service user, using the MCX user service authorization procedure specified in 3GPP TS 33.180 [25].

10.6.3 Migration to partner MC system

10.6.3.1 General

The following subclauses describe the procedure used for user authentication and service authorization when migrating to a partner MC system.

To enable migration, the inter-domain MCX user service authorization procedures specified in 3GPP TS 33.180 [25] are used.

10.6.3.2 Information flows

10.6.3.2.1 Migration service authorization request

Table 10.6.3.2.1-1 describes the information flow migration service authorization request sent from the MC service client of the migrating MC service user to the partner MC service server, and from the partner MC service server to the primary MC service server of the migrating MC service user.

Table 10.6.3.2.1-1: Migration service authorization request

Information element	Status	Description
MC service ID (see NOTE 1)	M	The MC service ID of the migrating MC service user provided by the partner MC system.
MC service ID	M	The MC service ID of the migrating MC service user in the primary MC system of the MC service user.
MC service user profile index (see NOTE 2)	M	The MC service user profile index of the selected MC service user profile.
NOTE 1: The MC service ID is provided by the identity management server in the partner MC system during authentication of the migrating MC service user. NOTE 2: The MC service user profile index refers to the MC service user profile provided by the primary MC system of the MC service user that has been selected by the MC service user in order to request migrated MC service on the partner MC system.		

10.6.3.2.2 Migration service authorization response

Table 10.6.3.2.2-1 describes the information flow migration service authorization response sent from the primary MC service server of the migrating MC service user to the partner MC service server of the migrating MC service user, and from the partner MC service server to the MC service client of the migrating MC service user. This information flow is sent individually addressed on unicast or multicast.

Table 10.6.3.2.2-1: Migration service authorization response

Information element	Status	Description
MC service ID (see NOTE)	M	The MC service ID of the migrating MC service user provided by the partner MC system.
MC service ID (see NOTE)	M	The MC service ID of the migrating MC service user in the primary MC system of the MC service user.
Result	M	Success or failure of the migration MC service authorization request
NOTE: The MC service IDs are the MC service IDs that were provided in the migration service authorization request.		

10.6.3.2.3 Migration service de-authorization notification

Table 10.6.3.2.3-1 describes the information flow migration service de-authorization notification sent by a MC service server of Primary MC system of migrated MC service user to a migrated partner MC system from which MC service user is migrating out.

Table 10.6.3.2.3-1: Migration service de-authorization notification

Information element	Status	Description
MC service ID (see NOTE 1)	M	The MC service ID of the migrated MC service user provided by the partner MC system.
MC service ID	M	The MC service ID of the migrated MC service user in the primary MC system of the MC service user.
NOTE 1: The MC service ID is provided by the identity management server in the partner MC system during authentication of the migrated MC service user.		

10.6.3.2.4 MC service authorization notification

Table 10.6.3.2.4-1 describes the information flow about the notification for successful completion of MC service user service authorization after migrating to the partner MC system.

Table 10.6.3.2.4-1: MC service user authorization notification

Information element	Status	Description
MC service ID	M	The MC service ID of the migrating MC service user provided by the partner MC system.
Service authorization Indication	M	Indication to provide the successful completion of MC service user service authorization after migrating to the partner MC system

10.6.3.3 Procedures

10.6.3.3.1 Migration service authorization procedure

The procedure for service authorization for migration to a partner MC system and subsequent service authorization to migration partner MC system is shown in figure 10.6.3.3.1-1.

Pre-conditions

- The MC service user wishes to migrate to the partner MC system.
- The MC service client has been configured with an MC service user profile that contains the necessary parameters needed for connectivity with the partner MC system.
- A user authentication process has taken place which has supplied the necessary credentials to the MC service client to permit service authorization to take place in the partner MC system.

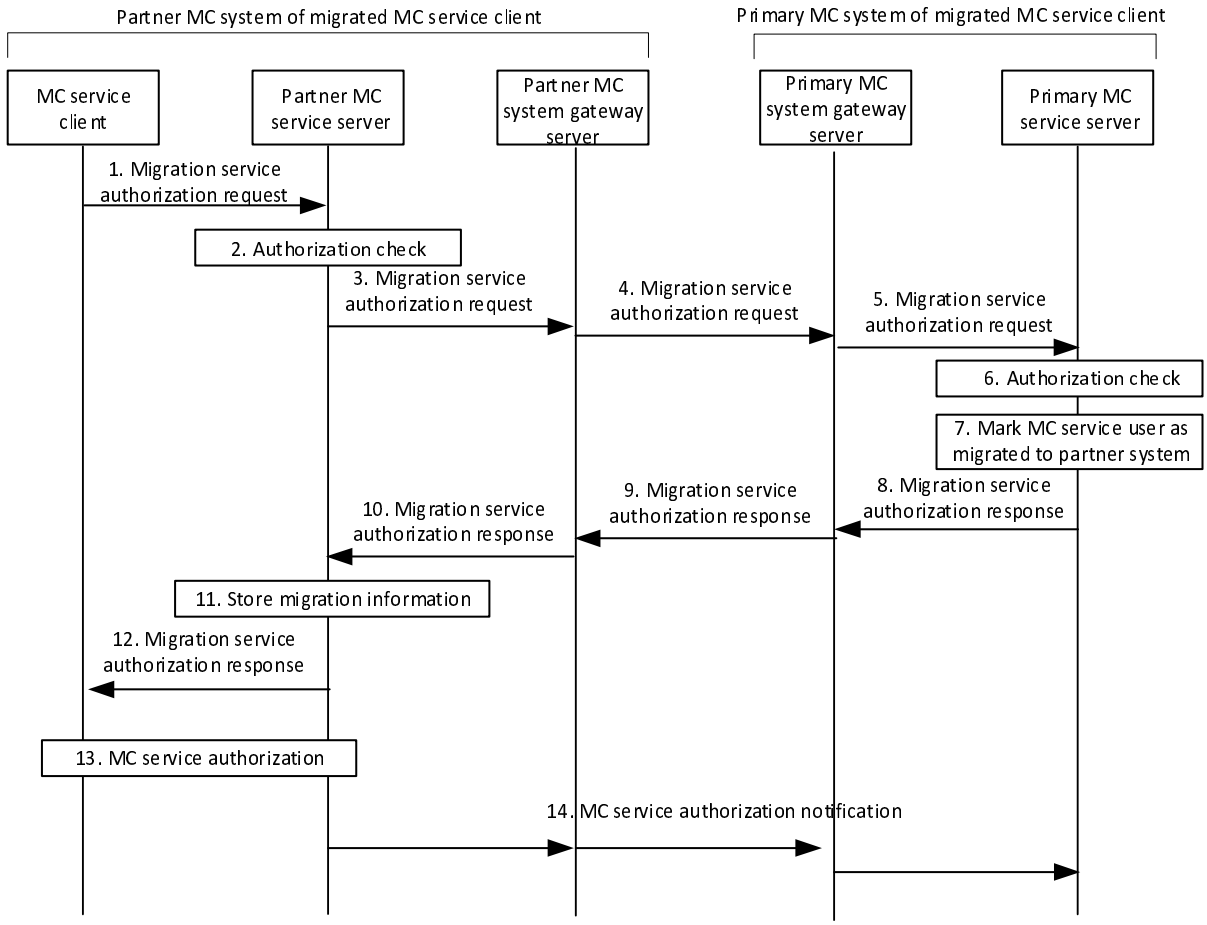

Figure 10.6.3.3.1-1: Service authorization for migration to partner MC system and subsequent service authorization

1. The MC service client requests migration service authorization with the partner MC service server indicating the selected MC service user profile to be used during migrated MC service. The MC service client provides both the MC service ID provided during user authentication in the partner MC system, and the MC service ID of the MC service user in the primary MC system of the MC service user.

NOTE 1: The migrating MC service client also provides authentication credentials which are specified in 3GPP TS 33.180 [25].

2. The partner MC service server performs an initial authorization check to verify that the MC service user is permitted to migrate to the partner MC system from the primary MC system of the MC service user.

NOTE 2: The criteria for the initial authorization check is outside the scope of the present document, but for example could be based on a pre-configured list of users who are expected to request migrated service authorization.

3. The partner MC service server identifies the primary MC system of the MC service user of the MC service client by use of the MC service ID of the MC service user in the primary MC system of the MC service user, which was presented by the MC service client in step 1, and sends a migration service authorization request to the gateway server in the partner MC system.

4. The partner MC system gateway server identifies the primary MC system of the MC service user from the MC service ID presented in step 3, and forwards the migration service authorization request to the gateway server of the primary MC system.

5. The gateway server in the primary MC system of the MC service user identifies the primary MC service server of the MC service user from the MC service ID presented in step 3, and forwards the migration service authorization request to that MC service server.

6. The primary MC service server of the MC service user performs an authorization check, to verify that migration is permitted to that partner MC system by this MC service user using the indicated MC service user profile.

7. The primary MC service server marks the MC service user as having migrated, and records the partner MC system as the migrated MC system. The primary MC service server also stores other necessary information related to the migrated MC service user (e.g., MC service ID of the migrated MC service user provided by the primary MC system mapped to the MC service ID of the migrated MC service user provided by partner MC system).

8. The primary MC service server sends a migration service authorization response to the gateway server in the primary MC system.

9. The gateway server in the primary MC system sends the migration service authorization response to the gateway server in the partner MC system.

10. The gateway server in the partner MC system sends the migration service authorization response to the partner MC service server.

11. The partner MC service server stores the necessary information related to the migrated MC service user (e.g., MC service ID of the migrated MC service user provided by the primary MC system mapped to the MC service ID of the migrated MC service user provided by partner MC system). The migration status of the MC service user allows proper communication redirection back to the primary MC system once the migrated MC service user is no longer migrated on this partner MC system.

NOTE 3: The stored necessary information both in the primary MC system and partner MC system related to the migrated MC service user (e.g., MC service ID of the migrated MC service user provided by the primary MC system mapped to the MC service ID of the migrated MC service user provided by partner MC system) is used for proper communication redirection only after successful completion of MC service authorization at partner MC system (i.e. migrated MC system).

12. The partner MC service server sends the migration service authorization response to the MC service client, confirming that successful migration and service authorization has taken place.

NOTE 4: If topology hiding is not used, the migration service authorization request and migration service authorization response messages are sent between the MC service servers in the primary and partner MC system without the need to be sent via an MC gateway server.

13. The MC service user successfully completes the MC service authorization with the MC service server within the partner MC system to which the MC service user is migrating into.

14. The partner MC service server of partner MC system notifies the primary MC system of the MC service user of the MC service client by sending the MC service authorization notification.

10.6.3.3.2 Migration service de-authorization procedure initiated by MC service server

10.6.3.3.2.1 Migrated MC service user returns back to its primary MC system

The procedure for migration service de-authorization from a partner MC system is shown in figure 10.6.3.3.2.1-1.

NOTE 1: When the MC service from the partner MC system is stopped for the MC service user is out of scope of the present document.

Pre-conditions

- The MC service user has successfully completed the MC service authorisation with the MC service server within the primary MC system to which the MC service user is returning back from migrated MC system.

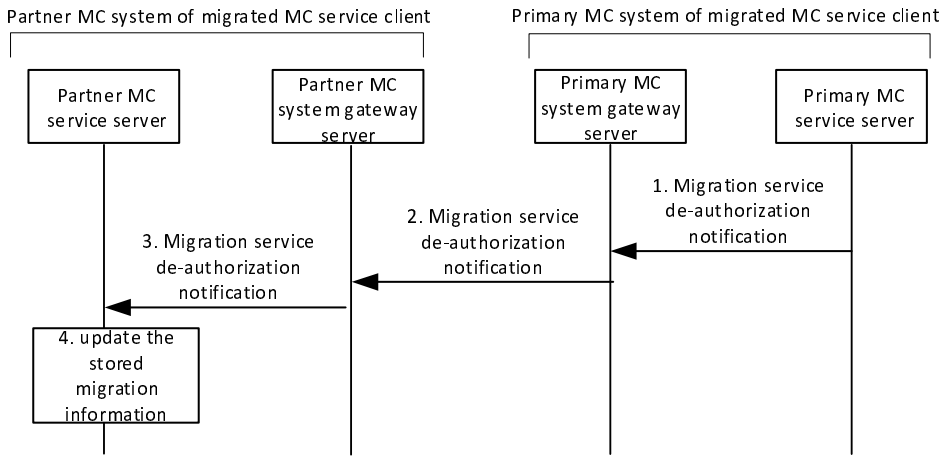

Figure 10.6.3.3.2.1-1 Service de-authorization of migration from partner MC system

1. The primary MC service server sends a migration service de-authorization notification to the primary MC system gateway server.

2. The primary MC system gateway server sends the migration service de-authorization notification to the partner MC system gateway server.

NOTE 2: If topology hiding is not used, the migration service de-authorization notification message is sent between the MC service servers in the primary and partner MC system without the need to be sent via an MC gateway server.

3. The partner MC system gateway server sends the migration service de-authorization notification to the partner MC service server.

4. The partner MC service server updates the stored necessary information related to the was-migrated MC service user accordingly, (e.g., MC service user's MC service ID provided by the primary MC system mapped to the MC service ID provided by partner MC system).

NOTE 3: The period of how long MC system B will maintain the mapping information is left for implementation.

10.6.3.3.2.2 Migrated MC service user migrate to another partner MC system

The procedure for migration service de-authorization from a partner MC system is shown in figure 10.6.3.3.2.2-1.

Pre-conditions

- The MC service user has successfully completed the MC service authorization with the MC service server within the partner MC system C to which the MC service user is migrating into.

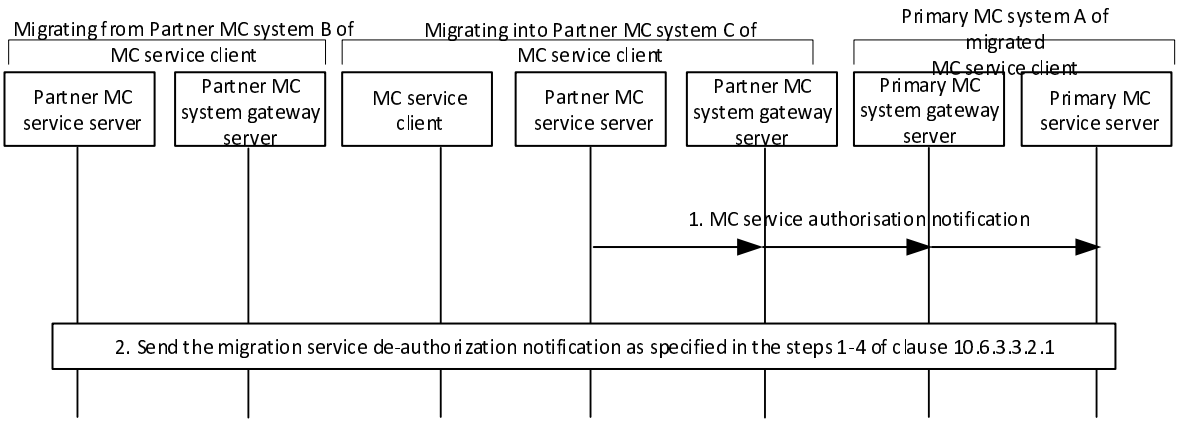

Figure 10.6.3.3.2.2-1 Service de-authorization of migration from partner MC system

1. The partner MC service server of partner MC system C notifys the primary MC system of the MC service user of the MC service client by sending the MC service authorization notification
2. Send the migration service de-authorization notification as specified in the steps 1-4 in Figure 10.6.3.3.2.1-1 of clause 10.6.3.3.2.1.

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, FEC information)
Monitoring state	O	The monitoring state is used to control if the client is actively monitoring the MBMS bearer quality or not.
Announcement acknowledgment	O	Indicate if the MC service server requires an acknowledgement of the MBMS bearer announcement.
ROHC information	O	Indicate the usage of ROHC and provide the parameters of the ROHC channel to signal to the ROHC decoder.
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.
MBMS reception quality level	O	The reception quality level per TMGI (see NOTE)
NOTE: The set of quality levels helps service continuity in MBMS scenarios. A reception quality level may help to make an efficient switching decision to another bearer. How these levels are used is implementation specific.		

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 to another MC service server (MBMS bearer control 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 (MBMS bearer control role) to the MC service server.

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 to an MC service server (MBMS bearer control 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
MC Group ID	O	The MC group id for when the request is sent for a specific group call.

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 (MBMS bearer control role) that has a desired bearer to the MC service server.

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
Media stream identifier	O	This element identifies the media stream of the SDP used for the group call (e.g. MBMS subchannel).
Media distribution indicator	O	Indicates to the MC service server whether the media in the ongoing group communication should be sent or not

10.7.2.8 Identify multicast participants request

Void

10.7.2.9 Remove call from bearer request

Void

10.7.2.10 Media distribution release

Table 10.7.2.10-1 describes the information flow media distribution release from the MC service server to an MC service server (MBMS bearer control role) that has the used bearer.

Table 10.7.2.10-1: Media distribution release

Information element	Status	Description
TMGI	M	TMGI information
Bandwidth	M	The bandwidth released by the MC service server that used the bearer
MC Group ID	O	The MC group id for when the request is sent for a specific group call.

10.7.2.11 Media broadcasting notification

Void.

10.7.2.12 Group status notification

Table 10.7.2.12-1 describes the information flow for the group status notification from MC service server to MC service client.

Table 10.7.2.12-1: Group status notification

Information element	Status	Description
MC service group ID	M	The MC service group ID of the group
Status of the group	M	Indicate the group has on-going call or not

10.7.2.13 MBMS suspension report

Table 10.7.2.13-1 describes the information flow for the MBMS suspension report from MC service client to MC service server.

Table 10.7.2.13-1: MBMS suspension report

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

10.7.3 Procedures for MBMS usage

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.

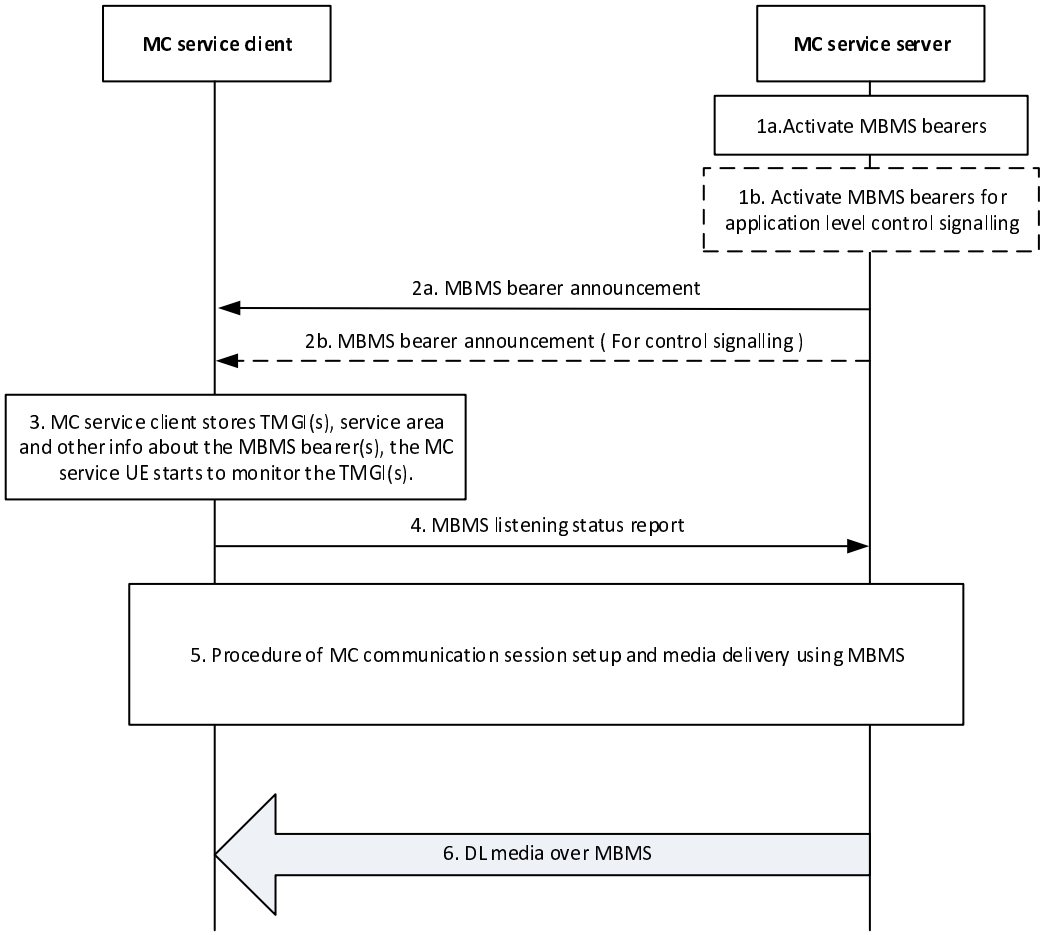

Figure 10.7.3.1.2-1: Use of pre-established MBMS bearers

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.

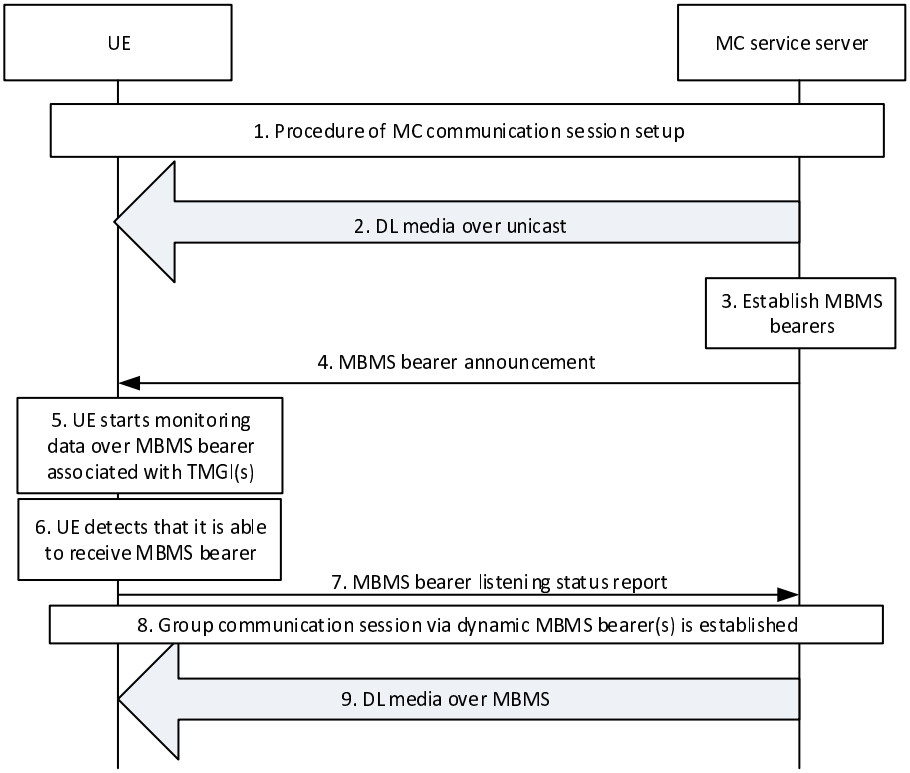

Figure 10.7.3.2-1: Use of dynamic MBMS bearer establishment

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 the MBMS listening status associated to the monitored TMGI, (e.g. that it is successfully receiving the TMGI). The MC service client may also notify the MBMS reception quality level of the TMGI. MC service server stops sending media data over unicast way to the MC service client.

NOTE 2: The MBMS reception quality level may be used by the MC service server to make an efficient decision to switch again to a unicast transmission or to take measures to prepare such a switch (e.g. when the quality level indicates that the reception quality of the MBMS bearer is decreasing or reaching an insufficient quality level for the reception of MC services).

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

NOTE 3: 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.

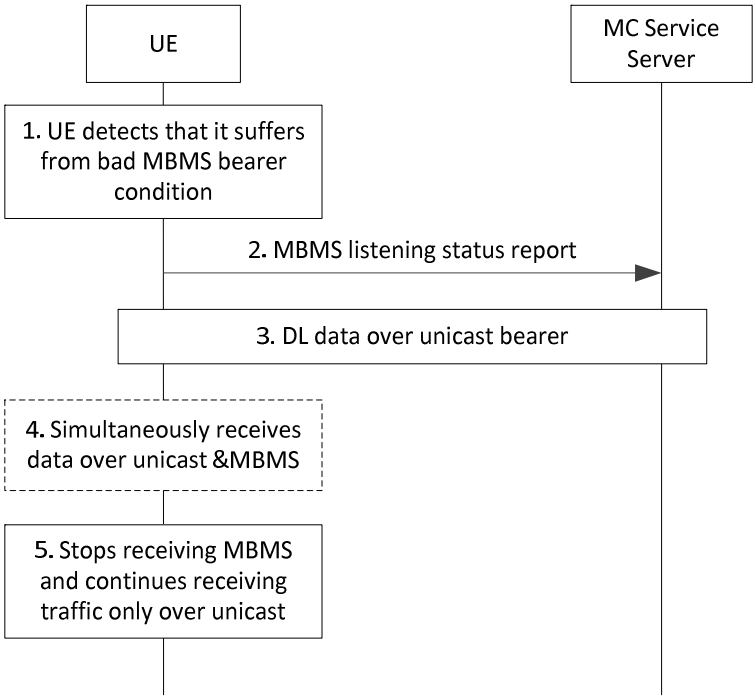

Figure 10.7.3.3-1: Switching from MBMS delivery to unicast delivery

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.

NOTE 1: To efficiently notify the MC service server, e.g., when the MC service client detects that the reception quality of the MBMS bearer is decreasing or reaching an insufficient quality level for the reception of MC services, the MC service client proactively may send to the MC service server a MBMS listening status report including the MBMS reception quality level.

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

NOTE 2: 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 dynamic data (e.g. status of the group)
- 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.

The MC service client shall not send responses to group-addressed application level control signalling unless instructed or configured to respond.

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.

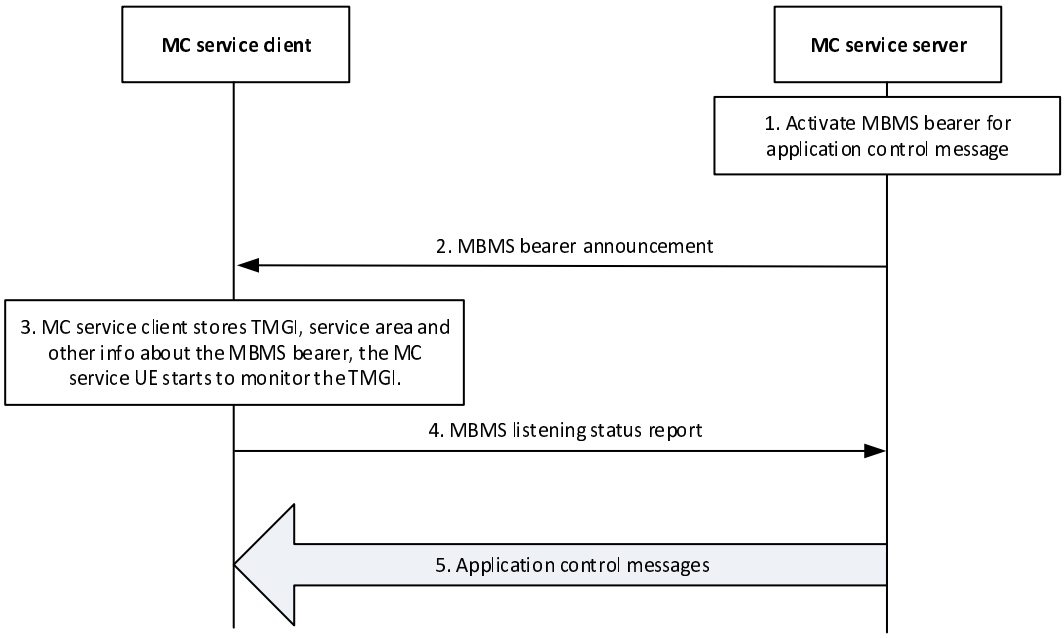

Figure 10.7.3.4.2-1: Use of MBMS bearer for application level control signalling

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. The MC service client may also indicate at which MBMS reception quality level it has received the MC service media on the MBMS bearer. Hence, 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.

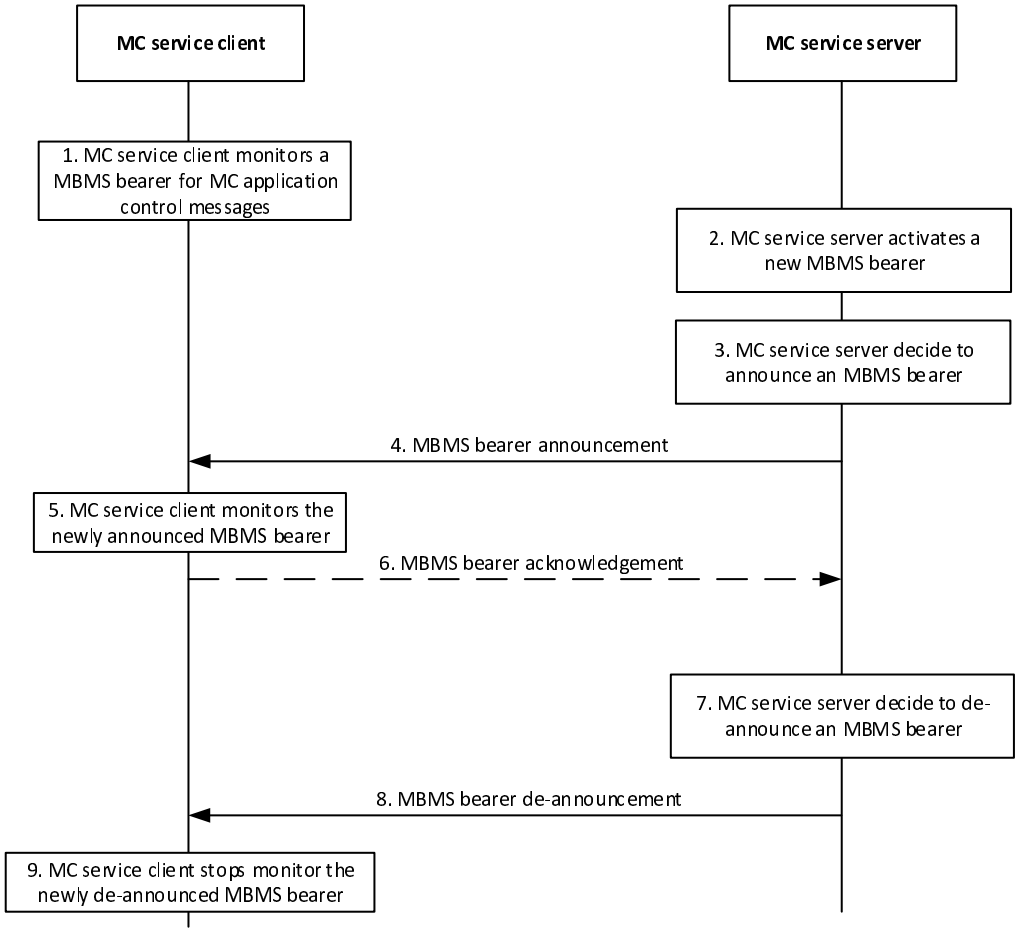

Figure 10.7.3.5.2-1: MBMS bearer announcement over an MBMS bearer used for application control messages

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. Furthermore, based on the received quality, the MC service client may notify the MC service server at which MBMS reception quality level it has received the MC service media on the MBMS bearer.

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 can be 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

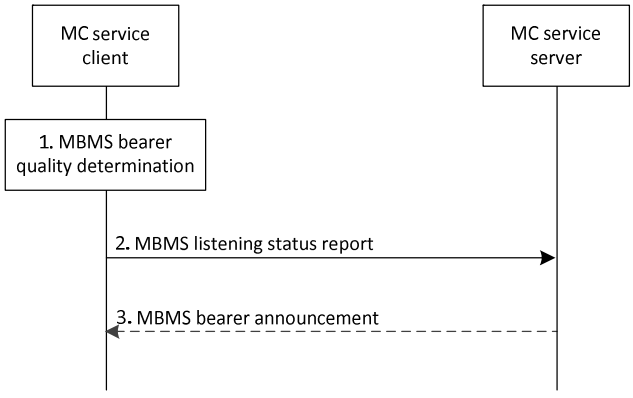

Figure 10.7.3.6.2-1: MBMS bearer quality detection

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 can 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. The MC service client may also map the determined MBMS bearer quality to a MBMS reception quality level. The

MBMS reception quality level indicates at which specific MBMS bearer quality level the MC service media has been received. Based on the MBMS reception quality level, the MC service server may efficiently decide to switch to another bearer or to take measures to prepare such a switch.

NOTE 1: The set of MBS reception quality levels and the mapping of the determined MBMS bearer quality to those levels are left to implementation.

Editor's note: The set of MBMS reception quality levels and the mapping of the determined MBMS bearer quality to those levels are FFS.

NOTE 2: 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 is used to define the MBMS listening status, which indicates if the MBMS bearer quality has been acceptable or not to receive a specific MC service media. If the MBMS bearer quality is mapped to a different MBMS reception quality level, the MC service client may send an MBMS listening status report including the MBMS reception quality level.

NOTE 3: 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 4: 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.

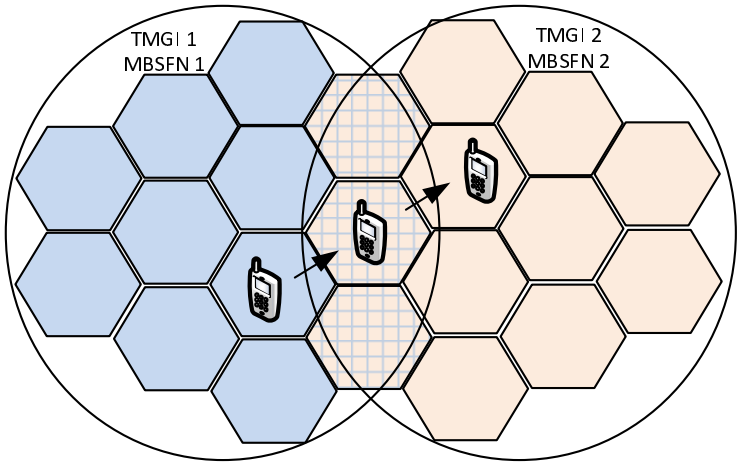

Figure 10.7.3.7.2-1: Two MBMS bearer using overlapping MBSFN areas

The procedural steps will work as follows:

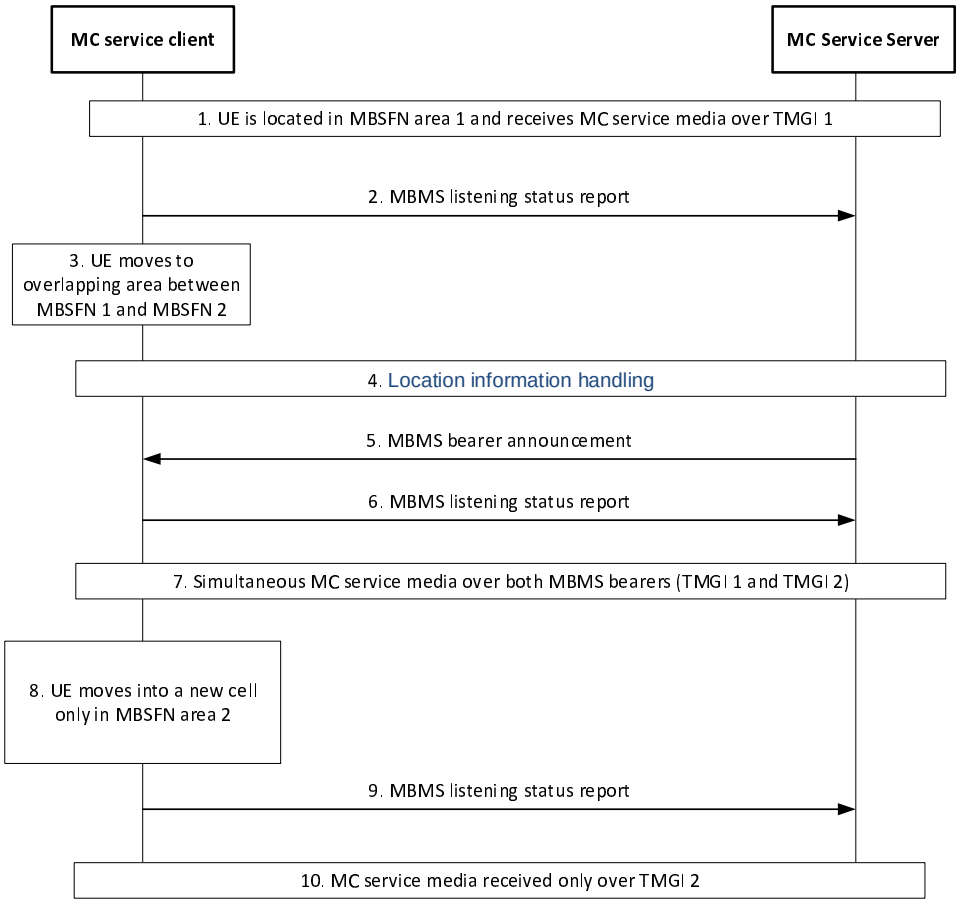

Figure 10.7.3.7.2-2: Service continuity when moving from one MBSFN to another

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 MC service client notifies the MC service server that it is successfully receiving the MC service media over TMGI 1. The MC service client may also notify the MBMS reception quality level of TMGI 1.

NOTE 1: The MBMS reception quality level may be used by the MC service server to make an efficient decision to switch to another MBMS bearer or to a unicast bearer, or to take measures to prepare such a switch (e.g. when the quality level indicates that the reception quality of the MBMS bearer is decreasing or reaching an insufficient quality level for the reception of MC services).

3. 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.

4. Location information are provided from the MC service UE via the Location management client to the Location management server. For that, the MC service UE uses the SAI information found in the system information block (SIB) transmitted by the radio cells. The location management server provides the location information to the MC service server.

NOTE 2: Whether the MC service server has subscribed for notifications, as described in clause 10.9.3.6.1 of the present document, Event-trigger location information notification procedure, or uses on-demand requests, as described in clause 10.9.3.6.2 of the present document, On-demand usage of location information procedure, is out of scope.

5. The MC service server sends to the MC service client a MBMS bearer announcement with information related to TMGI 2 (if the MC service server had not done it before). Hence, the MC service client knows that TMGI 2 transmits the same MC service media.

6. The MC service client notifies the MC service server that it is successfully receiving TMGI 1 and TMGI 2. The MC service client may also notify the MBMS reception quality level per TMGI.

7. The MC service client may receive the MC service media over both MBMS bearers, i.e. TMGI 1 and TMGI 2. The MC service client may also verify that it is the same content sent on both bearers. The duplicated packets may also be used to perform error corrections.

8. The UE moves into a new cell in MBSFN area 2, where only TMGI 2 is active.

9. The MC service client notifies the MC service server that it is successfully receiving the MC service media over TMGI 2. The MC service client may also notify the MBMS reception quality level of TMGI 2.

10. The MC service client receives the MC service media only over TMGI 2.

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), as described in steps 4-6 above. To send the location report and the MBMS listening report by the MC service client to the MC service server 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 10.7.3.7.2-3. 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.

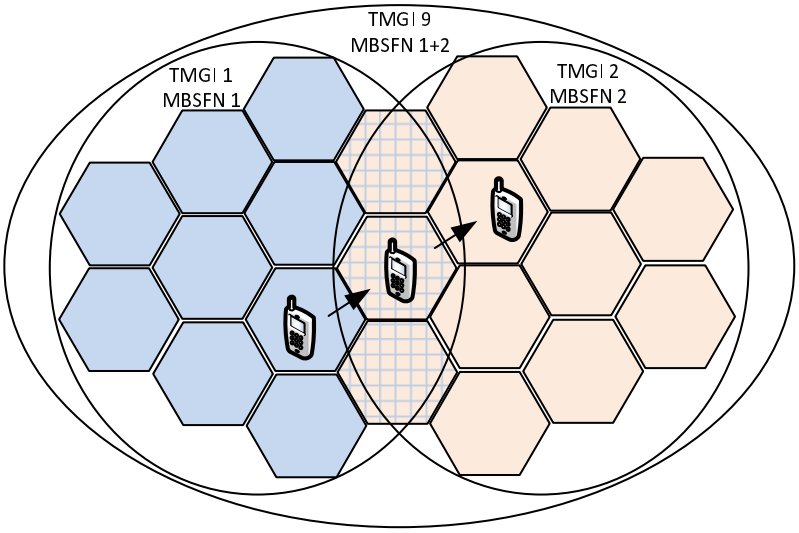

Figure 10.7.3.7.2-3: Two MBMS bearer using overlapping MBSFN areas with a separate MC application signalling bearer

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.

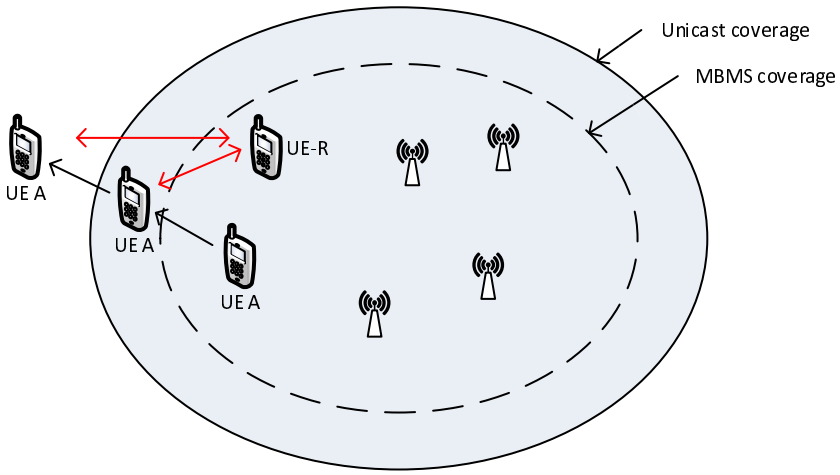

Figure 10.7.3.7.3-1: UE A is moving from a position in MBMS coverage to outside the network coverage passing an area where only unicast is possible

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.

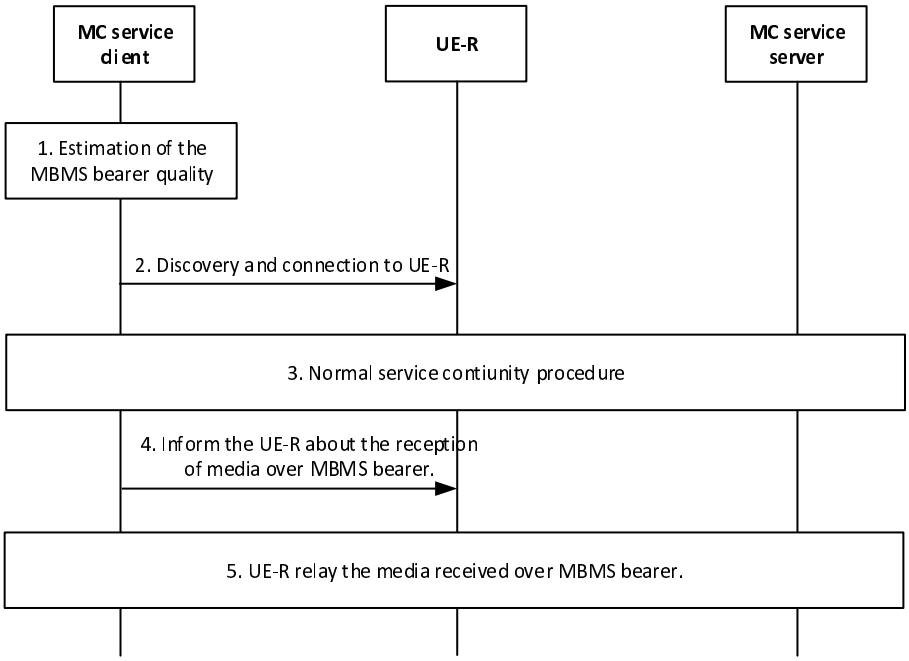

Figure 10.7.3.7.3-2: Service continuity over MBMS bearer using UE-to-network relay

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 service 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 UEs 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

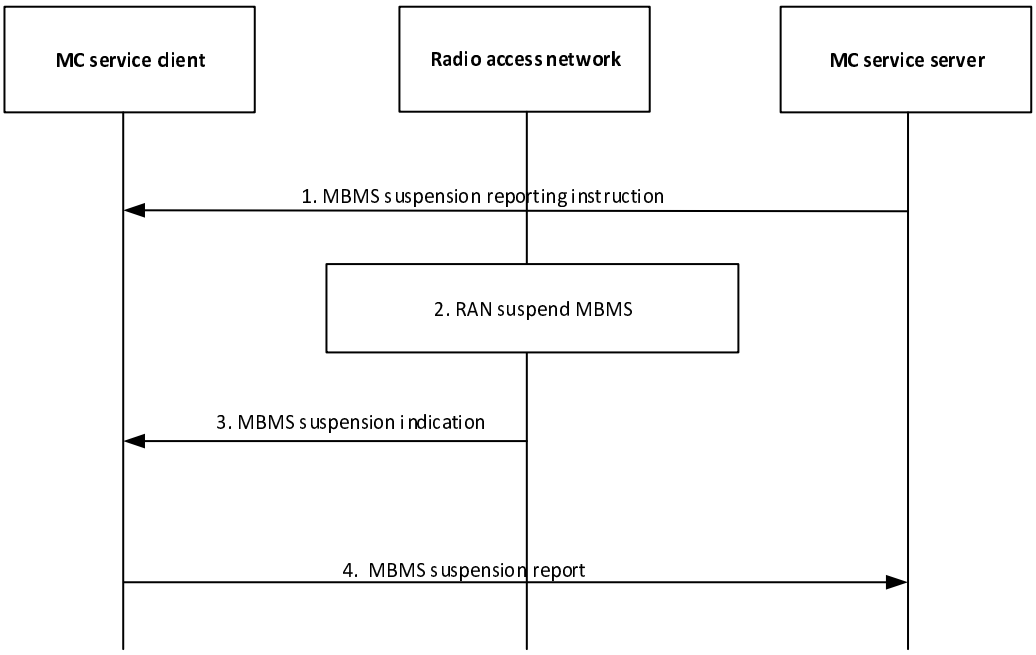

Figure 10.7.3.8.2-1: MBMS suspension notification from MC service client

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 may manage 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 control role. Different MC service servers may allocate bearers as needed and make them available for other MC service servers to use. The use of the procedure in this sub clause is optional. MC system that supports multi-server bearer coordination shall use this procedure.

NOTE: Within one group communication session, 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 control role) might be involved. For brevity, this clause only illustrates the simplest case.

10.7.3.9.2 Procedures

10.7.3.9.2.1 MBMS bearer coordination independent on broadcasted media

The procedure in this sub clause may be used when two or more MC service servers are serving users in the same area and are configured to share MBMS bearers for that specific area. The MC service servers may be of the same kind or different kind. The MC service servers are not participating in the same group call, which means that each MC service server broadcast media independently of each other.

Pre-conditions:

- All MC service servers are configured with the contact information of those MC service servers that are configured to take the MBMS bearer control role.

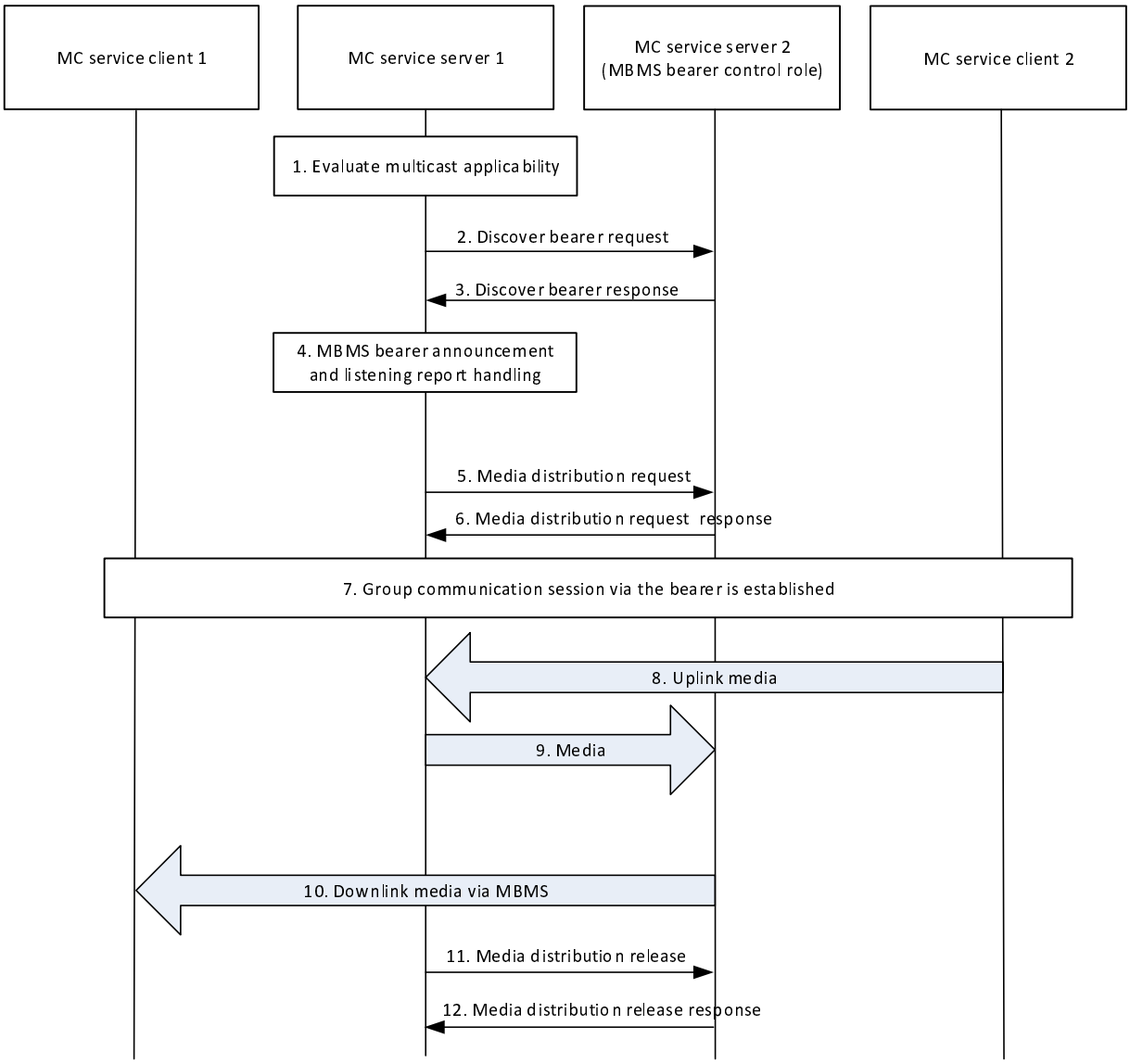

Figure 10.7.3.9.2.1-1: Multiple server MBMS procedure

1. The MC service server 1 evaluates 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.

2. The MC service server 1 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 1 consults a pre-configured list of MC service servers and sends them a discover bearer request. This request may be sent to several MC service servers.

NOTE: MC service servers of the same type can be configured to discover bearers from a single server. The single server then becomes a centralized entity for MBMS bearer control 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.

3. The MC service server 2 (MBMS bearer control role) responds with a discover bearer response indicating whether there is an MBMS bearer available in the specific MBMS service area with the requested bandwidth. The discover bearer response message includes the TMGI of the bearer that is shared between the MC service servers. If the bearer of interest has insufficient bandwidth, the polling MC service server 1 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 1 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 1 may then become available for other MC service servers (controlling role) for other MC service groups.

4. The MC service server 1 performs the MBMS bearer announcement and the MBMS listening reporting according relevant procedures specified in this specification. If the MC service server 2 is authorized to receive MBMS related location information from the users utilizing the services from MC service server 1, the MC service server 2 may optionally do the MBMS bearer announcement and handling the listening reports on behalf of MC service server 1. Listening reports shall in this case be sent to both MC service server 1 and MC service server 2.

5. The MC service server 1 sends a media distribution request to the MC service server 2 (MBMS bearer control role). The media distribution request is sent to reserve the specified capacity in the MBMS bearer.

6. MC service server 2 (MBMS bearer control role) sends a media distribution response to the MC service server 1 indicating whether the request can be supported and supplies details about the bearer.

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

8. MC service client 2 sends media on the uplink to the MC service server 1

9. The MC service server 1 forwards the media to MC service server 2 (MBMS bearer control role).

10. The MC service server 2 (MBMS bearer control role) distributes the media to MBMS served MC service client 1 via multicast.

11. The MC service server 1 sends a media distribution release request, informing the MC service server 2 (MBMB bearer control role) to request the MC service server 2 (MBMS bearer control role) to release the capacity that was reserved in step 5.

12. The MC service server 2 (MBMS bearer control role) respond to the request by sending a media distribution release request.

10.7.3.9.2.2 MBMS bearer coordination within one group call

The procedure in this sub clause may be used when two MC service servers are serving users in the same area and are configured to share MBMS bearers for that specific area. The MC service servers are of the same kind, and the MC service servers may participate in the same group call, and by that have a need to broadcast the same content.

Pre-conditions:

- All MC service servers are configured with the contact information of those MC service servers that are configured to take the MBMS bearer control role.

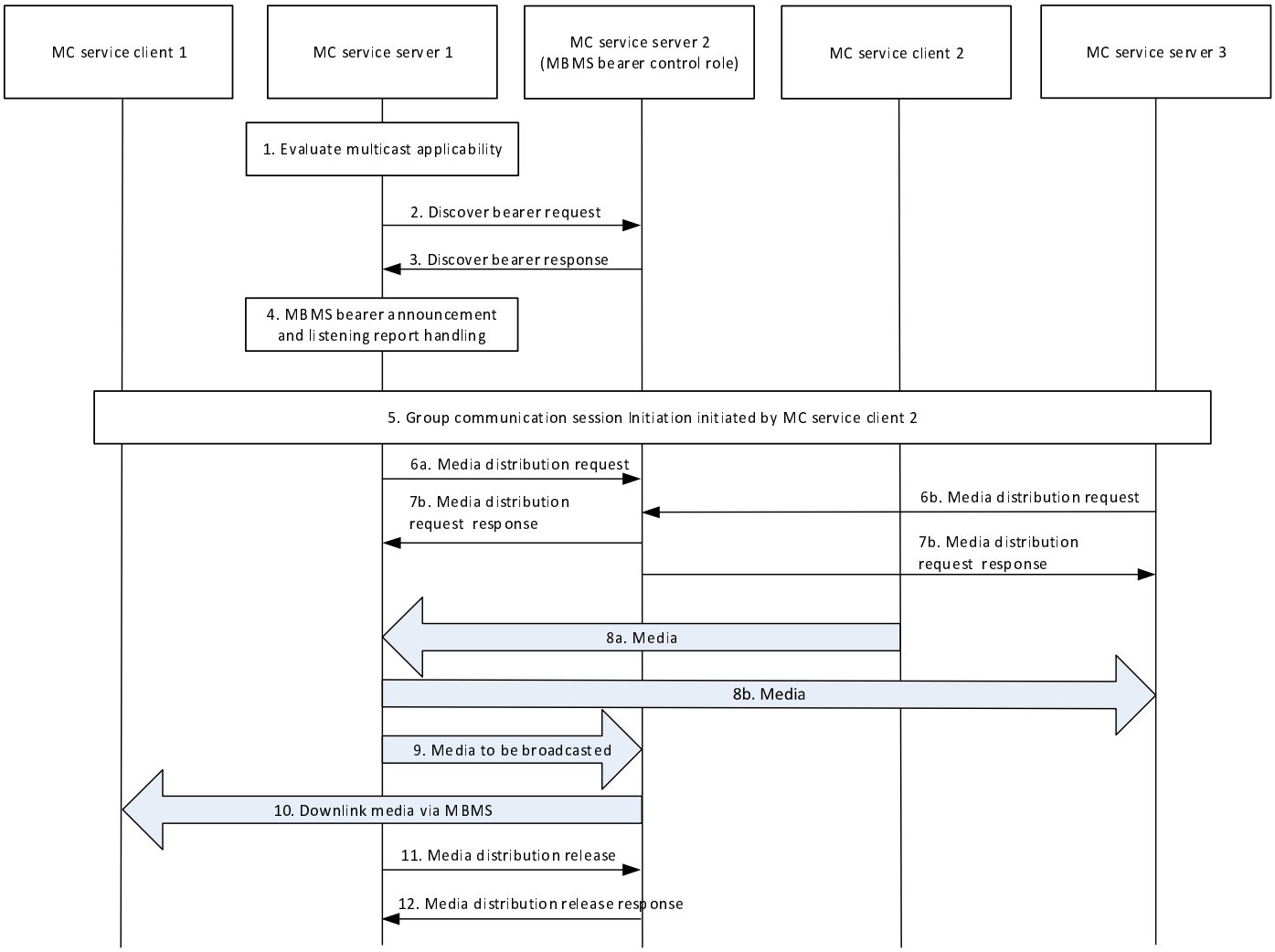

Figure 10.7.3.9.2.2-1: Multiple server MBMS procedure

1. The MC service server 1 evaluates 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.

2. The MC service server 1 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 1 consults a pre-configured list of MC service servers and sends them a discover bearer request. This request may be sent to several MC service servers.

NOTE 1: MC service servers of the same type can be configured to discover bearers from a single server. The single server then becomes a centralized entity for MBMS bearer control 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.

3. The MC service server 2 (MBMS bearer control role) responds with a discover bearer response indicating whether there is an MBMS bearer available in the specific MBMS service area with the requested bandwidth. The discover bearer response message includes the TMGI of the bearer that is shared between the MC service servers. If the bearer of interest has insufficient bandwidth, the polling MC service server 1 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 1 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 1 may then become available for other MC service servers (controlling role) for other MC service groups.

4. The MC service server 1 performs the MBMS bearer announcement and the MBMS listening reporting according relevant procedures specified in this specification. If the MC service server 2 is authorized to receive MBMS related location information from the users utilizing the services from MC service server 1, the MC service server 2 may optionally do the MBMS bearer announcement and handling the listening reports on behalf of MC service server 1. Listening reports shall in this case be sent to both MC service server 1 and MC service server 2.

NOTE 2: Step 1-4 is also performed by MC service server 3, but is not shown in the procedure to make it easier to read.

5. The MC service client 2 initiate a group call that is subject for multicast transmission. In this scenario there are more than one MC service server (i.e. MC service server 1 and MC service server 3) that serves MC service clients that are affiliated to the group, and by that should receive the media in the group call.

6a. The MC service server 1 sends a media distribution request to the MC service server 2 (MBMS bearer control role). The media distribution request includes the MC group identifier. This indicates that the media distribution request is used for this specific group call.

6b. The MC service server 3 sends a media distribution request to the MC service server 2 (MBMS bearer control role). The media distribution request includes the MC group identifier. This indicates that the media distribution request is used for this specific group call.

7a. The MC service server 2 (MBMS bearer control role) sends a media distribution response to the MC service server 1 indicating whether the request can be supported and supplies details about the bearer. This also includes details on which media stream that should be used for broadcasting the media on the MBMS bearer. This information is used in the MapGroupToBearer message sent by the MC service server when setting up the group call.

7b. The MC service server 2 (MBMS bearer control role) sends a media distribution response to the MC service server 3 indicating that the group call is already transmitted on the MBMS bearer by another MC service server. Based on the information, the MC service server 3 could decide to not broadcast media if media is already being broadcasted.

8a. The media is sent from the MC service client 2 to MC service server 1, which is the participating server for the MC service group of the group call.

8b. The media is forwarded to all MC service servers that are serving users that takes part in the group call.

NOTE 3: The figure above does not visualize the participating server for the MC service group and controlling server for the MC service group. The media is sent to all participating servers for the MC service group which are the servers that decide on unicast or multicast transmission.

9. The MC service server 1 forwards the media to MC service server 2 (MBMS bearer control role).

10. The MC service server 2 (MBMS bearer control role) distributes the media to MBMS served MC service client 1 via multicast.

11. The MC service server 1 sends a media distribution release request, informing the MC service server 2 (MBMS bearer control role) to request the MC service server 2 (MBMS bearer control role) to release the capacity that was reserved in step 5. The media distribution release request shall only be sent when the group call is terminated. 12. The MC service server 2 (MBMS bearer control role) respond to the request by sending a media distribution release request.

10.7.3.10 MBMS bearer event notification

10.7.3.10.1 General

The MC service server is an instantiation of a GCS AS. For the MC service server to know the status of the MBMS bearer, and thus know the network ability to deliver the service, it is required that the network provides MBMS bearer event notifications to the MC service server. The different events notified to the MC service server include the MBMS bearer start result (e.g., when the first cell successfully allocated MBMS resources), including information if any cells fail to allocate MBMS resources to a specific MBMS bearer.

10.7.3.10.2 Procedure

The procedure in figure 10.7.3.10.2-1 shows notification information flows from MC service server to BM-SC.

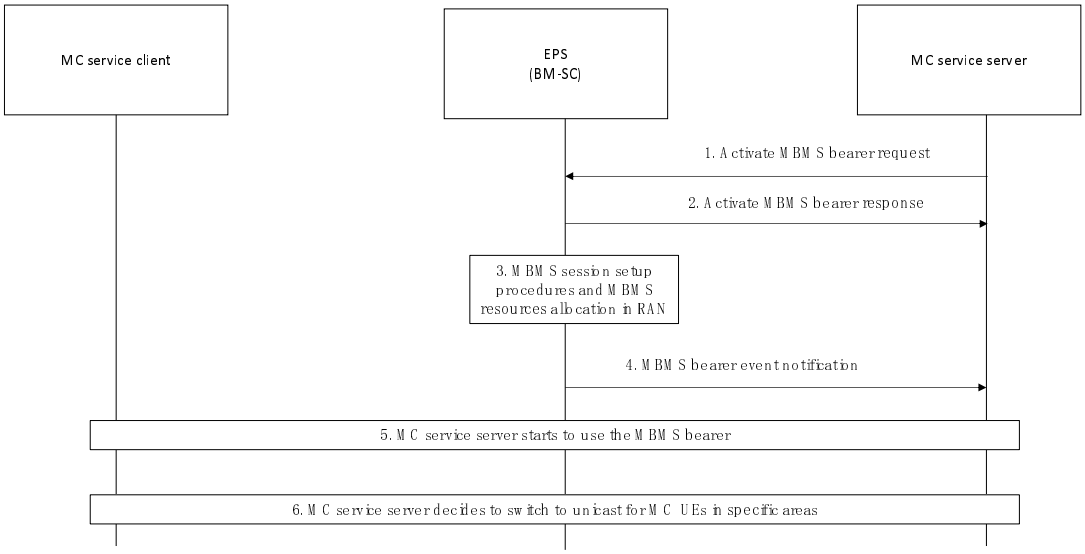

Figure 10.7.3.10.2-1: MBMS bearer event notification

1. The MC service server activates an MBMS bearer. The activation of the MBMS bearer is done on the MB2-C reference point and according to 3GPP TS 23.468 [18].
2. The BMSC will respond to the activation with an Activate MBMS bearer response message, according to 3GPP TS 23.468 [18].
3. The EPC and RAN will initiate the MBMS session start procedure according to 3GPP TS 23.246 [11]. This procedure is outside the scope of this specification.
4. At the first indication of a successful MBMS session start procedure, the BM-SC sends a MBMS bearer event notification, indicating that the MBMS bearer is ready to use.
5. The MC service server starts to use the MBMS bearer according to the MBMS procedures in this specification.
6. The MC service server may decide, based on the received events, to switch to unicast transmission for relevant MC service clients.

10.7.3.11 Use of FEC to protect MBMS transmissions

10.7.3.11.1 General

Application layer FEC can be used to recover the packet losses when delivering a MC service over MBMS, to reach its required level of QoS.

Support of FEC is optional for the MC service servers and MC service clients

Adding FEC introduces an extra latency in the end to end media transport. This extra latency is bounded to fulfil the low latency requirements for mission critical services.

FEC can be applied by the BM-SC if required by the MC service server (subclause 10.7.3.11.2), or directly by the MC service server (subclause 10.7.3.11.3). FEC is decoded by the MC service client. Either method is independent of the other.

The MC service server may consider the listening status reports from previous MBMS bearer quality detection procedures (subclause 10.7.3.6) to adjust the FEC parameters when delivering over a new MBMS bearer.

10.7.3.11.2 FEC encoding by the BM-SC

In this procedure, depicted in figure 10.7.3.11.2-1, the MC service server asks the BM-SC to apply FEC to a set of medias, transported by a MBMS bearer, using the Setup FEC request.

This procedure can be applied when using pre-established MBMS bearers (10.7.3.1) or dynamic MBMS bearers (10.7.3.2).

Pre-condition:

1. The MC service server has already activated a MBMS Bearer, with the MBMS Bearer request specified in 3GPP TS 23.468 [18].

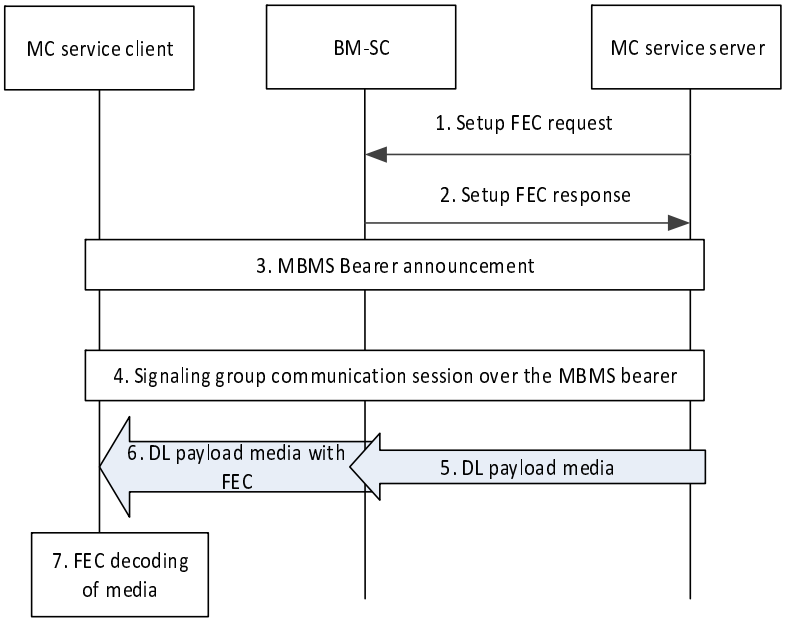

Figure 10.7.3.11.2-1: Application of FEC by the BM-SC

1. The MC service server decides to set up FEC for a set of MC service media flows. The request is done on the MB2-C reference point. It includes the following elements: the TMGI of the bearer transporting those media, the media descriptions (codecs, transport protocols, bitrates, destination ip addresses and ports), the identification of the FEC repair packet flow (IP destination and port), an upper bound to the additional latency resulting to FEC application. The MC Service server may perform this request several times to protect separately different sets of media transported within the same MBMS bearer.

2. If the BM-SC can satisfy the request, the Setup FEC response includes a modified list of media information and FEC information. The response also includes an identifier to the FEC process instance, which can be used to release the application of FEC for these media flows.

NOTE 1: Source media packets may be modified by the application of FEC (e.g. addition of a footer of header), leading to a modification of the delivery protocol to be announced within the media information.

NOTE 2: The Release FEC request is not shown on the figure.

3. The MC service server announces the MBMS bearer to the MC service client with the MBMS bearer announcement procedure, including the modified list of medias information and FEC information within the SDP information.

4. When the MC service server decides to transmit the MC service media flow for a group communication, the MC service server sends to the group a message identifying the MC service media flow and the TMGI of the MBMS bearer, such as the MapGroupToBearer message for MCPTT, specified in 3GPP TS 23.379 [16], or the MapGroupToBearer message for MCVideo, specified in 3GPP TS 23.380 [12].

5. The MC service server sends the downlink media to the BM-SC on the MB2-U reference points and according to 3GPP TS 23.468 [18].

6. The BM-SC performs FEC encoding of the downlink media in accordance to the announced FEC algorithm and parameters and delivers it over MBMS.

7. The MC service client performs FEC decoding of the encoded media flows in accordance to the announced FEC information and delivers the decoded flows to the media player.

NOTE 3: The need for a MC service server ability to turn off/on the production of repair packets on the BM-SC during the media transmission is out of scope of the present document.

10.7.3.11.3 FEC encoding by the MC service server

In this procedure, depicted in figure 10.7.3.11.3-1, FEC encoding is performed by the MC service server. The MC service server includes the FEC information within the MBMS bearer announcement. The FEC decoding is performed by the MC service client.

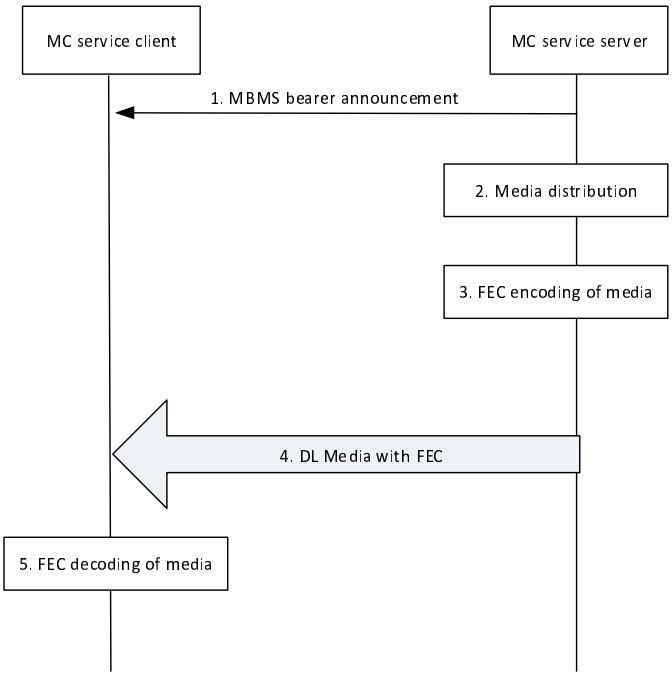

Figure 10.7.3.11.3-1: Application of FEC by the MC service server

1. The MC service server sends MBMS bearer announcement message with FEC information to the MC service clients.

2. As media packets arrive from the originating MC service UE (not shown in diagram), the media is processed by the media distribution function on the MC service server.

3. The MC service server performs FEC encoding and processing in accordance with the selected FEC algorithm.

4. The MC service server sends the media with FEC to the MC service client (both payload source packets and the FEC repair packets are sent on the MB2-U to the BM-SC, which transparently forwards them unmodified to the MC service client).

5. MC service client performs FEC decoding and processing in accordance with the selected FEC algorithm

10.7.3.12 Header compression over MBMS with ROHC

10.7.3.12.1 General

Support of ROHC over MBMS is optional for the MC service servers and MC service clients. If header compression and FEC are both applied to a communication over MBMS, the header compression shall be performed after the FEC encoding.

These procedures can be applied when using pre-established MBMS bearers (see clause 10.7.3.1) or dynamic MBMS bearers (see clause 10.7.3.2).

10.7.3.12.2 Header compression by the MC service server

In this procedure, depicted in figure 10.7.3.12.2-1, header compression is performed by the MC service server. The MC service server includes the ROHC information within the MBMS bearer announcement. The header decompression is performed by the MC service client.

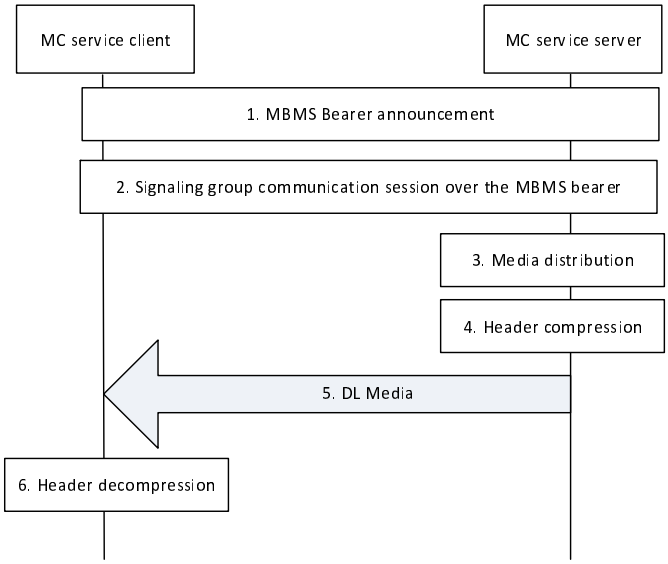

Figure 10.7.3.12.2-1: Header compression by the MC service server

1. The MC service server sends MBMS bearer announcement message with ROHC information to the MC service clients. The ROHC information contains the list of ROHC profiles and the ROHC context identifier range).
2. When the MC service server decides to transmit the MC service media flow for a group communication, the MC service server sends to the group a message identifying the MC service media flow and the TMGI of the MBMS bearer, such as the MapGroupToBearer message for MCPTT, specified in 3GPP TS 23.379 [16], or the MapGroupToBearer message for MCVideo, specified in 3GPP TS 23.281 [12].
3. As media packets arrive from the originating MC service UE (not shown in diagram), the media is processed by the media distribution function on the MC service server.
4. The MC service server performs header compression in accordance with the ROHC information.
5. The MC service server sends the header compressed media to the MC service client
6. The MC service client performs header decompression in accordance to the ROHC information

10.7.3.12.3 Header compression by the BM-SC

In this procedure, depicted in figure 10.7.3.12.3-1, the MC service server asks the BM-SC to compress headers for a set of medias, transported by a MBMS bearer, using the Setup ROHC request.

Pre-condition:

1. The MC service server has already activated a MBMS Bearer, with the MBMS Bearer request specified in 3GPP TS 23.468 [18].

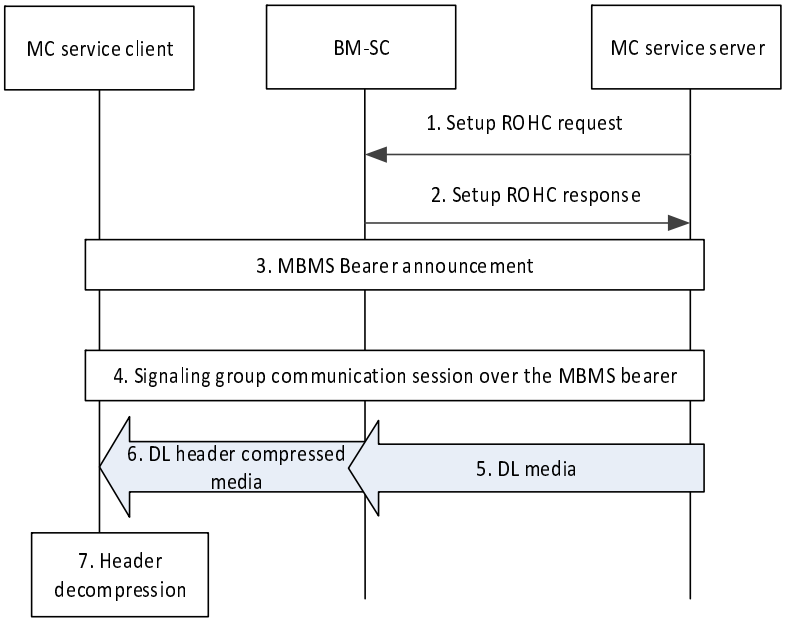

Figure 10.7.3.12.3-1: Header compression by the BM-SC

1. The MC service server decides to set up ROHC within a MBMS bearer. The request is done on the MB2-C reference point. It includes the following elements: the ROHC configuration, the list of RTP and UDP flows to be header compressed, characterized by their destination IPs and port numbers. For each of these flows, the request may indicate a target periodicity for the full header packets.

NOTE 1: The MC service server can later modify the ROHC configuration by performing again the Setup ROHC request.

NOTE 2: The Release ROHC request is also not shown on the figure.

2. If the BM-SC can satisfy the request, the Setup ROHC response confirm the application of header compression.

3. The MC service server announces the MBMS bearer to the MC service client with the MBMS bearer announcement procedure, including the ROHC information.

4. When the MC service server decides to transmit the MC service media flow for a group communication, the MC service server sends to the group a message identifying the MC service media flow and the TMGI of the MBMS bearer, such as the MapGroupToBearer message for MCPTT, specified in 3GPP TS 23.379 [16], or the MapGroupToBearer message for MCVideo, specified in 3GPP TS 23.281 [12].

5. The MC service server sends the downlink media to the BM-SC on the MB2-U reference points and according to 3GPP TS 23.468 [18].

6. The BM-SC compresses headers of the downlink media in accordance to the announced ROHC parameters and delivers it over MBMS.

7. The MC service client performs header decompression in accordance to the ROHC information.

10.7.3.13 Use of MBMS bearer for group status

The MC service server, e.g., MCPTT server, may use the MBMS bearer to inform the status of a group communication (indicating the group call is on-going or not) when the group call is set up on unicast bearers. The affiliated clients that will perform late entry chat group calls or rejoin calls may use this group status information to decide whether to join the calls. The information flows for group status notification are specified in subclause 10.7.2.12.

NOTE: The procedure described in clause 10.7.3.4 can be used for the transmission of the group status notification.

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 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. This information flow is sent individually addressed on unicast or multicast.

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 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 Void

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.
Scope of De-affiliation request	M	Indicating, whether de-affiliation is requested for this specific MC service client only, or for all MC service clients where this MC service ID has logged on.

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 system.
Scope of De-affiliation request	M	Indicating, whether de-affiliation is requested for this specific MC service client only, or for all MC service clients where this MC service ID has logged on.

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. This information flow is sent individually addressed on unicast or multicast.

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 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 Void

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. This information flow is sent individually addressed on unicast or multicast.

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.

10.8.2.13 MC service group de-affiliation notification

Table 10.8.2.13-1 describes the information flow MC service group de-affiliation notification from the MC service server to the MC service client. This information flow is sent individually addressed on unicast or multicast.

Table 10.8.2.13-1: MC service group de-affiliation notification

Information element	Status	Description
MC service ID	M	The MC service ID of the MC service user that will be de-affiliated.
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.

10.8.2.14 Notify group dynamic data request

Table 10.8.2.14-1 describes the information flow notify group dynamic data request from the MC service server to the group management server.

Table 10.8.2.14-1: Notify group dynamic data request

Information element	Status	Description
MC service group ID	M	The MC service group ID to which the GMS has subscribed and for which the group dynamic data needs to be updated.
MC service ID	M	The MC service ID for which the group dynamic data (e.g. affiliation status, de-affiliation status) needs to be updated.
Affiliation or de-affiliation status	M	Indicates the affiliation status or de-affiliation status for the MC service group ID.

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 profile and group policy from the group configuration 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; and

5. The group management server has subscribed to the MC service server within the MC system where the group is defined for affiliation status updates.

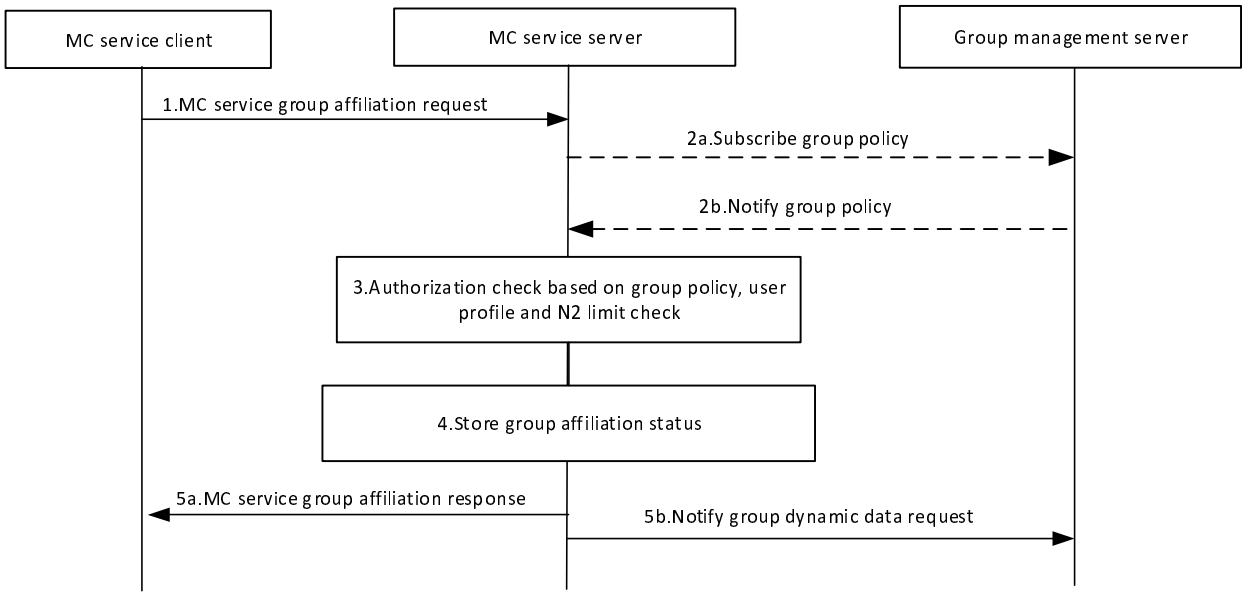

Figure 10.8.3.1-1: MC service group affiliation procedure

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 configuration from the group management server.

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

3. Based on the group policy from the group configuration and user profile, 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 system without topology hiding

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 system for a single MC service and where topology hiding is not required, it shall be subject to authorization from the partner MC

system where the MC service group(s) is defined, and whether it subjects to authorization from the primary MC 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 system where topology hiding is not required 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 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 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 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; and
6. The group management server has subscribed to the MC service server within the MC system where the group is defined for affiliation status updates.

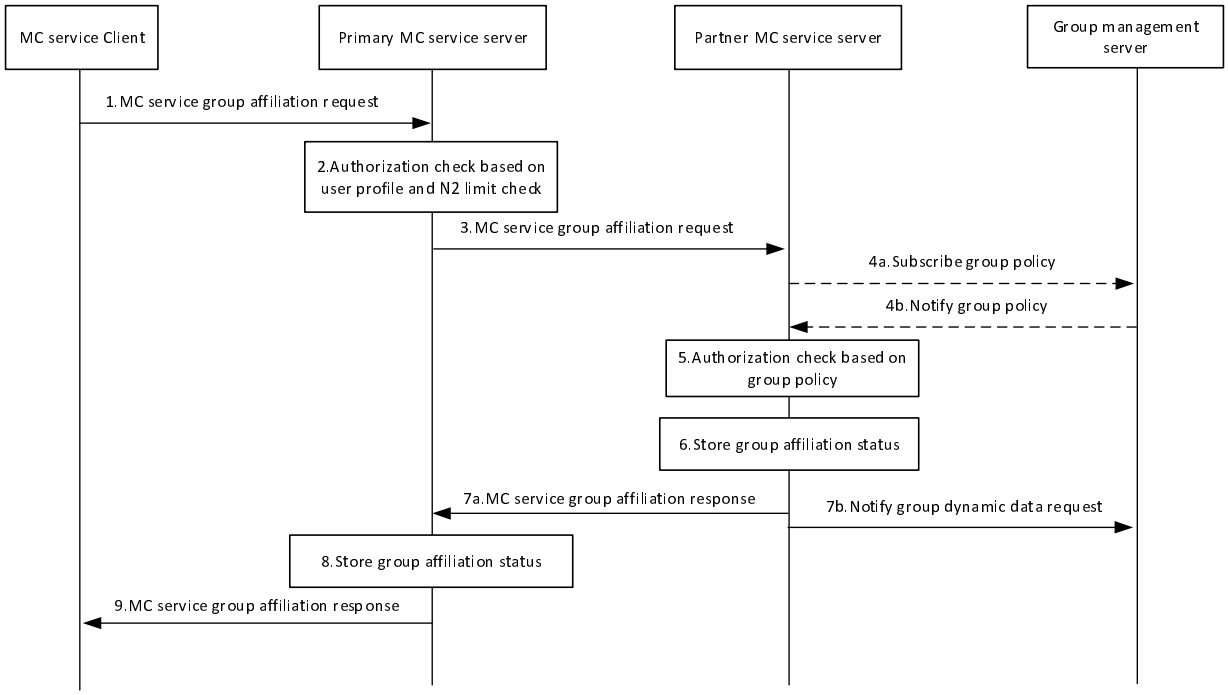

Figure 10.8.3.2.2-1: Affiliation for an MC service group defined in partner MC system where topology hiding is not required

1. The MC service client requests the MC service server of the primary MC system to affiliate to an MC service group or a set of MC service groups.
2. The MC service server of the primary MC system checks if the MC service client is authorized to affiliate to the requested MC service group(s) based on the user profile. 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 system, it determines to send group affiliation request to the corresponding MC service server of the partner MC system. The request may be routed through intermediate signalling nodes.

4a. The MC service server of the partner MC 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 configuration from the group management server.

4b. The MC service server of the partner MC system receives the group policy from the group configuration from the group management server via notification and locally caches the group policy from the group configuration.

5. Based on the group policy, the MC service server of the partner MC 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 system stores the affiliation status of the user for the requested MC service group(s).

7. The MC service server of the partner MC system sends the affiliation status result of requested MC service group(s) to the MC service server of the primary MC 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 system stores the affiliation status of the user for the requested MC service group(s).

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

10.8.3.2a Affiliation to MC service group(s) defined in partner MC system using topology hiding

10.8.3.2a.1 Functional description

When an MC service client wants to affiliate to MC service group(s) which is defined in a partner MC system for a single MC service using topology hiding, it shall be subject to authorization from the partner MC system where the MC service group(s) is defined, and may also be subject to authorization from the serving MC system of the MC service client.

10.8.3.2a.2 Procedure

Figure 10.8.3.2a.2-1 illustrates the group affiliation procedure to an MC service group defined in the partner MC system of the serving MC system of the MC service user, where topology hiding procedures are required.

Pre-conditions:

1. MC service client 1 is service authorized within its serving MC system.

2. The group host MC service server of the MC service group to which the MC service user of MC service client 1 wishes to affiliate is located in the partner MC system of the serving MC system of MC service client 1

3. Topology hiding is required by both MC systems

4. The serving MC system of MC service client 1 and the group home MC system are configured to allow topology hiding to take place.

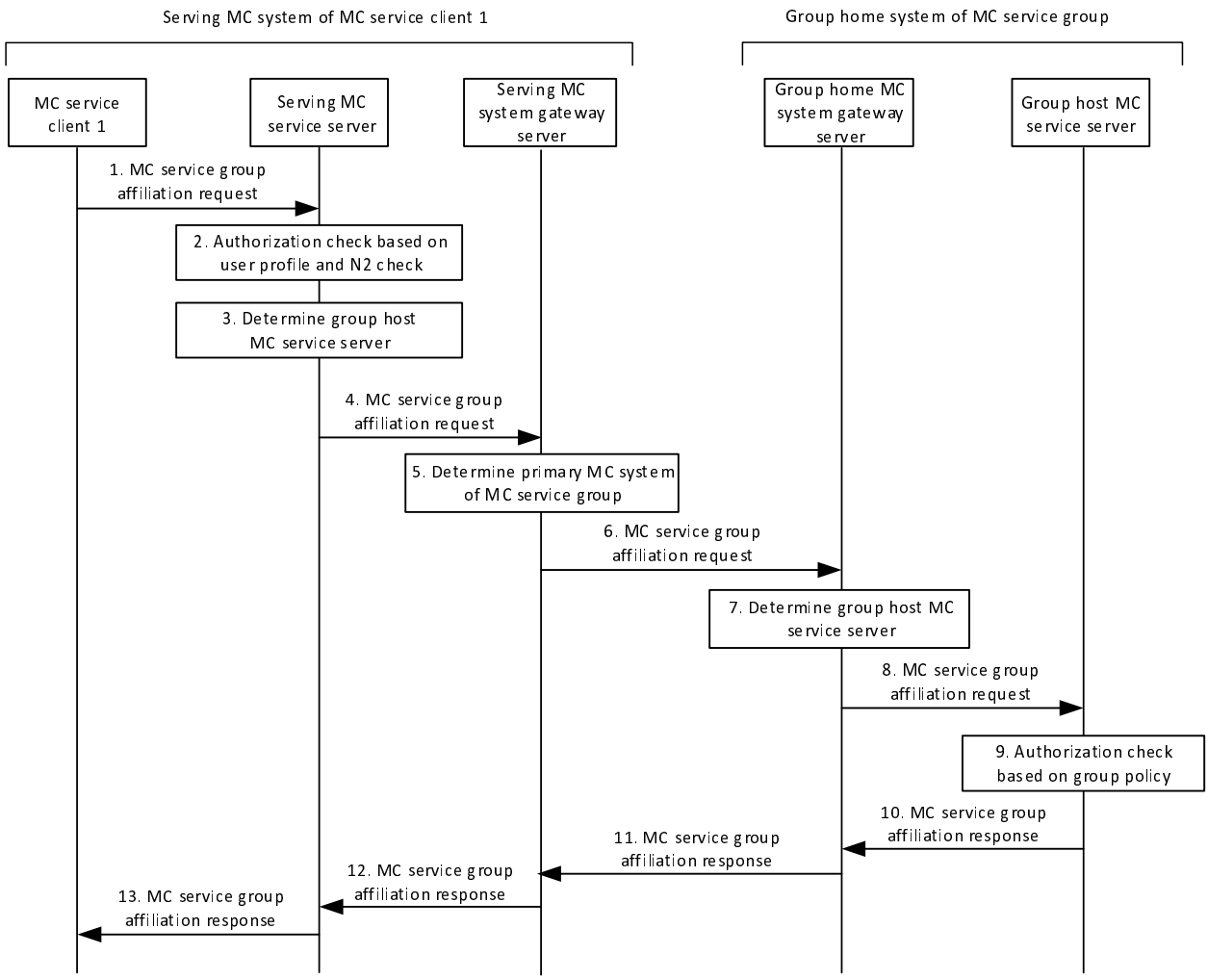

Figure 10.8.3.2a.2-1: Group affiliation to an MCservice group defined in partner MC system using topology hiding

1. MC service client 1 initiates an MC service group affiliation request to the serving MC service server of MC service client 1 on behalf of its MC service user.

2. The MC service server of the serving MC system checks that the MC service client 1 is authorized to affiliate to the requested MC service group based on the user profile, and that the maximum number of MC service groups that the user can be affiliated to (N2) has not been exceeded.

3. The MC service server determines the group host MC service server of the MC service group. The MC service group is identified to have a different group home MC system, and if topology hiding is required by the serving MC system of MC service client 1, the serving MC system gateway server is determined to act as proxy group host MC service server for the MC service group.

4. The MC service server of the serving MC system forwards the MC service group affiliation request to the gateway server of the serving MC system.

NOTE 1: If the serving MC system of MC service client 1 does not require topology hiding, the serving MC service server of MC service client 1 is able to send the MC service group affiliation request directly to the gateway server of the group home MC system in step 4, omitting steps 5 and 6.

5. The gateway server determines which MC system is the group home system for the MC service group.

6. The gateway server in the serving system of MC service client 1 forwards the MC service group affiliation request to the gateway server of the group home MC system of the MC service group.

NOTE 2: If the group home MC system does not require topology hiding, the request from the serving MC system of MC service client 1 is sent directly to the group host MC service server in either step 4 or step 6, omitting steps 7 and 8.

7. The gateway server of the group home MC system of the MC service group determines which MC service server is the group host MC service server for that MC service group.

8. The gateway server of the group home system of the MC service group forwards the MC service group affiliation request to the group host MC service server of the MC service group.

9. The group host MC service server in the partner MC system checks whether the user of MC service client 1 is authorized to affiliate to the MC service group based on the MC service group configuration. The group host MC service server may optionally subscribe to the GMS containing the group configuration information, and receive notification of group policy from the group configuration. The group host MC service server shall update the GMS with the affiliation status of the user for the requested MC service group by sending the notify group dynamic data request (not shown in the figure).

10. The group host MC service server sends an MC service group affiliation response to the gateway server in the group home MC system of the MC service group.

NOTE 3: If the group home MC system does not require topology hiding, the MC service group affiliation response is sent directly to the gateway server of the serving MC system of MC service client 1.

11. The gateway server in the group home MC system forwards the MC service group affiliation response to the gateway server in the serving MC system of MC service client 1.

NOTE 4: If the serving MC system of MC service client 1 does not require topology hiding, the MC service group affiliation response is sent directly to the serving MC service server of MC service client 1.

12. The gateway server in the serving MC system of MC service client 1 forwards the MC service group affiliation response to the serving MC service server of MC service client 1.

13. The serving MC service server of MC service client 1 forwards the MC service group affiliation response to MC service client 1.

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; and

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.

3. The group management server has subscribed to the MC service server within the MC system where the group is defined for affiliation status updates.

4. The MC service server has subscribed to the MC service functional alias controlling server within the MC system for functional alias activation/de-activation updates.

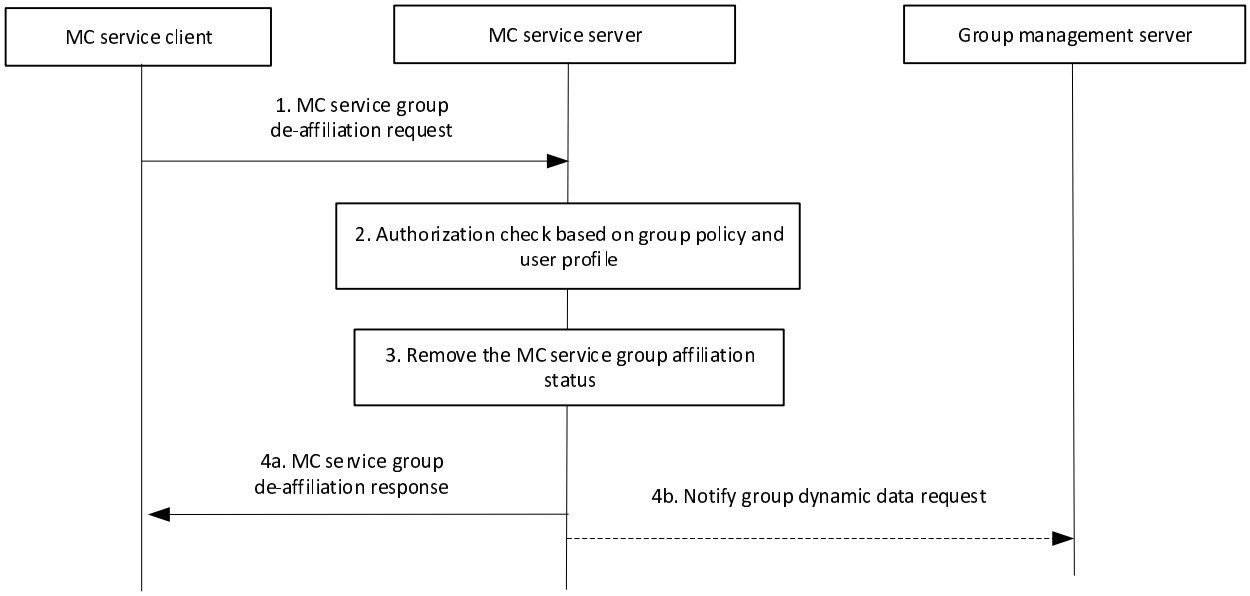

Figure 10.8.4.2-1: MC service group de-affiliation procedure

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 profile and stored group policy from the group configuration, 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). The authorisation check includes whether the MC service user has activated a certain functional alias which prevents de-affiliating or whether the MC service user is the last user who has bound a certain functional alias to the group which also prevents de-affiliating.

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), either for the requesting specific MC service client only, or for all MC service clients, where this user has logged on to.

4. MC service server provides to the MC service client the group de-affiliation response (4a). When the MC service user has logged into multiple MC service clients concurrently, the MC service server updates the group management server with the de-affiliation status of the user for the requested MC service group(s) only when the MC service ID de-affiliates for the provided MC service group(s) from the last MC service client. If the MC service user has logged into only one client then the MC service server and update 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 system

The procedure for de-affiliation from affiliated MC service group(s) which is defined in partner MC 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; and

2. The group management server has subscribed to the MC service server within the MC system where the group is defined for affiliation status updates.

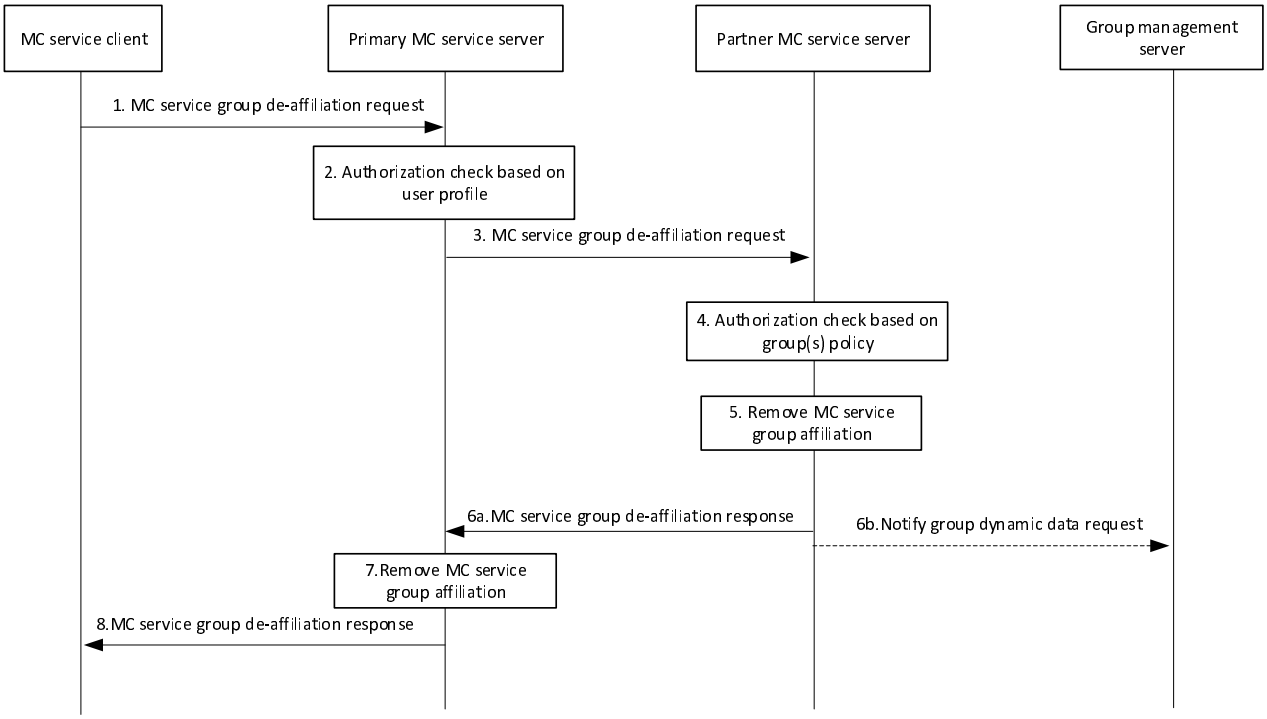

Figure 10.8.4.3-1: De-affiliation from an MC service group defined in partner MC system

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 profile. 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 from the group configuration, 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), either for the requesting specific MC service client only, or for all MC service clients, where this user has logged on to.

6. The partner MC service server sends the MC service group de-affiliation response to primary MC service server (6a) . When the MC service user has logged into multiple MC service clients concurrently, the MC service server updates the group management server with the de-affiliation status of the user for the requested MC service group(s) only when the MC service ID de-affiliates for the provided MC service group(s) from the last MC service client. If the MC service user has logged into only one client then the MC service server 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 system, considering that the user may have logged on to multiple MC service clients and that de-affiliation may have been performed only for the specific MC service client from which the de-affiliation request has been sent, or for all MC service clients, where this user has been affiliated to this MC service group.

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

10.8.4.4 MC server initiated group de-affiliation procedure

The procedure for the MC service server to trigger a de-affiliation with an MC service group is described in figure 10.8.4.4-1.

Pre-conditions:

1. The MC service user has previously affiliated to the group, and the MC service server has stored the status of MC service group affiliation;
2. Following a relevant trigger condition, e.g. the user moving outside the permitted geographical operational area of the MC service group, or the permitted geographical operational area is modified, causing user outside of the permitted geographical operational area, the MC service server de-affiliates the user from the MC service group; and
3. The group management server has subscribed to the MC service server within the MC system where the group is defined for affiliation status updates.
4. The MC service server has subscribed to the MC service functional alias controlling server within the MC system for functional alias activation/de-activation updates.

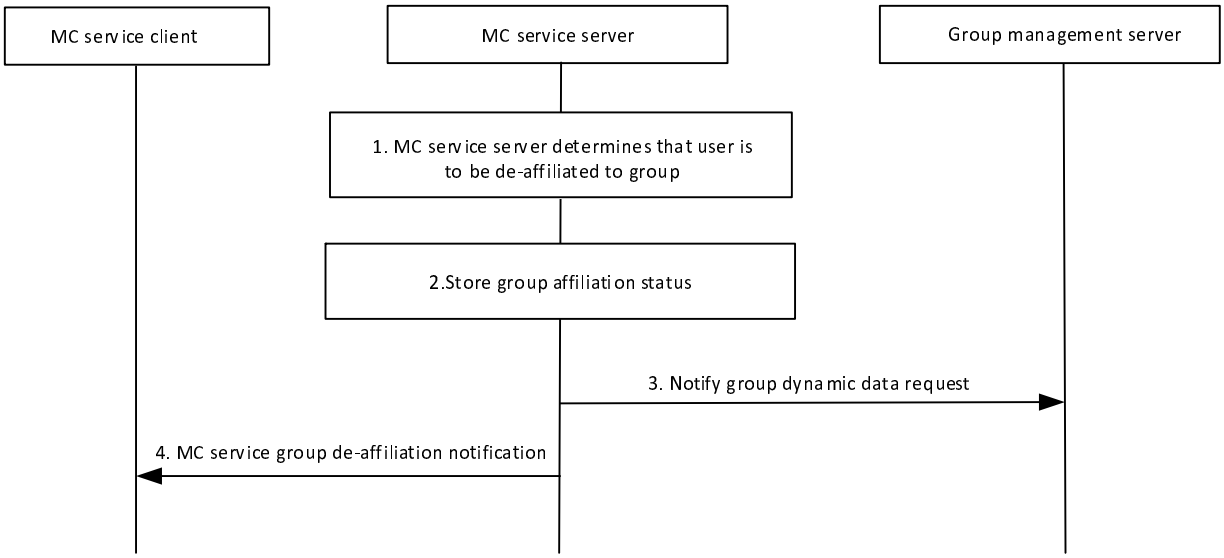

Figure 10.8.4.4-1: MC service server initiated group de-affiliation procedure

1. The MC service server determines the MC service client could be de-affiliated to the group again due to the trigger event, e.g. the permitted geographical operational area is modified, causing the user outside of the permitted geographical operational area of the MC service group, the MC service server needs to de-affiliate the MC Service user from the group.
2. The MC service server changes the affiliation status of the user.
3. The MC service server updates the group management server with the de-affiliation status of the user for the requested MC service group(s).
4. The MC service server provides a de-affiliation notification with the group information to the MC service client.

10.8.4.5 MC server initiated group de-affiliation from group defined in partner MC system

The procedure for the MC service server to trigger a de-affiliation from an MC service group which is defined in partner MC system is described in figure 10.8.4.5-1.

Pre-conditions:

1. The MC service user has previously affiliated to the group, and the MC service server has stored the status of MC service group affiliation;

2. Following a relevant trigger condition (e.g. the user moving outside the permitted geographical operational area of the MC service group, or the permitted geographical operational area is modified), the de-affiliation for the MC service user is initiated by the MC service server from the MC service group;

3. 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; and

4. The group management server has subscribed to the MC service server within the MC system where the group is defined for affiliation status updates.

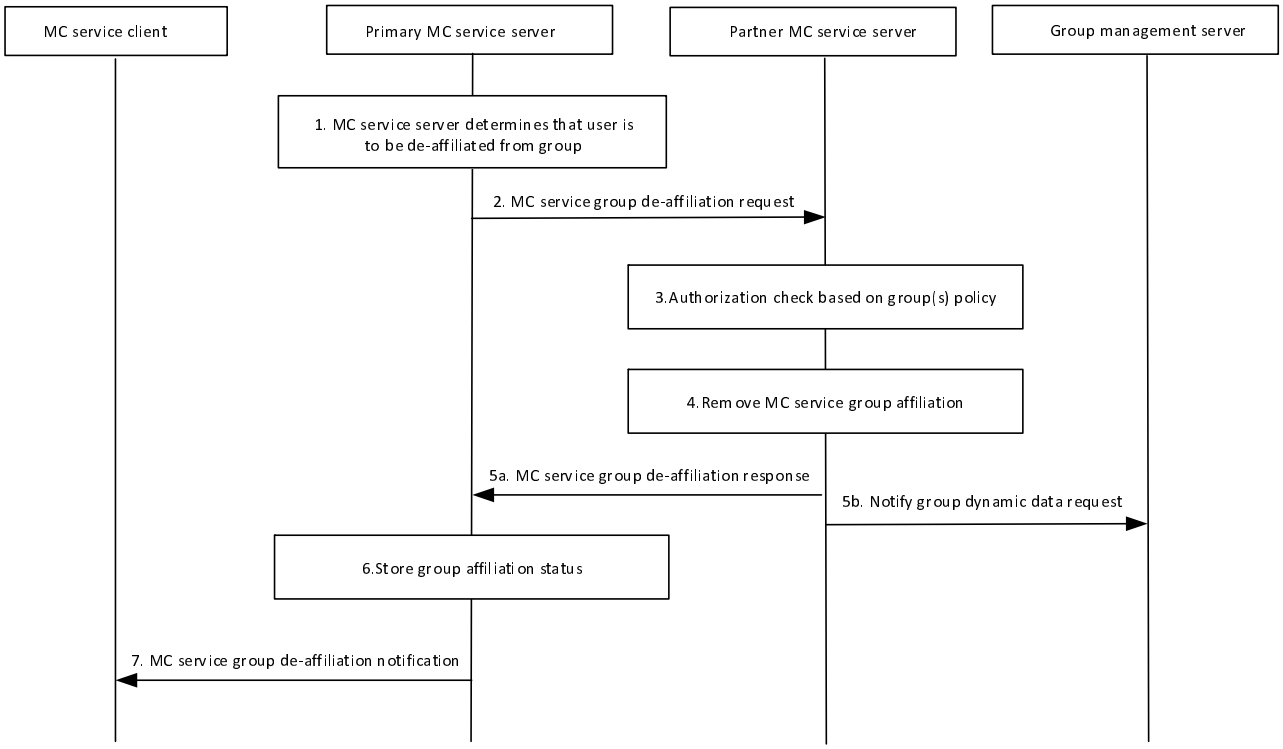

Figure 10.8.4.5-1: MC service server initiated group de-affiliation from group in partner system procedure

1. The MC service server determines the MC service client could be de-affiliated to the group due to the trigger event, e.g. the permitted geographical operational area is modified, causing the user outside of the permitted geographical operational area of the MC service group, the MC service server needs to de-affiliate the MC Service user from the group.

2. Based on the stored MC service group information, 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.

3. Based on the stored group policy from the group configuration, 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).

4. 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).

5. The partner MC service server sends the MC service group de-affiliation response to primary MC service server (5a) and updates the group management server with the de-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.

6. The primary MC service server changes the affiliation status of the user.

7. The MC service server provides a de-affiliation notification with the group information 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 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:

1. 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;

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

3. The group management server has subscribed to the MC service server within the MC system where the group is defined for affiliation status updates.

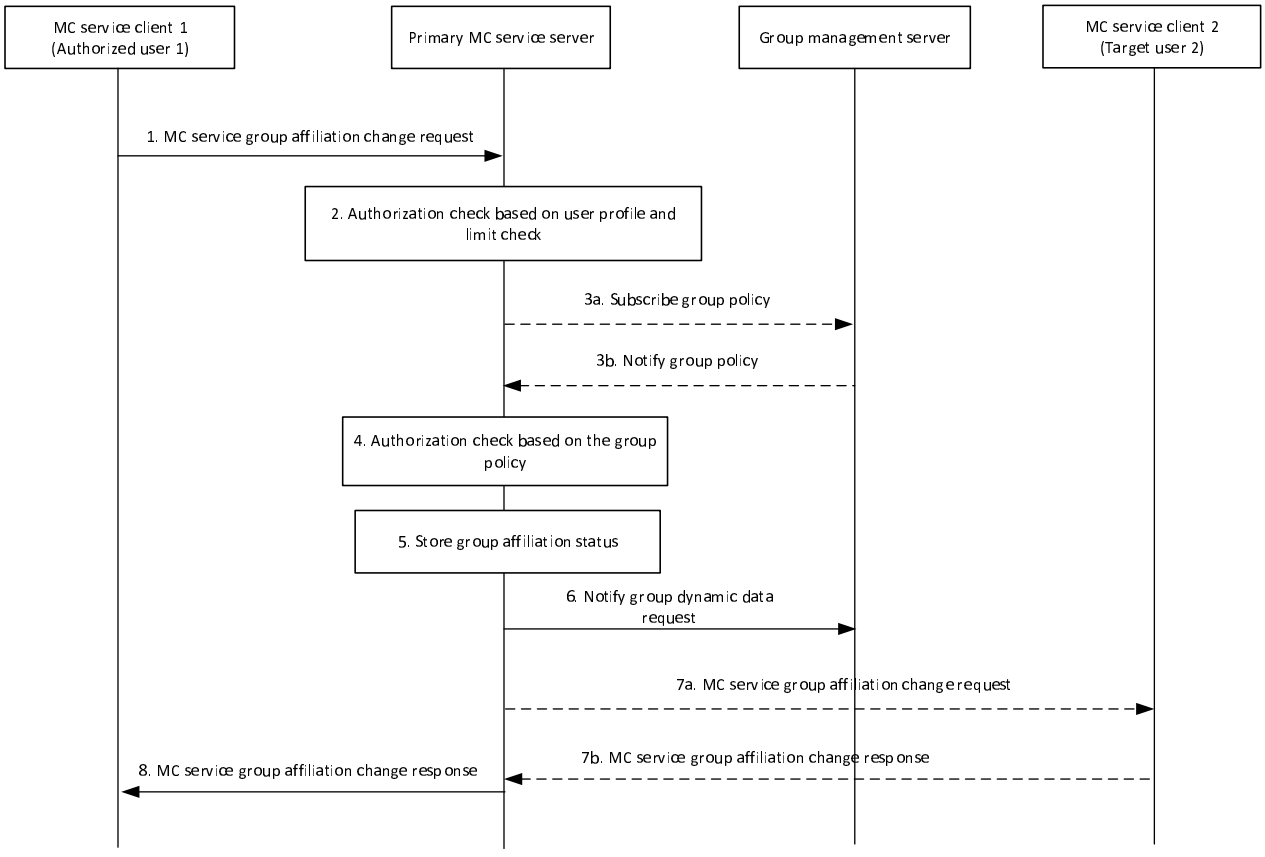

Figure 10.8.5.1.1-1: Remotely change MC service group affiliation – mandatory mode

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 profile. 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 configuration from the group management server.

3b. The primary MC service server receives the group policy from the group configuration from the group management server via notification and locally caches the group policy from the group configuration.

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 profile or group policy from the group configuration e.g. information regarding user(s) authorization to affiliate or to de-affiliate to MC service group(s), priority, and other related configuration data.

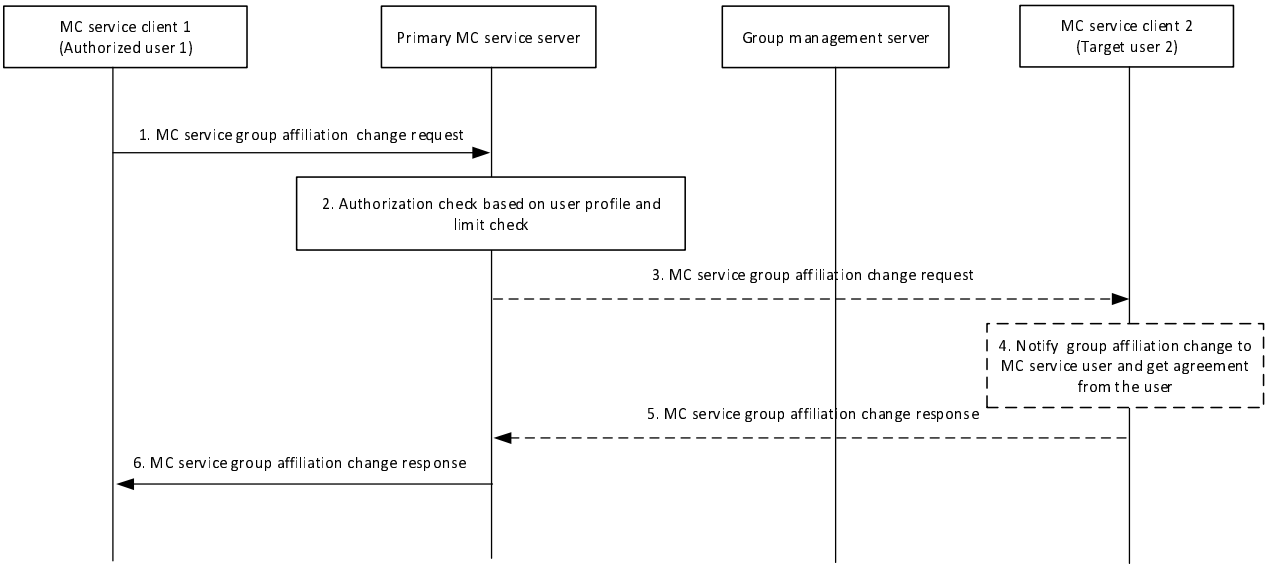

Figure 10.8.5.1.2-1: Remotely change MC service group affiliation – negotiated mode

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 profile and the group policy from the group configuration (i.e. if not available, the primary MC service server obtains the group policy from the group configuration 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 systems, the primary MC service server performs the affiliation or de-affiliation procedures by interacting with the partner MC 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 systems, the primary MC service server can wait until all the partner MC systems provides the MC service group affiliation change response messages.

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

10.8.5.2.1 Authorized user remotely changes another MC service user's affiliated MC service group(s) defined in partner MC 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 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:

1. 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;
2. 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 system;
3. The partner MC service server may have retrieved the group related information from the group management server;
4. 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; and
5. The partner group management server has subscribed to the MC service server within the MC system where the group is defined for affiliation status updates.

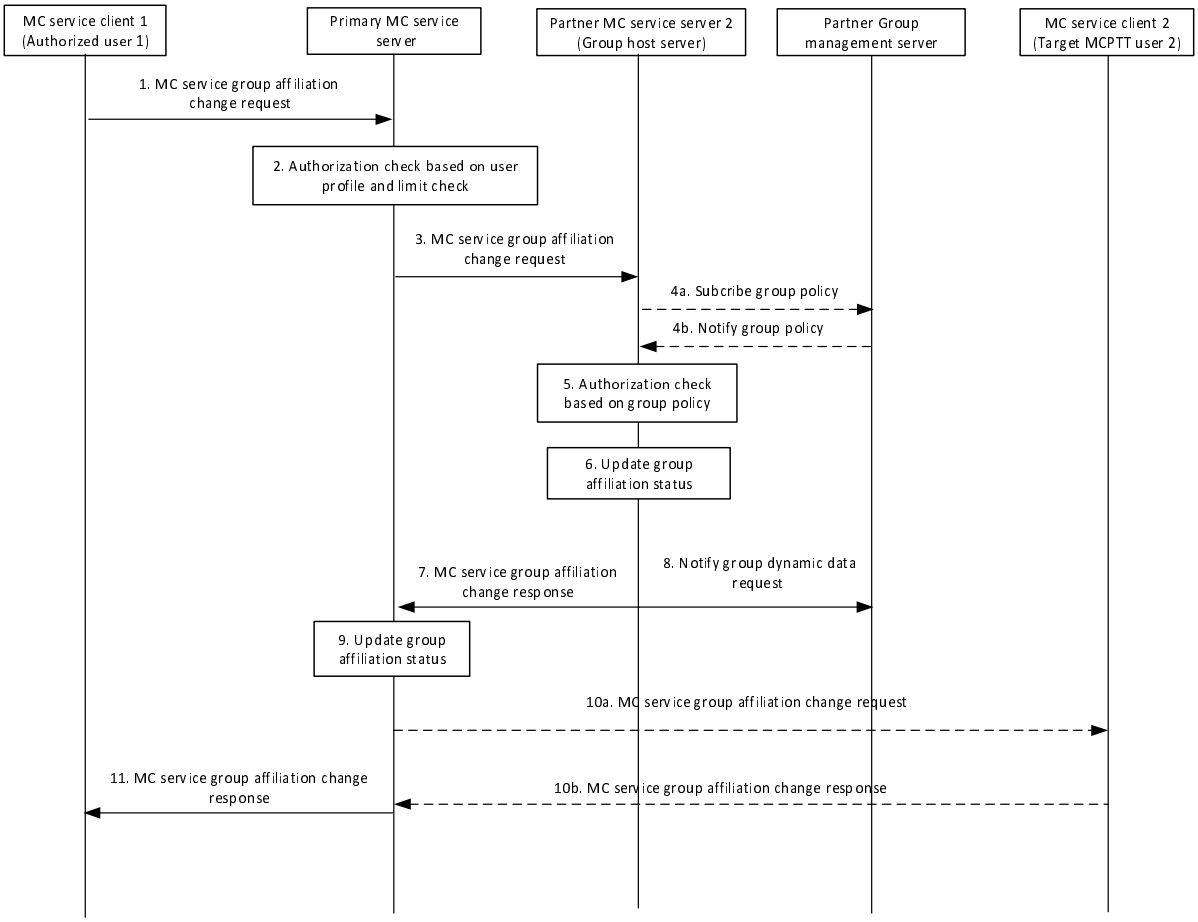

Figure 10.8.5.2.1-1: Remote change MC service group affiliation defined in partner MC system – mandatory mode

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 profile. 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 configuration from the group management server.

4b. The partner MC service server receives the group policy from the group configuration from the group management server via notification and locally caches the group policy from the group configuration.

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 sends the MC service group affiliation change response to the primary MC service server.

8. 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).

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.

The location management client can be configured to store location information while not reporting location information to the location management server. The location management client may report stored location information to the location management server.

NOTE: Configuration and location information transmission may occur while there is a communication link between the location management client and location management server.

In the information flows of clause 10.9.2, and procedures of clause 10.9.3:

- the term "requesting MC service user" is used to refer to the MC service user which sends a request to subscribe to location information reports, to trigger a location information report or to modify existing location information triggers from another MC service user;
- the term "requested MC service user" is used to refer to the MC service user whose location information is requested or existing location information triggers are to be modified; and
- the term "reporting MC service user" is used to refer to the MC service user which provides location related information based on on-demand request or trigger criteria.

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 (see NOTE 1)	Identifies what location information is requested, except for emergency or imminent peril calls or emergency alerts
Requested emergency location information	O (see NOTE 1)	Identifies what location information is requested, for emergency or imminent peril calls or emergency alerts
Triggering criteria in non-emergency cases	O (see NOTE 1)	Identifies when the location management client will send the location report in non-emergency cases
Handling criteria in not reporting location information cases	O	Identifies when the location management client will store location information (e.g. never, off-network, IOPS)
Triggering criteria in not reporting location information cases	O (see NOTE 2)	Identifies the causes when the location management client will generate location information
Minimum time between consecutive reports	O (see NOTE 1)	Defaults to 0 if absent and 0 for emergency calls, imminent peril calls and emergency alerts
Triggering criteria in emergency cases	O (see NOTE 1)	Identifies when the location management client will send the location report in emergency cases
NOTE 1: If none of the information elements is present, this represents a cancellation for location reporting based on Triggering criteria in emergency and non-emergency cases, if configured. NOTE 2: If not present, location information is generated based on Triggering criteria in emergency and non-emergency cases, if configured.		

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 (LMC – LMS)

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)
MC service ID (see NOTE 4)	O	Identity of the requesting MC service user.
Functional alias(es) (see NOTE 1)	O	Functional alias that corresponds to the reporting MC service ID.
Functional alias	O	Functional alias that corresponds to the requesting MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
MC service UE label	O	Generic name of the reporting MC service UE
Triggering event (see NOTE 3)	M	Identity of the event that triggered the sending of the report
Location Information (see NOTE 2)	M	Location information of the individual MC service user
NOTE 1: Each functional alias corresponds to an individual MC service ID. NOTE 2: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided. NOTE 3: An on-demand request may be the triggering event. NOTE 4: In case of an on-demand request of an MC service user the MC service ID shall be provided. In case of an MC service server request or an event-triggered report, no MC service ID is provided.		

Table 10.9.2.2-2 describes the information flow from the location management server to the location management client for location information reporting.

Table 10.9.2.2-2: Location information report (LMS – LMC)

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)
MC service ID	M	Identity of the requesting MC service user.
Functional alias(es) (see NOTE 1)	O	Functional alias that corresponds to the reporting MC service ID.
Functional alias	O	Functional alias that corresponds to the requesting MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
MC service UE label	O	Generic name of the reporting MC service UE
Triggering event (see NOTE 3)	M	Identity of the event that triggered the sending of the report
Location Information (see NOTE 2)	M	Location information of the individual MC service user
NOTE 1: Each functional alias corresponds to an individual MC service ID. NOTE 2: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided. NOTE 3: An on-demand request may be the triggering event.		

Table 10.9.2.2-3 describes the information flow from the location management server to the MC service server for location information reporting.

Table 10.9.2.2-3: Location information report (LMS – MC service server)

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)
Functional alias(es) (see NOTE 1)	O	Functional alias that corresponds to the MC service ID.
Triggering event (see NOTE 3)	M	Identity of the event that triggered the sending of the report
Location Information (see NOTE 2)	M	Location information of the individual MC service user
NOTE 1: Each functional alias corresponds to an individual MC service ID. NOTE 2: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided. NOTE 3: An on-demand request may be the triggering event.		

Table 10.9.2.2-4 describe the information flow to support the handling of location information across MC systems.

Table 10.9.2.2-4: Location information report (LMS – LMS)

Information element	Status	Description
MC service ID	M	Identity of the reporting MC service user at partner MC system
Functional alias	O (see NOTE 1)	Functional alias of the reporting MC service user at partner MC system
MC service ID	M (see NOTE 2)	Identity of the requesting MC service user at primary MC system
Functional alias	O (see NOTE 2)	Functional alias of the requesting MC service user at primary MC system
MC service UE label	O	Generic name of the reporting MC service UE at partner MC system
Triggering event (see NOTE 3)	M	Identity of the event that triggered the sending of the report
Location Information (see NOTE 4)	M	Location information of the individual MC service user at partner MC system
NOTE 1: It shall be present if used with the Functional alias associated request. NOTE 2: Only present, if provided with the associated request. NOTE 3: An on-demand request may be the triggering event. NOTE 4: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided.		

10.9.2.3 Location information request

Tables 10.9.2.3-1, 10.9.2.3-2 and 10.9.2.3-3 describe the information flow from the MC service server to the location management server and from the location management server to the location management client and from location management client to location management server respectively for requesting an immediate location information report.

Table 10.9.2.3-1: Location information request (MC service server to location management server)

Information element	Status	Description
MC service ID list	O (see NOTE)	List of MC service users whose location information is requested
Functional alias	O (see NOTE)	Location information of MC service users who have activated this functional alias is requested
NOTE: Either the MC service ID list or the functional alias must be present.		

Table 10.9.2.3-2: Location information request (Location management server to location management client)

Information element	Status	Description
MC service ID	M	Identity of MC service user whose location information is requested
MC service ID	O	Identity of the requesting MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
Functional alias	O	Functional alias that corresponds to the requested MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
Functional alias	O	Functional alias that corresponds to the requesting MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)

Table 10.9.2.3-3: Location information request (Location management client to location management server)

Information element	Status	Description
MC service ID	M	Identity of the requesting authorized MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
MC service ID list	O (see NOTE)	List of MC service users whose location information is requested
Functional alias	O	Functional alias that corresponds to the requesting MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
Functional alias	O (see NOTE)	Functional alias that corresponds to the requested MC service user(s) (e.g. MCPTT ID, MCVideo ID, MCData ID)
NOTE: Either the MC service ID list or the functional alias must be present.		

Tables 10.9.2.3-4 describe the information flow to support the handling of location information across MC systems.

Table 10.9.2.3-4: Location information request (Location management server to location management server)

Information element	Status	Description
MC service ID	M (see NOTE 1)	Identity of the requesting authorized MC service user at primary MC system
Functional alias	O (see NOTE 1)	Functional alias that corresponds to the requesting MC service user at primary MC system
MC service ID list	O (see NOTE 2)	List of identities of those MC service users at partner MC system whose location information are requested
Functional alias	O (see NOTE 2)	Functional alias of those MC service users at partner MC system whose location information are requested
NOTE 1: Only present if Location information client has initiated the request. NOTE 2: Either the MC service ID list or the functional alias must be present.		

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 (see NOTE 1)	Identity of the requesting authorized MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
Functional alias	O	Functional alias that corresponds to the requesting MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
MC service ID	O (see NOTE 1) (see NOTE 3)	Identity of the requested MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
Functional alias	O (see NOTE 3)	Functional alias that corresponds to the requested MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID).
Immediate Report Indicator	O (see NOTE 2)	Indicates whether an immediate location report is required
Requested non-emergency location information	O (see NOTE 2)	Identifies what location information is requested, except for emergency or imminent peril calls or emergency alerts
Requested emergency location information	O (see NOTE 2)	Identifies what location information is requested, for emergency or imminent peril calls or emergency alerts
Triggering criteria in non-emergency cases	O (see NOTE 2)	Identifies when the client will send the location report in non-emergency cases
Triggering criteria in emergency cases	O (see NOTE 2)	Identifies when the client will send the location report in emergency cases
Minimum time between consecutive reports	O (see 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 shall 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 shall be an MCPTT ID. NOTE 2: At least one of these rows shall be present. NOTE 3: Either the MC service ID or the functional alias must 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 (MC service server – LMS)

Information element	Status	Description
MC service ID list	M	List of MC service users whose location information is requested
Time between consecutive reports	M (see NOTE)	Indicates the interval time between consecutive reports. The provided time is to be used for all MC service IDs provided in the MC service ID list.
NOTE: If the interval time has a value of zero then the location management server will send the Location information notification immediately the location information report is received from the MC service user in the MC service ID list.		

Table 10.9.2.5-2 describes the information flow from the location management client to the location management server for location information subscription request.

Table 10.9.2.5-2: Location information subscription request (LMC – LMS)

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 (see NOTE)	Indicates the interval time between consecutive reports. The provided time is to be used for all MC service IDs provided in the MC service ID list.
NOTE: If the interval time has a value of zero then the location management server will send the Location information notification immediately the location information report is received from the MC service user in the MC service ID list.		

Table 10.9.2.5-3 describes the information flow from the location management server in the primary MC system to the location management server in the partner MC system for the location information subscription request.

Table 10.9.2.5-3: Location information subscription request (LMS – LMS)

Information element	Status	Description
MC service ID (see NOTE 1)	M	Identity of the requesting MC service user in the primary MC system
MC service ID list	M	List of the identities of MC service users in the partner MC system whose location information are requested
Time between consecutive location notifications (see NOTE 2)	M	Indicates the interval time between consecutive location notifications
NOTE 1: This element is only present when the request is originated by an MC service client. NOTE 2: If the interval time has a value of zero then the location management server will send the location information notification immediately after the location information update is received from the MC service user in the MC service ID list.		

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 or location management client and from the location management server in the partner MC system to the location management server in the primary MC system for the location information subscription response.

Table 10.9.2.6-1: Location information subscription response

Information element	Status	Description
MC service ID (see NOTE 1)	M	Identity of the requesting MC service user
Subscription status (see NOTE 2)	M	Indicates the subscription result
NOTE 1: This element is only present when the associated request was originated by an MC service client. NOTE 2: The subscription status provides the status for each MC service ID listed with the associated request.		

10.9.2.7 Location information notification

Table 10.9.2.7-1 and Table 10.9.2.7-2 describe the information flows from the location management server to the MC service server and from the location management server to the location management client.

Table 10.9.2.7-1: Location information notification (LMS to MC service server)

Information element	Status	Description
MC service ID	M	Identity of the MC service user whose location information is being notified
Triggering event	M	Identity of the event that triggered the sending of the notification
Location Information (see NOTE)	M	Location information
NOTE: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided.		

Table 10.9.2.7-2: Location information notification (LMS to LMC)

Information element	Status	Description
MC service ID	M	Identity of the MC service user whose location information is being notified
Functional alias	O	Functional alias that corresponds to the MC service user whose location information is being notified
MC service ID	M	Identity of the MC service user subscribed to location information
Triggering event	M	Identity of the event that triggered the sending of the notification
Location Information (see NOTE)	M	Location information
MC service UE label	O	Generic name of the reporting MC service UE
NOTE: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided.		

Table 10.9.2.7-3 describes the information flow from the location management server in the partner MC system to the location management server in the primary MC system.

Table 10.9.2.7-3: Location information notification (LMS to LMS)

Information element	Status	Description
MC service ID	M	Identity of the MC service user whose location information is being notified
Functional alias	O	Functional alias that corresponds to the MC service user whose location information is being notified
Triggering event	M	Identity of the event that triggered the sending of the notification
Location Information (see NOTE)	M	Location information
MC service UE label	O	Generic name of the reporting MC service UE
NOTE: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided.		

10.9.2.8 Location information cancel subscription request

Table 10.9.2.8-1 describes the information flow from the MC service server to the location management server for location information cancel subscription request.

Table 10.9.2.8-1: Location information cancel subscription request (MC service server to location management server)

Information element	Status	Description
MC service ID list	M	List of identities of the MC service users for whom location information is no longer required

Table 10.9.2.8-2 describes the information flow from the location management client to the location management server for location information cancel subscription request.

Table 10.9.2.8-2: Location information cancel subscription request (Location management client to location management server)

Information element	Status	Description
MC service ID (see NOTE 1)	M	Identity of the requesting MC service user
MC service ID (see NOTE 2)	O	Identity of the MC service user, whose subscription is to be cancelled
MC service ID list	M	List of identities of the MC service users for whom location information is no longer required
NOTE 1: Authorized or subscribed MC service user. NOTE 2: Only used with the authorized MC service user.		

Table 10.9.2.8-3 describes the information flow from the location management server in the primary MC system to the location management server in the partner MC system for the location information cancel subscription request.

Table 10.9.2.8-3: Location information cancel subscription request (Location management server to location management server)

Information element	Status	Description
MC service ID (see NOTE 1)	M	Identity of the requesting MC service user in the primary MC system
MC service ID (see NOTE 2)	O	Identity of the MC service user in the partner MC system, whose subscription is to be cancelled
MC service ID list	M	List of the identities of MC service users in the partner MC system for whom location information is no longer required
NOTE 1: Authorized or subscribed MC service user and only present when the request was originated by an MC service client. NOTE 2: Only used with the authorized MC service user.		

10.9.2.9 Location information cancel subscription response

Table 10.9.2.9-1 describes the information flow from the location management server to the MC service server for location information cancel subscription response.

Table 10.9.2.9-1: Location information cancel subscription response (Location management server to MC service server)

Information element	Status	Description
MC service ID list	M	List of identities of MC service users, whose subscription has been requested to be cancelled
Subscription cancel response	M	Indicates the cancel subscription result

Table 10.9.2.9-2 describes the information flow from the location management server to the location management client for location information cancel subscription response.

Table 10.9.2.9-2: Location information cancel subscription response (Location management server to location management client)

Information element	Status	Description
MC service ID	M	Identity of the requesting MC service user
MC service ID (see NOTE)	O	Identity of the MC service user, whose subscription has been requested to be cancelled
MC service ID list	M	List of identities of MC service users for whom location information is no longer required
Subscription cancel response	M	Indicates the cancel subscription result
NOTE: Only used with the authorized MC service user. Must be present, if used with the associated request.		

Table 10.9.2.9-3 describes the information flow from the location management server in the partner MC system to the location management server in the primary MC system for location information cancel subscription response.

Table 10.9.2.9-3: Location information cancel subscription response (Location management server to location management server)

Information element	Status	Description
MC service ID (see NOTE 1)	M	Identity of the requesting MC service user in the primary MC system
MC service ID (see NOTE 2)	O	Identity of the MC service user in the partner MC system, whose subscription has been requested to be cancelled
MC service ID list	M	List of identities of MC service users in the partner MC system for whom location information is no longer required
Subscription cancel response (see NOTE 3)	M	Indicates the cancel subscription result
NOTE 1: This element is only present when the associated request was originated by an MC service client. NOTE 2: Only used with the authorized MC service user. Must be present, if used with the associated request. NOTE 3: Provides the status for each MC service ID listed with the associated request.		

10.9.2.10 Location report response

Table 10.9.2.10-1 describes the information flow from the location management server to the requesting location management client for the location information reporting when using functional alias.

Table 10.9.2.10-1: Location report response

Information element	Status	Description
MC service ID	M	Identity of the reporting MC service user whose location information is requested
MC service ID	M	Identity of the MC service user who requested the location information based on a provided functional alias
Functional alias	O	Functional alias that corresponds to the MC service ID of the reporting MC service user
Triggering event	M	Identity of the event that triggered the sending of the report
Location Information (see NOTE)	M	Location information for the corresponding functional alias and its MC service ID
MC service UE label	O	Generic name of the reporting MC service UE
NOTE: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided.		

10.9.2.11 Location information history status request

Table 10.9.2.11-1 describes the information flow from the location management client to the location management server to request the status of stored location information, following a return to report location information to the location management server.

Table 10.9.2.11-1: Location information history status request (LMC – LMS)

Information element	Status	Description
MC service ID	M	Identity of the MC service user from whom status is requested
MC service ID	M	Identity of the MC service user, who has requested the status

Table 10.9.2.11-2 describes the information flow from the location management server to the location management client to request the status of stored location information, following a return to report location information to the location management server.

Table 10.9.2.11-2: Location information history status request (LMS – LMC)

Information element	Status	Description
MC service ID	M	Identity of the MC service user from whom status is requested

Table 10.9.2.11-3 describes the information flow from the MC service server to the location management server to request the status of stored location information, following a return to report location information to the location management server.

Table 10.9.2.11-3: Location information history status request (MC service server – LMS)

Information element	Status	Description
MC service ID	M	Identity of the MC service user from whom status is requested
MC service ID	O	Identity of the MC service user, who has requested the status

10.9.2.12 Location information history status report

The location management client stored location information, while not reporting location information to the location management server, and subsequently the reporting may start following the reestablishment of a communication link between the location management client and the location management server.

Table 10.9.2.12-1 describes the information flow from the location management client to the location management server to report the status of stored location information.

Table 10.9.2.12-1: Location information history status report (LMC – LMS)

Information element	Status	Description
MC service ID list	M	List of identities (e.g. MCPTT ID, MCData ID, MCVideo ID) of the MC service user who reports the status
Number of stored reports	O	Indicates either zero or the number of available reports
Start time	O	First time of measurement of the available reports
End time	O	Last time of measurement of the available reports
Triggered event list (see NOTE)	M	Identifies the criteria when the location management client generated location information, while not reporting location information
NOTE: Each triggered criterion is shown once with either the associated Number of stored reports, or with the associated Start time, or with the associated Start time and End time or with the associated End time.		

Table 10.9.2.12-2 describes the information flow from the location management server to the location management client to report the status of stored location information.

Table 10.9.2.12-2: Location information history status report (LMS – LMC)

Information element	Status	Description
MC service ID	M	Identity of the MC service user who reports the status
MC service ID	M	Identity of the MC service user to receive the status report
Number of stored reports	O	Indicates either zero or the number of available reports
Start time	O	First time of measurement of the available reports
End time	O	Last time of measurement of the available reports
Triggered event list (see NOTE)	M	Identifies the criteria when the location management client generated location information, while not reporting location information
NOTE: Each triggered criterion is shown once with either the associated Number of stored reports, or with the associated Start time, or with the associated Start time and End time or with the associated End time.		

Table 10.9.2.12-3 describes the information flow from the location management server to the MC service server to report the status of stored location information.

Table 10.9.2.12-3: Location information history status report (LMS - MC service server)

Information element	Status	Description
MC service ID	M	Identity of the MC service user who reports the status
Number of stored reports	O	Indicates either zero or the number of available reports
Start time	O	First time of measurement of the available reports
End time	O	Last time of measurement of the available reports
Triggered event list (see NOTE)	M	Identifies the criteria when the location management client generated location information, while not reporting location information
NOTE: Each triggered criterion is shown once with either the associated Number of stored reports, or with the associated Start time, or with the associated Start time and End time or with the associated End time.		

10.9.2.13 Location information history request

The location management client stored location information, while not reporting location information to the location management server, and subsequently the reporting may start following the reestablishment of a communication link between the location management client and the location management server. Either all or a subset of the stored location information may be requested prior to the location information history reporting.

Table 10.9.2.13-1 describes the information flow from the location management client to the location management server for the location information history request of stored location information.

Table 10.9.2.13-1: Location information history request (LMC – LMS)

Information element	Status	Description
MC service ID	M	Identity of the MC service user from whom reports are requested
MC service ID	M	Identity of the MC service user who requests location information
Number of stored reports (see NOTE)	O	Indicates the number of requested reports
Start time (see NOTE)	O	Indicates to send reports having this time of measurement and newer
End time (see NOTE)	O	Indicates to send reports having this time of measurement and older
Triggered event list (see NOTE)	O	Identifies the criteria when the location management client generated location information, while not reporting location information
Minimum time between consecutive reports	O	Defaults to 0 if absent
NOTE: If none of these information elements is present, all stored location information shall be reported. Information elements may combined to request a subset of the available location information.		

Table 10.9.2.13-2 describes the information flow from location management server to the location management client for the location information history request of stored location information.

Table 10.9.2.13-2: Location information history request (LMS – LMC)

Information element	Status	Description
MC service ID	M	Identity of the MC service user from whom reports are requested
Number of stored reports (see NOTE)	O	Indicates the number of requested reports
Start time (see NOTE)	O	Indicates to send reports having this time of measurement and newer
End time (see NOTE)	O	Indicates to send reports having this time of measurement and older
Triggered event list (see NOTE)	O	Identifies the criteria when the location management client generated location information, while not reporting location information
Minimum time between consecutive reports	O	Defaults to 0 if absent
NOTE: If none of these information elements is present, all stored location information shall be reported. Information elements may combined to request a subset of the available location information.		

Table 10.9.2.13-3 describes the information flow from the MC service server to the location management server for the location information history request of stored location information.

Table 10.9.2.13-3: Location information history request (MC service server – LMS)

Information element	Status	Description
MC service ID	M	Identity of the MC service user from whom reports are requested
Number of stored reports (see NOTE)	O	Indicates the number of requested reports
Start time (see NOTE)	O	Indicates to send reports having this time of measurement and newer
End time (see NOTE)	O	Indicates to send reports having this time of measurement and older
Triggered event list (see NOTE)	O	Identifies the criteria when the location management client generated location information, while not reporting location information
Minimum time between consecutive reports	O	Defaults to 0 if absent
NOTE: If none of these information elements is present, all stored location information shall be reported. Information elements may combined to request a subset of the available location information.		

10.9.2.14 Location information history report

The location management client stored location information, while not reporting location information to the location management server, and subsequently the reporting may start following the reestablishment of a communication link between the location management client and the location management server.

Table 10.9.2.14-1 describes the information flow from the location management client to the location management server for the location information history reporting of stored location information.

Table 10.9.2.14-1: Location information history report (LMC – LMS)

Information element	Status	Description
MC service ID list	M	List of identities of the reporting MC service user (e.g. MCPTT ID, MCData ID, MCVideo ID)
Triggered event	M	Identifies the criterion when the location management client generated location information, while not reporting location information
Location Information (see NOTE 1)	M	Location information
MC service UE label	O	Generic name of the reporting MC service UE
History report (see NOTE 2)	O	Location information history report indicator
NOTE 1: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided. NOTE 2: Only present, if triggering criteria in emergency cases or triggering criteria in non-emergency cases used.		

Table 10.9.2.14-2 describes the information flow from the location management server to the location management client for the location information history reporting of stored location information.

Table 10.9.2.14-2: Location information history report (LMS – LMC)

Information element	Status	Description
MC service ID	M	Identity of the reporting MC service user
MC service ID	M	Identity of the MC service user, who has requested location information
Triggered event	M	Identifies the criterion when the location management client generated location information, while not reporting location information
Location Information (see NOTE 1)	M	Location information
MC service UE label	O	Generic name of the reporting MC service UE
History report (see NOTE 2)	O	Location information history report indicator
NOTE 1: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided. NOTE 2: Only present, if triggering criteria in emergency cases or triggering criteria in non-emergency cases used.		

Table 10.9.2.14-3 describes the information flow from the location management server to the MC service server for the location information history reporting of stored location information.

Table 10.9.2.14-3: Location information history report (LMS - MC service server)

Information element	Status	Description
MC service ID	M	Identity of the reporting MC service user
Triggered event	M	Identifies the criterion when the location management client generated location information, while not reporting location information
Location Information (see NOTE 1)	M	Location information
History report (see NOTE 2)	O	Location information history report indicator
NOTE 1: This may contain multiple sets of elements for the MC service user. The following elements shall accompany the location information elements: time of measurement and optional accuracy. The following location information elements shall be optional (configurable) present: longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs, with at least one provided. NOTE 2: Only present, if triggering criteria in emergency cases or triggering criteria in non-emergency cases used.		

10.9.2.15 Location information history cancel request

Table 10.9.2.15-1 describes the information flow from the location management client to the location management server for the cancellation request of location information history reporting.

Table 10.9.2.15-1: Location information history cancel request (LMC – LMS)

Information element	Status	Description
MC service ID	M	Identity of the reporting MC service user
MC service ID	M	Identity of the MC service user, who has requested the cancellation
Cancellation type	O	Type of cancellation (e.g. from reporting LMC, from LMS, from LMC and LMS)

Table 10.9.2.15-2 describes the information flow from the location management server to the location management client for the cancellation request of location information history reporting.

Table 10.9.2.15-2: Location information history cancel request (LMS – LMC)

Information element	Status	Description
MC service ID	M	Identity of the reporting MC service user

Table 10.9.2.15-3 describes the information flow from the MC service server to the location management server for the cancellation request of location information history reporting.

Table 10.9.2.15-3: Location information history cancel request (MC service server - LMS)

Information element	Status	Description
MC service ID	M	Identity of the reporting MC service user
MC service ID	O	Identity of the MC service user, who has requested the cancellation

10.9.2.16 Location information history cancel response

Table 10.9.2.16-1 describes the information flow from the location management server to the MC service server for the cancellation response of location information history reporting.

Table 10.9.2.16-1: Location information history cancel response (LMC – LMS)

Information element	Status	Description
MC service ID list	M	List of identities (e.g. MCPTT ID, MCData ID, MCVideo ID) of the reporting MC service user

Table 10.9.2.16-2 describes the information flow from the location management server to the location management client for the cancellation response of location information history reporting.

Table 10.9.2.16-2: Location information history cancel response (LMS – LMC)

Information element	Status	Description
MC service ID	M	Identity of the reporting MC service user
Response	M	Confirm cancellation from reporting LMC, from LMS or from reporting LMC and LMS

Table 10.9.2.16-3 describes the information flow from the MC service server to the location management server for the cancellation response of location information history reporting.

Table 10.9.2.16-3: Location information history cancel response (LMS - MC service server)

Information element	Status	Description
MC service ID	M	Identity of the reporting MC service user

10.9.2.17 Location reporting temporary configuration request

Table 10.9.2.17-1 describes the information flow from the location management client and location management server in the primary MC system to the location management server and location management client in the partner MC system for the location reporting temporary configuration request.

Table 10.9.2.17-1: Location reporting temporary configuration request

Information element	Status	Description
MC service ID	M	Identity of the authorized and configuring MC service user located in the primary MC system
Functional alias	O	Functional alias that corresponds to the authorized and configuring MC service user located in the primary MC system
MC service ID	M	Identity of the MC service user located in the partner MC system whose location reporting has to be configured
Functional alias	O	Functional alias that corresponds to MC service user located in the partner MC system whose location reporting has to be configured
MC service UE label	O	Generic name of the to be configured MC service UE
Temporary location reporting configuration (see NOTE 1)	M	Provides set of location reporting parameters to be used temporarily.
Configuration expiration criteria (see NOTE 2)	O	Criteria for restoration of original location reporting parameters (e.g. timer).
NOTE 1: All or a subset of the location reporting parameters described in clause 10.9.2.1 of the present document are used. If empty the original location reporting parameters are used, immediately. NOTE 2: Ignored with an empty Temporary location reporting configuration.		

10.9.2.18 Location reporting temporary configuration response

Table 10.9.2.18-1 describes the information flow from the location management client and location management server in the partner MC system to the location management server and location management client in the primary MC system for the location reporting temporary configuration response.

Table 10.9.2.18-1: Location reporting temporary configuration response

Information element	Status	Description
MC service ID	M	Identity of the authorized and configuring MC service user located in the primary MC system
Functional alias	O	Functional alias that corresponds to the authorized and configuring MC service user located in the primary MC system
MC service ID	M	Identity of the MS service user located in the partner MC system whose location reporting has been configured
Functional alias	O	Functional alias that corresponds to the MS service user located in the partner MC system whose location reporting has been configured
MC service UE label	O	Generic name of the configured MC service UE
Result	M	Indicates the status of each configuration parameter

10.9.2.19 Restrict location information dissemination request

Table 10.9.2.19-1 describes the information flow from the location management client to the location management server for restricting the location information dissemination further.

Table 10.9.2.19-1: Restrict location information dissemination request information elements

Information Element	Status	Description
MC service ID	M	Identity of the requesting MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
Restrict Location Information Dissemination	M	Indicates to enable or disable the location information dissemination
List of users (see NOTE 1, NOTE 2)	O	Indicates that the restriction of the location information dissemination is applicable for the list of users.
Functional Alias (see NOTE 1, NOTE 2, NOTE 3)	O	Indicates that the restriction of the location information dissemination is applicable for the list of users who have activated this functional alias.
NOTE 1: If not present, restricting of the location information dissemination is applicable to any users. Dissemination restriction to a particular set of users is not possible if the LMC client applies local restrictions to stop providing location information per local policies. NOTE 2: Either the MC service ID list or the functional alias must be present. NOTE 3: The LMS track the users activating and de-activating functional alias so that associated restriction record can be updated accordingly.		

10.9.2.20 Restrict location information dissemination response

Table 10.9.2.20-1 describes the information flow from the location management server to the location management client for response to restricting the location information dissemination request.

Table 10.9.2.20-1: Restrict location information dissemination response information elements

Information Element	Status	Description
MC service ID	M	Identity of the requesting MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
Restrict Location Information Dissemination status	M	Indicates the result of restricting the location information dissemination

10.9.2.21 Restrict location information dissemination notification

Table 10.9.2.21-1 and Table 10.9.2.21-2 describes the information flow from the location management server to the location management client and from the location management server to the MC service server for notifying about restricting the location information dissemination of another location management client.

Table 10.9.2.21-1: Restrict location information dissemination notification information elements (LMS to LMC)

Information Element	Status	Description
MC service ID	M	Identity of the MC service user whose location information dissemination retriction information is being notified (e.g. MCPTT ID, MCVideo ID, MCData ID)
MC service ID	M	Identity of the MC service user subscribed to location information
Location Information Dissemination information	M	Indicates whether the dissemination of another MC service user's location information is enabled or disabled

Table 10.9.2.21-2: Restrict location information dissemination notification information elements (LMS to MC service server)

Information Element	Status	Description
MC service ID	M	Identity of the MC service user whose location information dissemination retriction information is being notified (e.g. MCPTT ID, MCVideo ID, MCData ID)
Location Information Dissemination information	M	Indicates whether the dissemination of another MC service user's location information is enabled or disabled

10.9.3 Procedure

10.9.3.1 Event-triggered location reporting procedure

NOTE 1: This procedure is valid for single MC system operation only.

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. The conditions could include, for example, 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 time of measurement, accuracy, longitude, latitude, speed, bearing, altitude, ECGI, MBMS SAIs.

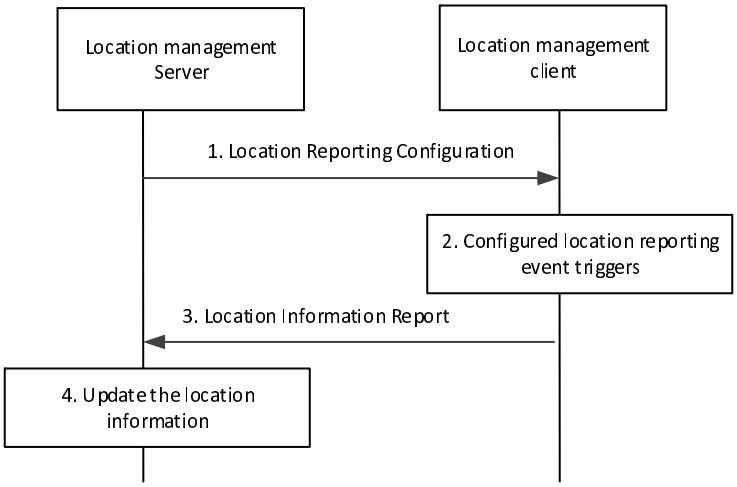

Figure 10.9.3.1-1: Event-triggered location reporting procedure

1. The location management server sends location reporting configuration message to the location management 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 location management client or as a group message over an MBMS bearer to update the location reporting configuration for multiple location management clients at the same time.

NOTE 2: 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 3: 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. If the location information report contains an optional MC service UE label, the location management server stores it together with the location information for the reporting location management client.

10.9.3.2 On-demand location reporting procedure

NOTE: This procedure is valid for single MC system operation only.

The location management server can request MC service 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.

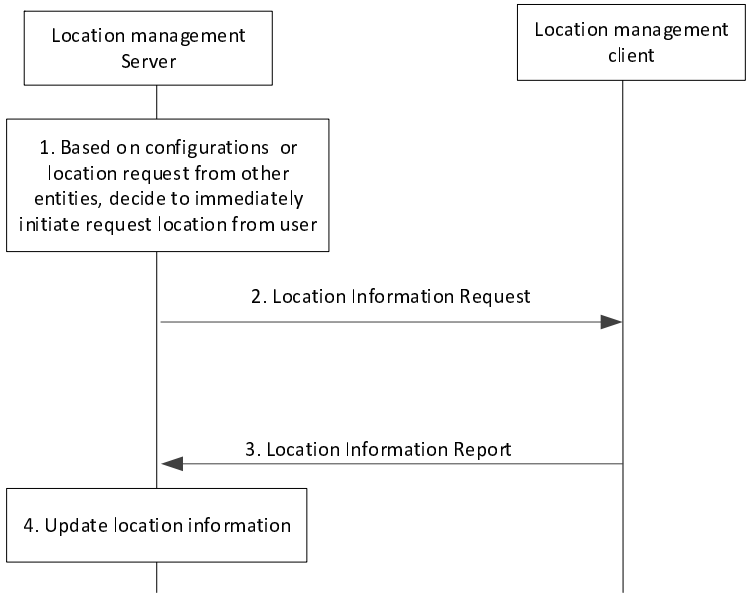

Figure 10.9.3.2-1: On-demand location information reporting procedure

1. Based on configurations such as periodical location information timer, or location information request from other entities (e.g., another location management client of an authorized user, MC service server), location management server initiates the immediate request of location information to be sent from the location management client.

2. The location management server sends a location information request to the location management client.

3. 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.

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, the location management server just stores the reporting location information for that location management client. If the location information report contains an optional MC service UE label, the location management server stores it together with the location information for the reporting location management client.

10.9.3.3 Client-triggered location reporting procedure

NOTE: This procedure is valid for single MC system operation only.

Figure 10.9.3.3-1 illustrates the high level procedure of client-triggered location reporting.

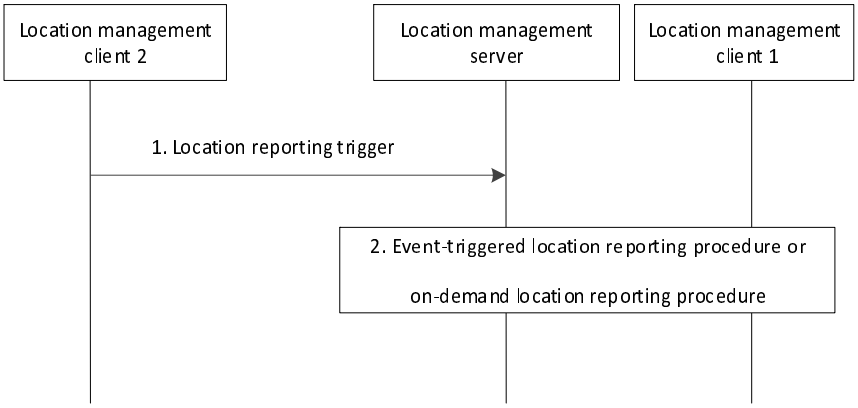

Figure 10.9.3.3-1: Client-triggered location reporting procedure

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 for location management client 1's location information. 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

NOTE: This procedure is valid for single MC system operation only.

The location reporting cancel procedure reuses the information flow of location reporting configuration.

Pre-conditions:

- The location management client has been provided with location reporting configuration information.

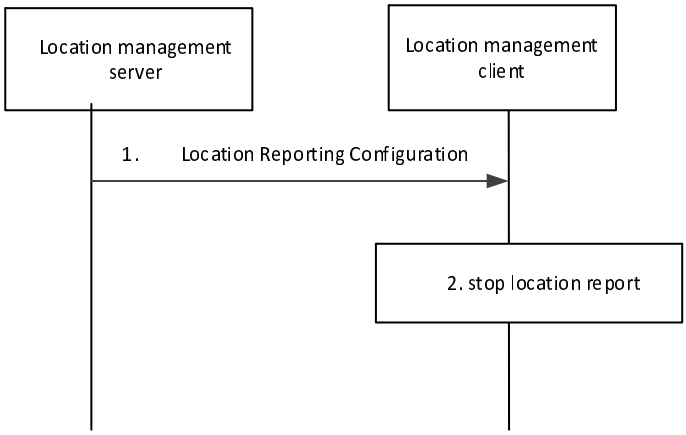

Figure 10.9.3.4-1: Location reporting cancel procedure

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

NOTE 1: This procedure is valid for single MC system operation only.

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.

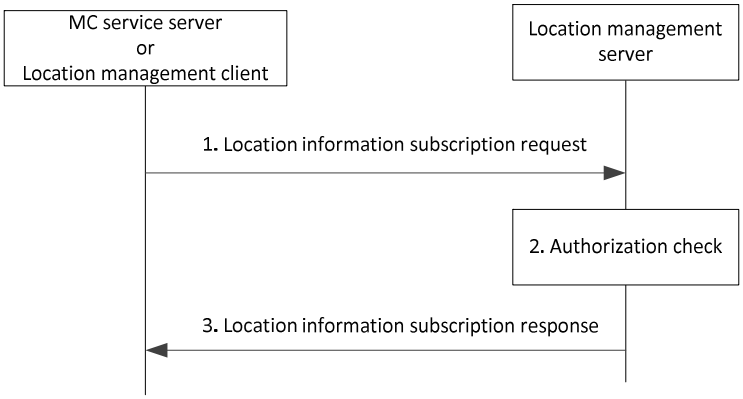

Figure 10.9.3.5-1: Location information subscription request procedure

1. MC service server or location management client 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 checks if the location management client is authorized to initiate the location information subscription request.

NOTE 2: As the MC service server is implicitly trusted, the Location management server needs not to check the authorization for the MC service server.

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

NOTE 1: This procedure is valid for single MC system operation only.

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.

Pre-condition:

1. The MC service server or location management client has subscribed to the location information of a target MC service user.

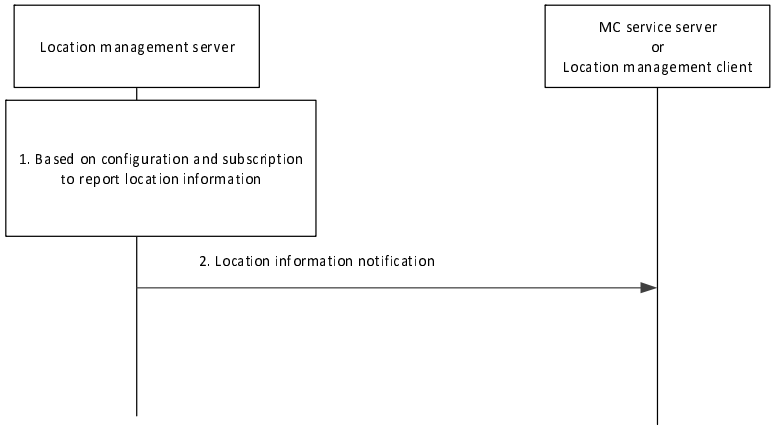

Figure 10.9.3.6.1-1: Event-trigger usage of location information procedure

1. Based on configuration, e.g., subscription, periodical location information timer, the location management server is triggered to report the latest user location information of the target MC service user to the subscribed MC service server or subscribed location management client. The location management server has verified that the subscribed MC service server or subscribed location management client is authorized to receive the user location information of the target MC service user.

2. The location management server sends the location information notification including the latest location information of one MC service user to the MC service server or to the location management client. The latest location information is derived from the location report procedure as described in clause 10.9.3.1, or from PLMN operator (e.g. LCS network). If the optional MC service UE label is present, the location management server sends it, as part of the location information notification, to the MC service user.

NOTE 2: The MC service server does not receive the MC service UE label.

10.9.3.6.2 On-demand usage of location information procedure

NOTE 1: This procedure is valid for single MC system operation only.

The MC service server or the location management client can request location information at any time by sending a location information request to the location management server, which may trigger location management server to send the location information report immediately.

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 other entities that would like to subscribe to location information at the location management server of an MC service user.

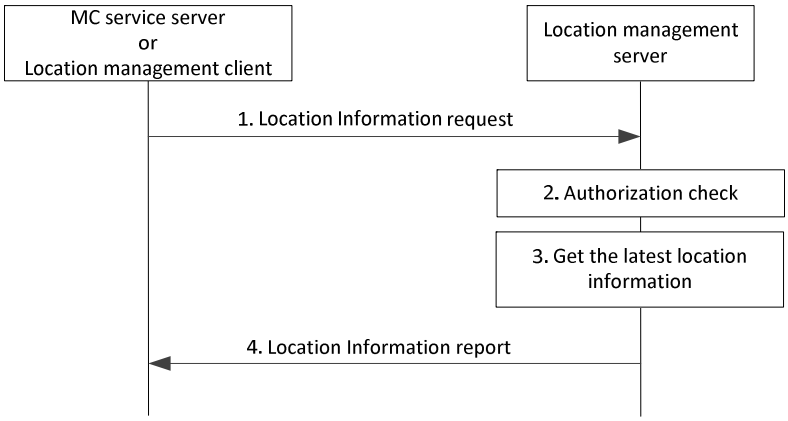

Figure 10.9.3.6.2-1: On-demand usage of location information procedure

1. MC service server or location management client send a location information request to the location management server.

2. The location management server checks if the location management client is authorized to request the location information.

NOTE 2: As the MC service server is implicitly trusted, the Location management server needs not to check the authorization for the MC service server.

3. The location management server acquires the latest location of the MC service clients being requested, by triggering an on-demand location report procedure as described in clause 10.9.3.2, or from PLMN operator (e.g. LCS network).

4. Then, location management server immediately sends the location information report including the latest location information acquired of one MC service user to the MC service server or to the location management client. If the optional MC service UE label is present, the location management server sends it, as part of the location information report, to the MC service user.

NOTE 3: The MC service server does not receive the MC service UE label.

10.9.3.7 Location information cancel subscription procedure

NOTE: This procedure is valid for single MC system operation only.

Figure 10.9.3.7-1 illustrates the high level procedure of location information cancel subscription request. The MC service server or the location management client can request the cancellation of location information subscriptions at any time from the location management server.

Pre-conditions:

- The authorized MC service user is in possession of the MC service ID of the MC service user as well as the location information subscriptions of this MC service ID.

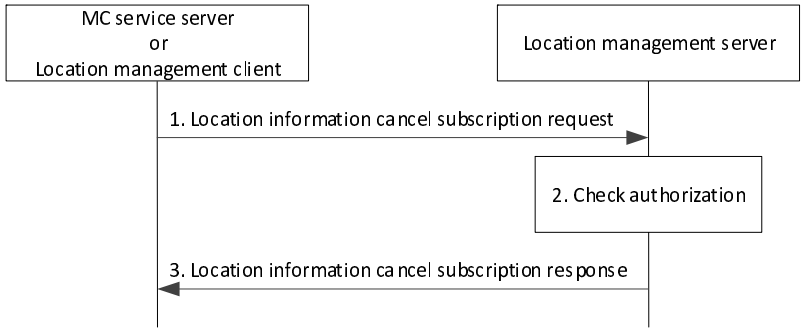

Figure 10.9.3.7-1: Location information cancel subscription request procedure

1. MC service server or location management client sends a location information cancel subscription request to the location management server to cancel the subscription for location information of one or more MC service users.

2. The location management server checks the authorization of this request.

NOTE: Whether the authorization check is a specific check of the requesting MC service user or is a general policy check is outside the scope of this procedure.

3. The location management server replies with a location information cancel subscription response indicating the cancel subscription status.

10.9.3.8 Location management using functional alias

10.9.3.8.1 Client-triggered one-time location information report

Figure 10.9.3.8.1-1 illustrates the procedure when a location management client requests one-time location information from other location management clients for location information reporting using functional alias, which can be shared between several MC service users. Under this condition, the actual location of all MC service users sharing the same functional alias are reported.

Pre-conditions:

1. MC service client 2 and MC service client 3 share the same functional alias.
2. MC service client 2 and MC service client 3 activated the functional alias.
3. MC service client 1 may have an activated functional alias.
4. The location management server has subscribed to the functional alias controlling MC service server within the MC system for functional alias activation/de-activation updates.

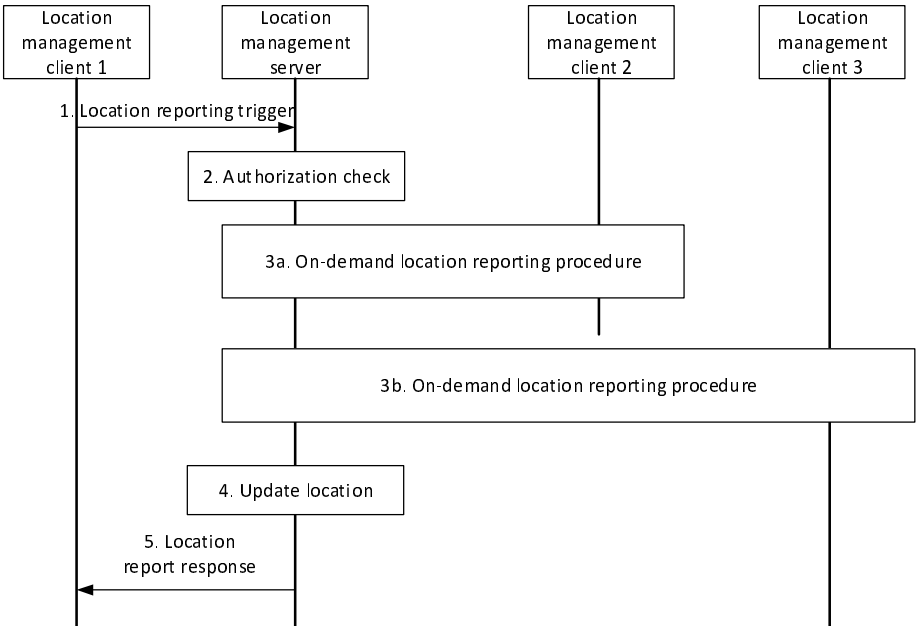

Figure 10.9.3.8.1-1: One-time location information report for shared functional alias

1. Location management client 1 sends a location reporting trigger, limited to one MC service at the time, to the location management server to activate a one-time location report procedure which shall retrieve the location information of the MC service users that may share the contained functional alias. Location management client 1 may include its own activated functional alias.
2. Location management server checks whether location management client 1 is authorized to send a location reporting trigger for location information of location management clients 2 and 3.
3. The location management server uses on-demand location reporting procedures. The location information request contains the functional alias provided by the location management client 1 to address location management client 2 and location management client 3.
4. Upon receiving the report, the location management server updates location of the reporting location management clients. If the location management server does not have location information of a reporting location management client before, then just stores the reporting location information for that location management client.
5. The location management server sends location report responses to location management client 1 containing the provided location information for each location management client using the given functional alias. If the optional MC service UE label is present, the location management server sends it, as part of the location report

response to location management client 1. If not all location management clients immediately respond to the location management server, i.e. other reports some time later, subsequent location reporting responses may be sent.

10.9.3.8.2 Client-triggered periodic location information report

Figure 10.9.3.8.2-1 illustrates the procedure when a location management client requests periodic location information from other location management clients for location information reporting using functional aliases which may be shared between several MC service users. Under this condition, the actual location of all MC service users sharing the same functional alias are reported.

Pre-conditions:

1. MC service client 2 and MC service client 3 share the same functional alias.
2. MC service client 2 and MC service client 3 activated the functional alias.
3. MC service client 1 may have an activated functional alias.
4. The location management server has subscribed to the functional alias controlling MC service server within the MC system for functional alias activation/de-activation updates.

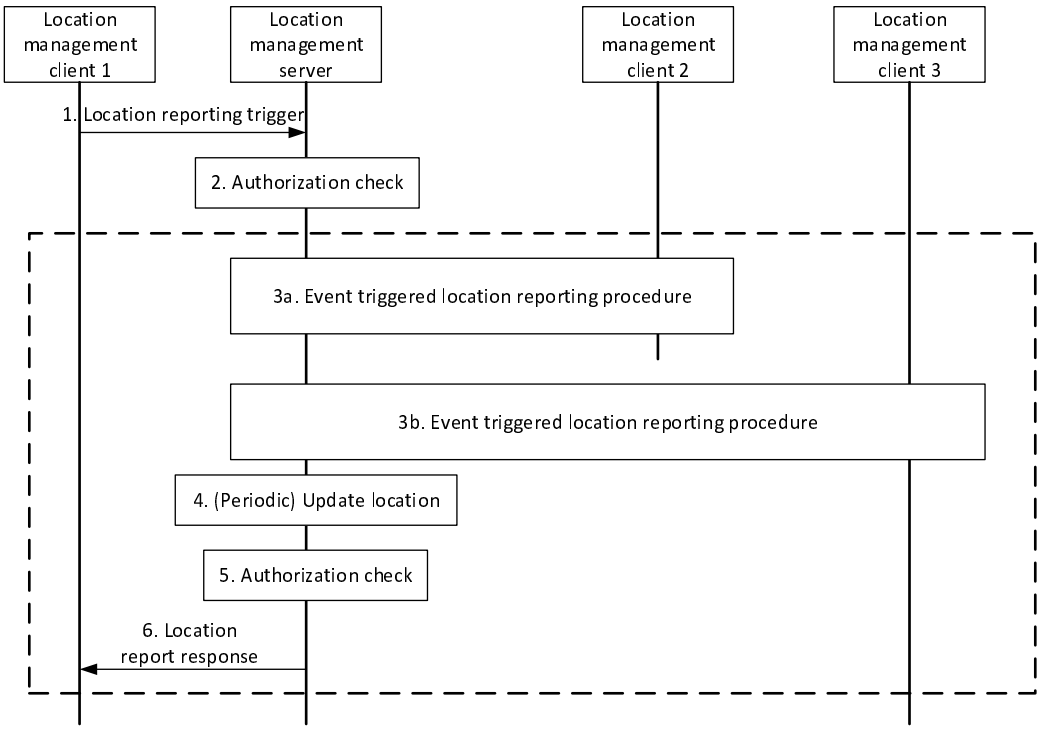

Figure 10.9.3.8.2-1: Periodic location information report for shared functional alias

1. Location management client 1 sends a location reporting trigger, limited to one MC service at the time, to the location management server to activate a periodic location reporting procedure which shall retrieve the location information of the MC service users sharing the contained functional alias. Location management client 1 may include its own activated functional alias.
2. Location management server checks whether location management client 1 is authorized to send a location reporting trigger for location information for location management clients that have activated the functional alias.
3. Depending on the information given by the location reporting trigger, the location management server uses event-triggered location information procedure and immediately send location information request to the location management clients that contains the functional alias requested by the location management client 1.

4. Upon receiving the reports, the location management server updates location of the reporting location management clients.

5. The location management server checks whether location management client 1 is authorized to receive location information for all location management clients that have activated the functional alias.

6. Based on the received location information reports, the location management server will periodically issue location report responses, one at a time for each location management client for which location management client 1 is authorized to receive location information, encompassing the MC service ID, the associated functional alias, the individual location information of the addressed MC service ID and the optional MC service UE label, if present.

NOTE 1: If a functional alias is deactivated for an MC service client, the corresponding location management client stops sending periodic location information reports.

NOTE 2: If a functional alias has been newly activated for an MC service client, the location management server activates location information reporting for this location management client.

NOTE 3: If a functional alias is simultaneously shared between several MC service IDs, all location management clients with the associated MC service IDs will send the location report until the functional alias status change, e.g. take-over, for the individual MC service ID.

10.9.3.9 Usage of location history reporting procedure

10.9.3.9.1 General

The location management client may get into a state where it cannot report location information to the location management server at any time after the initial location reporting configuration was provided by the location management server. If any location information trigger criterion applies, while not reporting location information to the location management server, the location management client stores the corresponding location information.

Trigger criteria while not reporting location information to the location management server may vary from trigger criteria while reporting location information to the location management server. Such trigger criteria may for example include not reported distance travelled, not reported elapsed time, not reported call initiation, not reported emergency alert, not reported emergency group call, not reported imminent peril group call and not reported emergency private call.

10.9.3.9.2 Report location history procedure

10.9.3.9.2.1 On-demand report location history procedure (LMC – LMS)

The location management server can request stored location information at any time from the location management client, following a return to report location information to the location management server.

Figure 10.9.3.9.2.1-1 illustrates the procedure for the on-demand based usage of location information history reporting from the location management client to the location management server.

Pre-conditions:

1. The location management client is configured to store location information, while not reporting location information to the location management server.

2. The location management client has stored location information based on triggering criteria in not reporting location information cases.

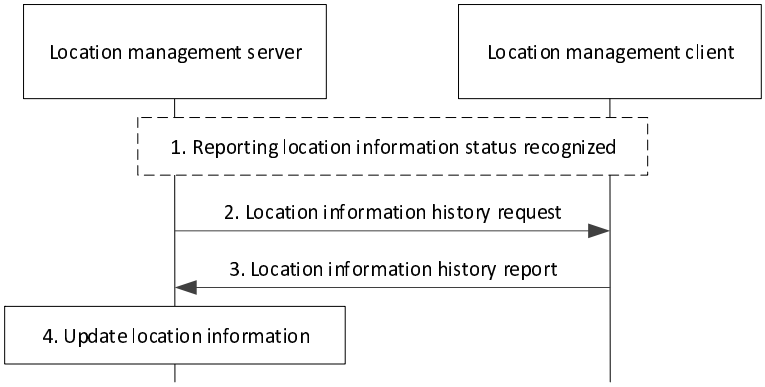

Figure 10.9.3.9.2.1-1: On-demand based usage of report location history procedure (LMC – LMS)

1. The location management client returns to report location information while there is a communication link between the location management client and location management server.

2. Location management server requests the stored location information.

NOTE 1: The location management client may provide the status of the stored location information prior to the request from location management server.

3. The location management client responds to the location management server with one or several stored location information history reports.

NOTE 2: The transmission of requested stored location information does not interrupt the reporting of location information.

NOTE 3: The most recent stored location information that qualifies for transmission is transmitted first.

NOTE 4: The transmission may be stopped at any time with the cancel location history reporting procedure, according to the procedure described in clause 10.9.3.9.4 of the present document.

4. The location management server updates the available location information with one or several stored location information and the optional MC service UE label, if present, from the location management client.

10.9.3.9.2.2 On-demand report location history procedure

The location management server can request stored location information at any time from the location management client, following a return to report location information to the location management server. The MC service server or the location management client may initiate the request of stored location information.

Figure 10.9.3.9.2.2-1 illustrates the procedure for the on-demand based usage of location history reporting.

Pre-conditions:

1. The location management client 1 is configured to store location information, while not reporting location information to the location management server.

2. The location management client 1 has stored location information based on triggering criteria in not reporting location information cases.

3. The location management server may have none, a subset or all available stored location information reports from location management client 1.

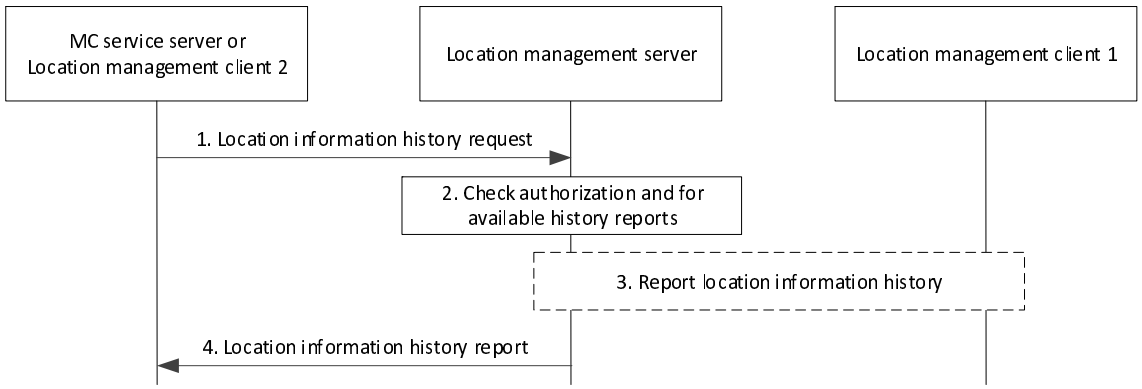

Figure 10.9.3.9.2.2-1: On-demand based usage of report location history procedure

1. The MC service server or the location management client 2 initiate the location information history request to the location management server.

NOTE: The MC service server or the location management client 2 may request the status on stored location information from location management client 1, prior to the location information history request.

2. The location management server checks the authorization of this request and compares the location information history request with the already retrieved stored location information from location management client 1.

3. The location management server requests stored location information from location management client 1 according to the procedure described in clause 10.9.3.9.2.1 of the present document, if the desired stored location information is not available on the location management server.

4. The location management server reports the requested stored location information to the MC service server or location management client 2. The location management server reports the optional MC service UE label, if present, to the location management client 2.

10.9.3.9.3 Usage of status location history reporting procedure

10.9.3.9.3.1 Status location history reporting procedure (LMC – LMS)

The location management client can report the status of stored location information at any time to the location management server, following a return to report location information to the location management server.

Figure 10.9.3.9.3.1-1 illustrates the procedure for the usage of the status reporting from the location management client.

Pre-conditions:

1. The location management client has returned to report location information and has stored location information reports.

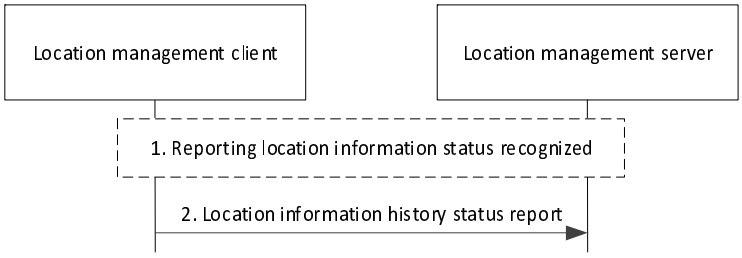

Figure 10.9.3.9.3.1-1: Status location history reporting procedure (LMC – LMS)

1. The location management client returns to report location information while there is a communication link between the location management client and location management server.
2. The location management client reports without a status request the status of the stored location information to the location information server.

10.9.3.9.3.2 On-demand status location history reporting procedure (LMS – LMC)

The location management server can request the status of stored location information at any time from the location management client, following a return to report location information to the location management server.

Figure 10.9.3.9.3.2-1 illustrates the procedure for the on-demand based usage of requesting the status of the stored location information from the location management client.

Pre-conditions:

1. The location management client has returned to report location information and has stored location information reports.

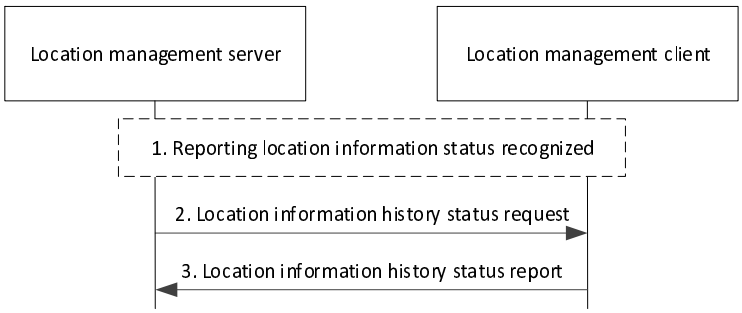

Figure 10.9.3.9.3.2-1: On-demand based usage of status location history reporting procedure (LMS – LMC)

1. The location management client returns to report location information while there is a communication link between the location management client and location management server.
2. The location management server requests the status of the stored location information from the location management client.
3. The location management client reports the status of the stored location information to the location information server.

10.9.3.9.3.3 On-demand status location history reporting procedure

The MC service server or the location management client can request the status of stored location information at any time, following a return to report location information to the location management server.

Figure 10.9.3.9.3.3-1 illustrates the procedure for the on-demand based usage of the status location history reporting procedure.

Pre-conditions:

1. The location management client 1 has returned to report location information and has stored location information reports.

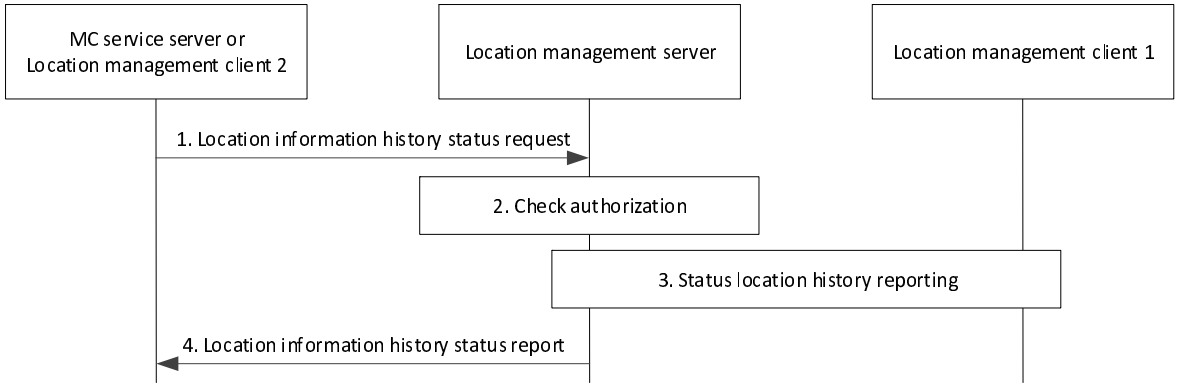

Figure 10.9.3.9.3.3-1: On-demand based usage of status location history reporting procedure

1. The MC service server or location management client 2 requests the status of the stored location information reports from the location management client 1.
2. The location management server checks the authorization of this request.
3. The location management server requests and receives the status report of the stored location information from location management client 1 according to the procedure described in clause 10.9.3.9.3.2 of the present document.
4. The location management server forwards this information to the MC service server or location management client 2.

10.9.3.9.4 Usage of cancel location history reporting procedure

10.9.3.9.4.1 General

The location management server can request cancellation of the transmission of location information history reports at any time following the start of transmission by sending a location information history cancel request to the reporting location management client. The MC service server or location management client could initiate the cancellation request, if those entities are aware of ongoing location information history reporting. The transmission cancellation does not have any effect on the configured triggering criteria in emergency cases, triggering criteria in non-emergency cases nor on the triggering criteria in not reporting location information cases.

10.9.3.9.4.2 Cancel location history reporting procedure (LMS – LMC)

Figure 10.9.3.9.4.2-1 illustrates the procedure for the cancellation on location history reporting from the location management server to the location management client.

Pre-conditions:

1. The location management client has returned to report location information and has stored location information reports.

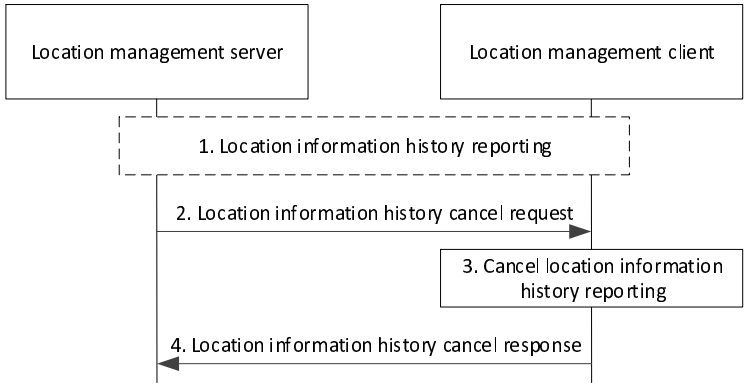

Figure 10.9.3.9.4.2-1: Cancel location history reporting procedure (LMS – LMC)

1. The location management client transmits stored location information while there is a communication link between the location management client and location management server.
2. The location management server requests the cancellation of the location information history reporting at any time during the transmission.
3. Location management client cancels the location information history reporting.
4. Location management client confirms the executed cancellation request.

10.9.3.9.4.3 Cancel location history reporting procedure

Figure 10.9.3.9.4.3-1 illustrates the procedure for the cancellation on location history reporting from the MC service server or location management client to the location management server.

Pre-conditions:

1. The location management client 1 has returned to report location information and has stored location information reports.

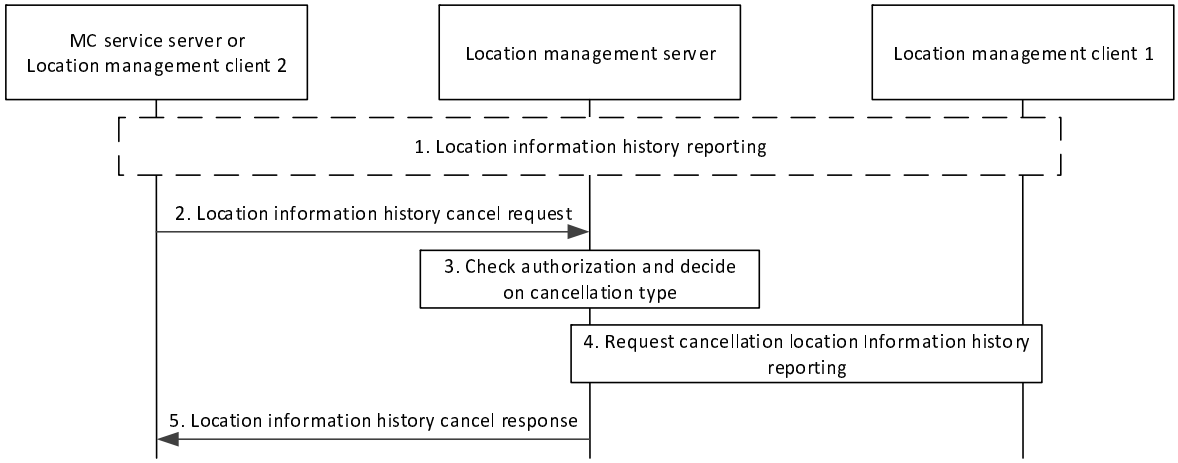

Figure 10.9.3.9.4.3-1: Cancel location history reporting procedure

1. The location management client 1 transmits stored location information while there is a communication link between the location management client and location management server.

2. The MC service server or location management client 2 requests the cancellation of the location information history reporting at any time during the transmission.
3. The location management server checks the authorization of this request and decides whether to cancel the transmission from the reporting location management client 1 as described in clause 10.9.3.9.4.2, to cancel the transmission from the location management server or to cancel the transmission from both.
4. If there are no other authorized location management clients requesting the location history of location management client 1, the location management server executes the requested cancellation.
5. Location management server confirms the executed cancellation.

10.9.3.10 Usage of location information across MC systems procedure

10.9.3.10.1 General

Interconnected MC systems in either the same security domain or different security domains share location information either through the direct connection of the location management servers or through the connected MC gateway servers.

10.9.3.10.2 On-demand request of location information procedure

The MC service server or location management client in the primary MC system can request MC service user's location information, which is in the partner MC system, at any time by sending a location information request to the location management server at primary MC system.

Figure 10.9.3.10.2-1 illustrates the high level procedure of on-demand request of location information.

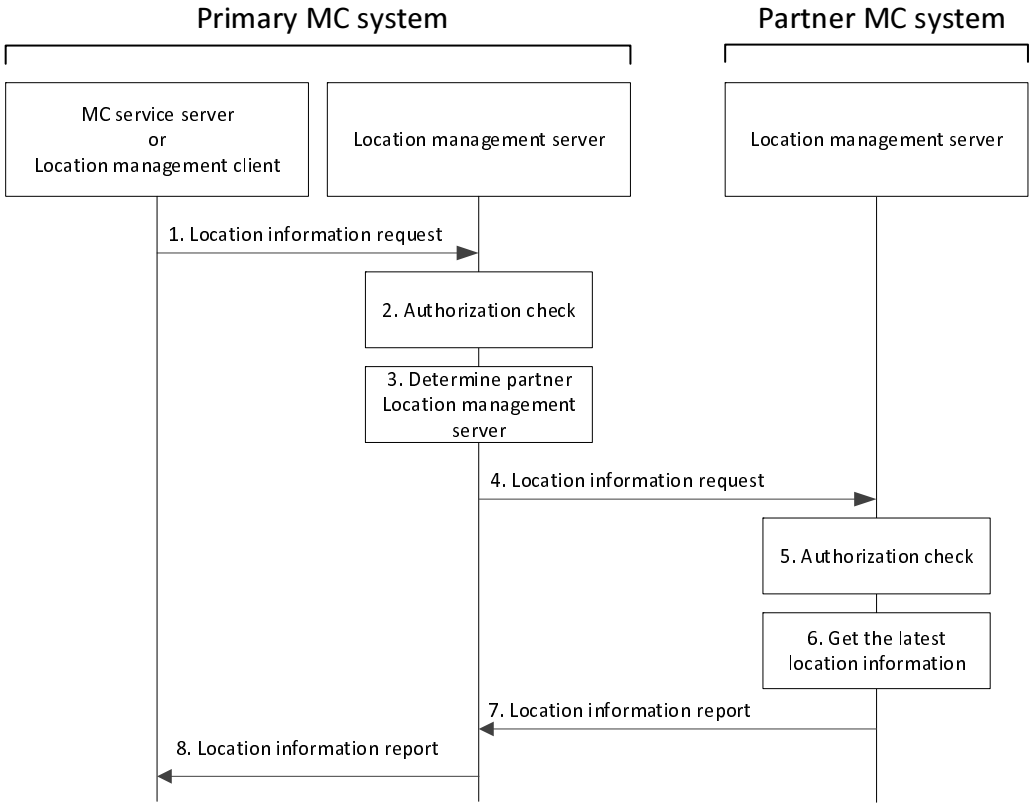

Figure 10.9.3.10.2-1: On-demand request of location information procedure

1. The MC service server or a location management client in the primary MC system requests on-demand location information of MC service user located in the partner MC system.

2. The location management server in the primary MC system checks if the provided information along with the configuration permit the request to proceed.

NOTE 1: Whether the authorization check is a specific MC service user based check or is a general policy check is outside the scope of this procedure.

3. The location management server in the primary MC system determines that the request has a target in a different MC system.

4. The location management server in the primary MC system sends the on-demand location information request to the location management server in the partner MC system.

5. The location management server in the partner MC system checks if the provided information along with the configuration permit the request to proceed.

NOTE 2: Whether the authorization check is a specific MC service user based check or is a general policy check is outside the scope of this procedure.

6. The location management server at partner MC system updates the location information, according to the procedure described in clause 10.9.3.2 or provides stored location information, based on the configuration for on-demand requests.

7. The location management server in the partner MC system sends the location information report, described in clause 10.9.2.2, to the MC service server in the primary MC system.

8. If the requesting location information management client is still authorized to receive the location report, the location management server in the primary MC system sends the location information report to the requesting location information management client.

10.9.3.10.3 Event-triggered location information notification procedure

The location management client in the partner MC system provides, based on configuration, periodic location information, which will be also forwarded to the subscribed entities.

Figure 10.9.3.10.3-1 illustrates the high level procedure of event-triggered sharing of location information.

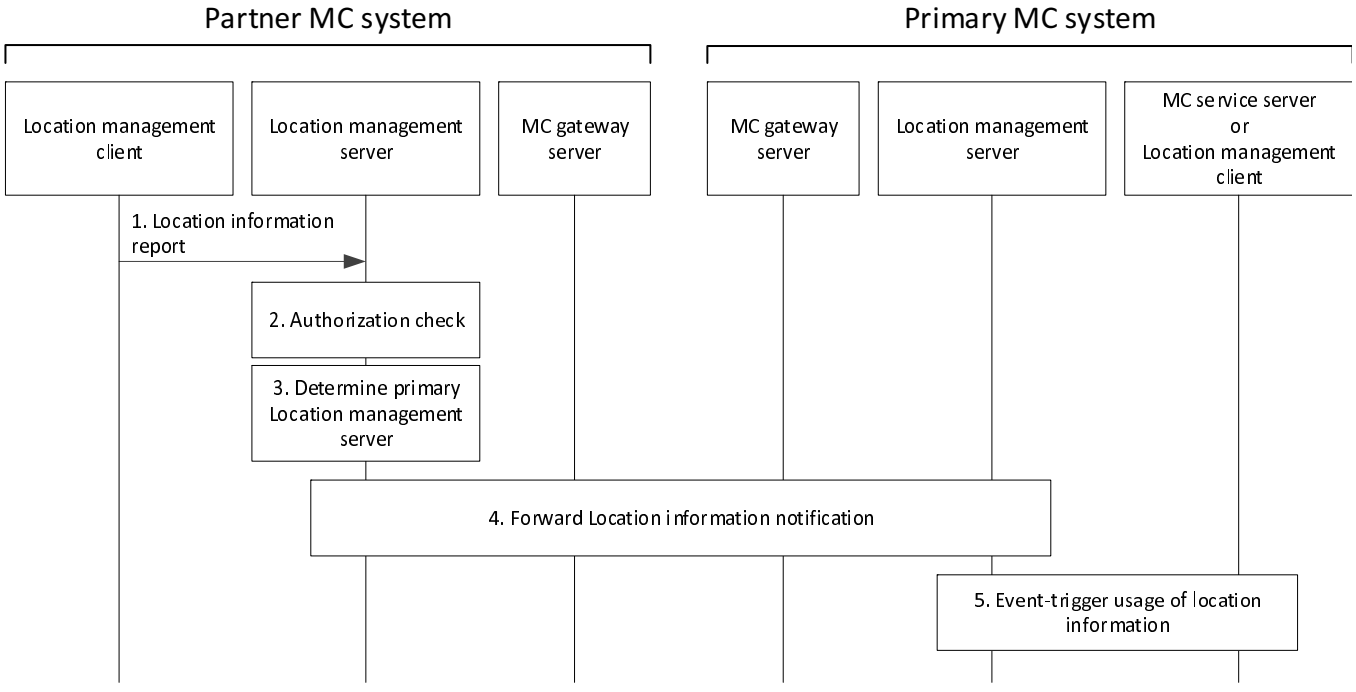

Figure 10.9.3.10.3-1: Event-triggered location information notification procedure

1. The location management client in the partner MC system is triggered, based on configuration, to send a location information report, according to described triggers in clause 10.9.3.1.

2. The location management server in the partner MC system checks if the provided information along with the configuration permit the report to proceed.

NOTE 1: Whether the authorization check is a specific MC service user based check or is a general policy check is outside the scope of this procedure.

3. The location management server in the partner MC system determines that the report has a target in a different MC system.

4. The location management server in the partner MC system sends the location information notification to the location management server in the primary MC system, according to the described information flow in clause 10.9.2.7.

5. The location management server in the primary MC system checks if the location management client is authorized to receive the location information and forwards the received location information, according to the procedure described in clause 10.9.3.6.1.

NOTE 2: As the MC service server is implicitly trusted, the Location management server needs not to check the authorization for the MC service server.

10.9.3.10.4 Location information subscription procedure

The location management client in the partner MC system provides, based on configuration, event triggered location information, which will be also forwarded to the subscribed entities.

Figure 10.9.3.10.4-1 illustrates the high level procedure of subscription to location information between interconnected MC systems.

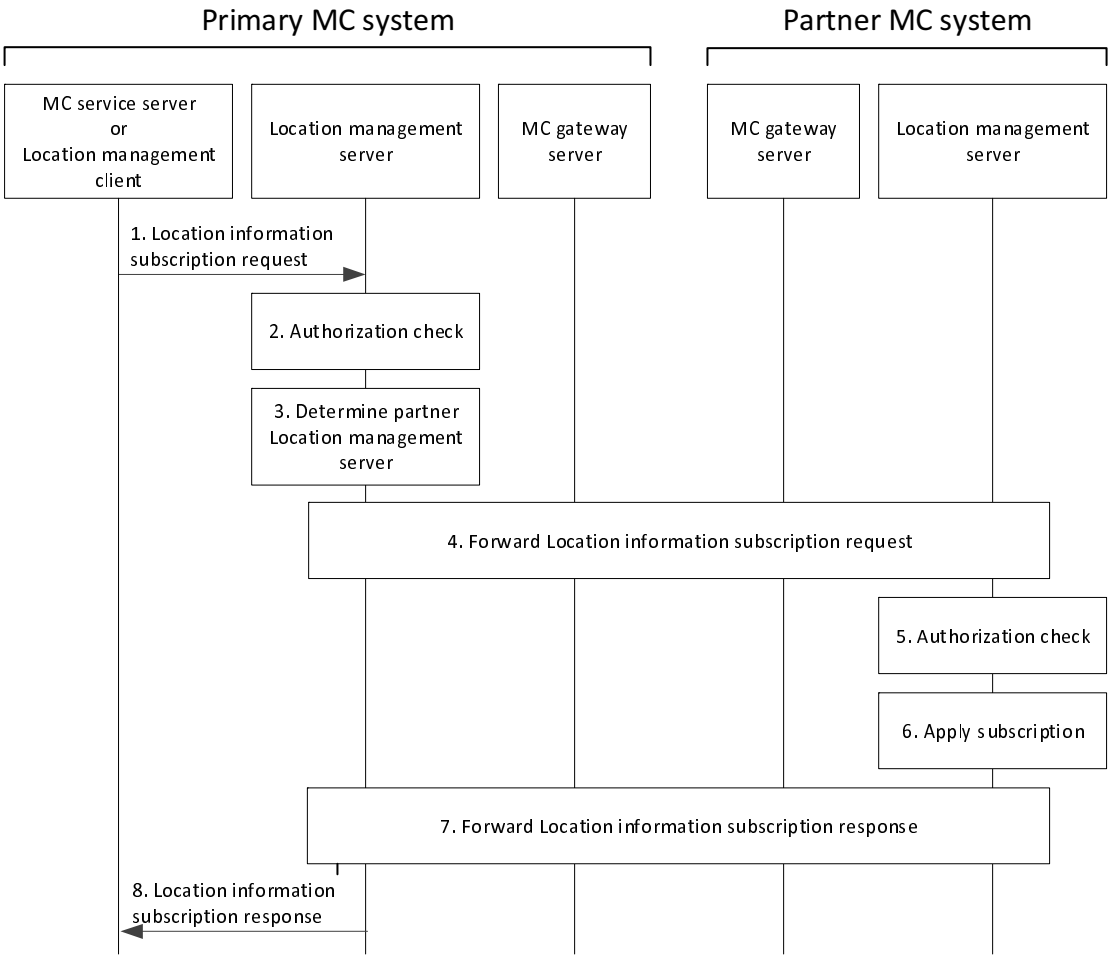

Figure 10.9.3.10.4-1: Location information subscription procedure

1. The MC service server or the location management client in the primary MC system request subscription to event-triggered location information of MC service users in the partner MC system by sending a location information subscription request to the location management server in the primary MC system, according to the described information flows in clause 10.9.2.5.

2. The location management server in the primary MC system checks if the provided information along with the configuration permit the request to proceed.

NOTE 1: Whether the authorization check is a specific MC service user based check or is a general policy check is outside the scope of this procedure.

3. The location management server in the primary MC system determines that the request has a target in a different MC system.

4. The location management server in the primary MC system sends the location information subscription request to the location management server in the partner MC system, according to the described information flow in clause 10.9.2.5.

5. The location management server in the partner MC system checks if the provided information along with the configuration permit the request to proceed.

NOTE 2: Whether the authorization check is a specific MC service user based check or is a general policy check is outside the scope of this procedure.

6. The location management server in the partner MC system applies the subscription.

7. The location management server in the partner MC system sends the location information subscription response to the location management server in the primary MC system.

8. The location management server in the primary MC system sends the location information subscription response to the requesting entity in the primary MC system, according to the described information flow in clause 10.9.2.6.

10.9.3.10.5 Location information cancel subscription procedure

The location management client in the primary MC system receives location information updates according to the subscriptions requested in the partner MC system. Those subscriptions can be cancelled anytime from the primary MC system.

Figure 10.9.3.10.5-1 illustrates the high level procedure of the subscription cancellation to location information between interconnected MC systems.

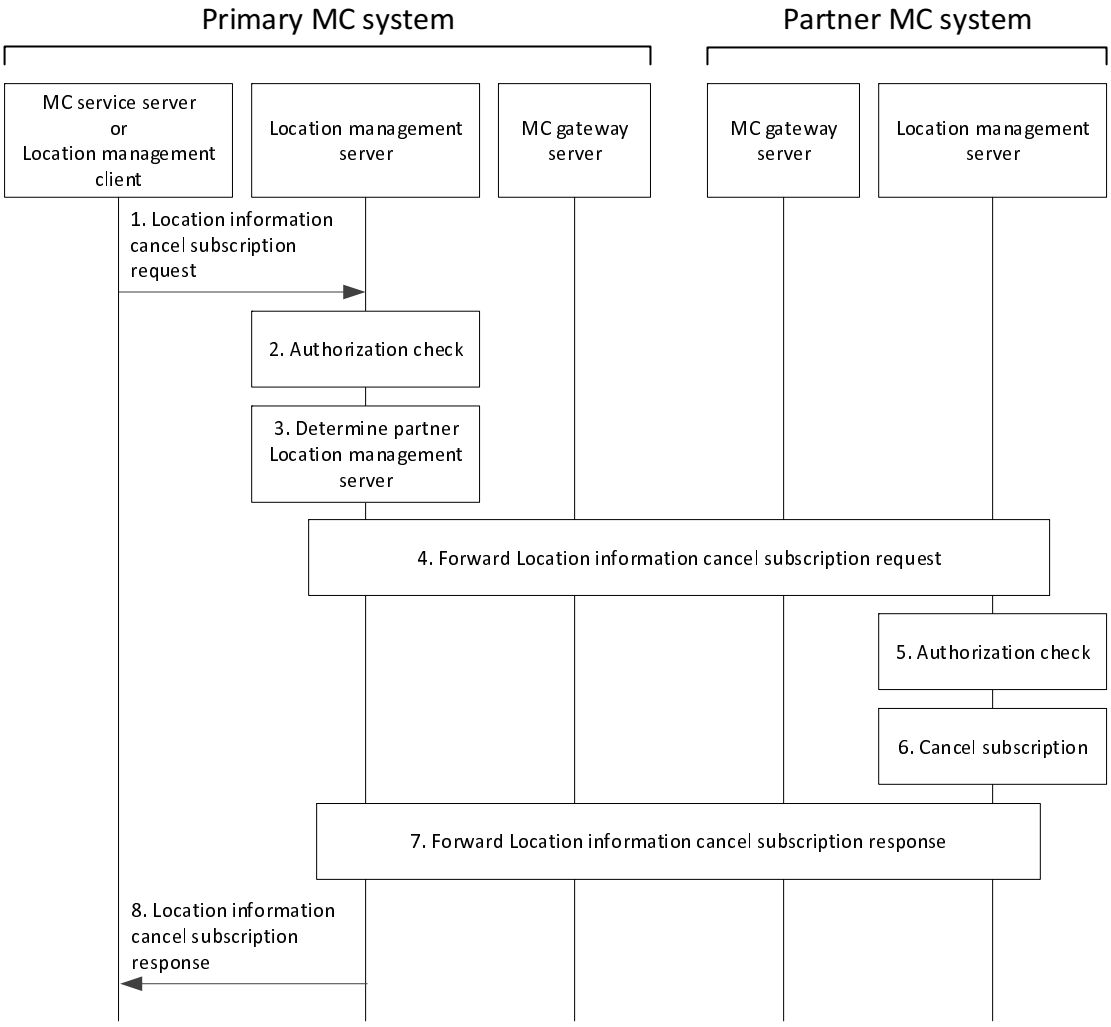

Figure 10.9.3.10.5-1: Location information cancel subscription procedure

1. The MC service server or the location management client in the primary MC system request the cancellation of subscriptions to event-triggered location information of MC service users in the partner MC system by sending location information cancel subscription requests to the location management server in the primary MC system, according to the described information flows in clause 10.9.2.8.

2. The location management server in the primary MC system checks if the provided information along with the configuration permit the request to proceed.

NOTE 1: Whether the authorization check is a specific MC service user based check or is a general policy check is outside the scope of this procedure.

3. The location management server in the primary MC system determines that the request has a target in a different MC system.

4. The location management server in the primary MC system sends the location information cancel subscription request to the location management server in the partner MC system, according to the described information flow in clause 10.9.2.8.

5. The location management server in the partner MC system checks if the provided information along with the configuration permit the request to proceed.

NOTE 2: Whether the authorization check is a specific MC service user based check or is a general policy check is outside the scope of this procedure.

6. The location management server in the partner MC system cancels the subscription.

7. The location management server in the partner MC system sends the location information cancel subscription response to the location management server in the primary MC system.

8. The location management server in the primary MC system sends the location information cancel subscription response to the requesting entity in the primary MC system, according to the described information flow in clause 10.9.2.9.

10.9.3.10.6 Location reporting temporary configuration procedure

An authorized MC service user in the primary MC system in charge of MC service users either currently completely or partially operating in a partner MC system is able to configure event-based location information for the involved MC service users at any time by sending configuration parameters. Those configuration parameters are temporarily used, while the configuration parameters of the primary MC system are reinstated either by the configuration expiration criteria or by request from the authorized MC service user.

Figure 10.9.3.10.6-1 illustrates the high level procedure of location reporting temporary configuration procedure.

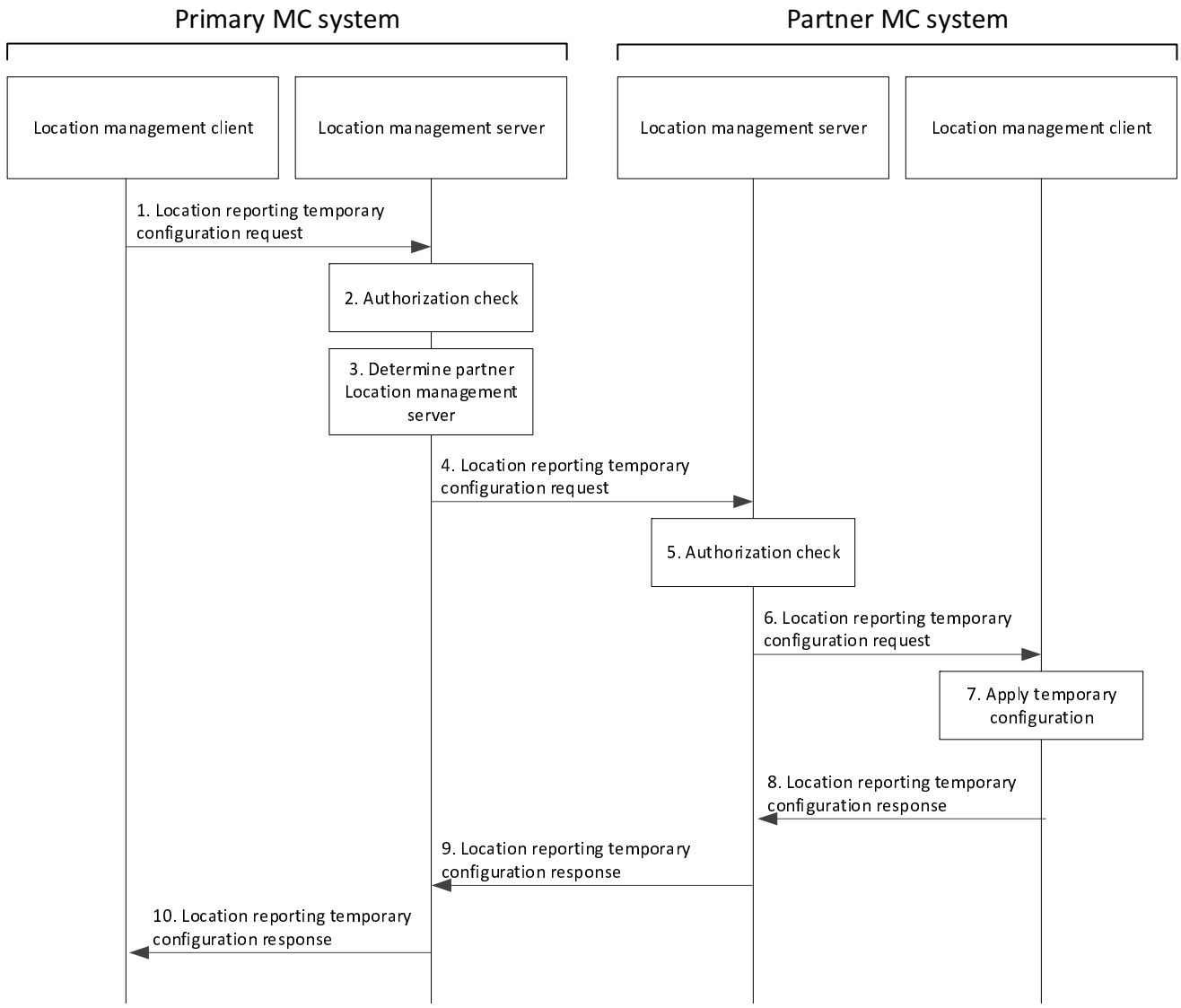

Figure 10.9.3.10.6-1: Location reporting temporary configuration procedure

1. The location management client in the primary MC system requests to configure the location reporting of MC service user(s) located in the partner MC system.

2. The location management server in the primary MC system checks if the provided information along with the configuration permit the request to proceed.

NOTE 1: Whether the authorization check is a specific MC service user based check or is a general policy check is outside the scope of this procedure.

3. The location management server in the primary MC system determines that the request has a target in a different MC system.

4. The location management server in the primary MC system sends the location reporting temporary configuration request to the location management server in the partner MC system.

5. The location management server in the partner MC system checks if the provided information along with the configuration permit the request to proceed.

NOTE 2: Whether the authorization check is a specific MC service user based check or is a general policy check is outside the scope of this procedure.

6. The location management server in the partner MC system forwards the location reporting temporary configuration request to the location management client in the partner MC system. The location management server in the partner MC system may adjusts the configuration parameters.

7. The location management client in the partner MC system applies the temporary configuration parameters and stores the original configuration parameters as well as sets the configuration expiration criteria.

8. The location management client in the partner MC system sends the location reporting temporary configuration response to the location management server in the partner MC system. The location reporting temporary configuration response includes the full status report on all configuration parameters, even if only one configuration parameter has received a request of adaptation.

9. The location management server in the partner MC system sends the location reporting temporary configuration response to the location management server in the primary MC system.

10. The location management server in the primary MC system sends the location reporting temporary configuration response to the location management client in the primary MC system.

10.9.3.11 Restrict location information dissemination procedure

The location management client can control the location information dissemination at any time by sending a restrict location information dissemination request to the location management server, which will indicate to the location management server whether the location information can be disseminated further or not.

Figure 10.9.3.11-1 illustrates the high level procedure whether to enable/disable the restriction to distribute the location information further or not.

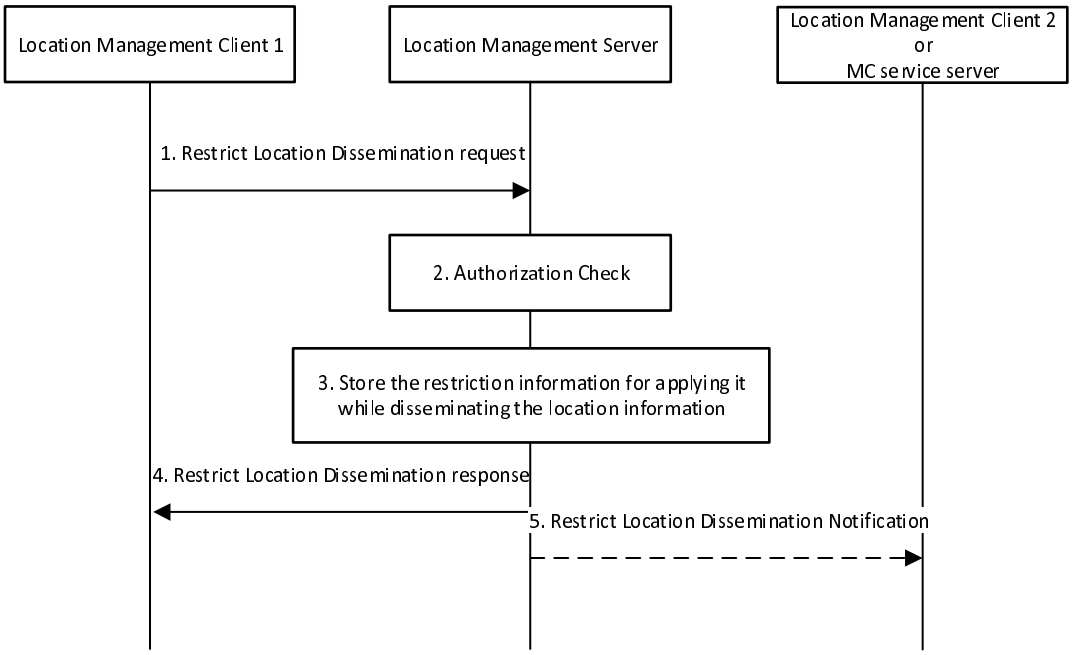

Figure 10.9.3.11-1: Restrict the location information dissemination procedure

1. The location management client 1 initiates a request for restricting the location information dissemination, containing an indication to enable the restriction or disable the restriction. By default, the location management server can disable the restriction, i.e. location information of user can be distributed further. The request may provide the list of MC service IDs of MC service users (e.g. based on the role or selected users or any). The list could be pre-defined or dynamic or based on any other criteria.

NOTE 1: In accordance with local policies, the LMC can apply local restrictions by stopping providing location information when a location dissemination request has been activated.

2. The location management server checks if the location management client 1 is authorized to restrict the location information dissemination.

3. The location management server updates restriction information of the reporting location management client 1. If the location management server does not have the restriction record for the location information dissemination of the requesting location management client 1 before, then just store the restriction record for that location management client 1.

NOTE 2: The location server, depending on local policies, can choose to not apply the restriction of location information for emergency services (e.g. Emergency Call, Emergency alert, Imminent peril call, etc.) and for authorized users (e.g. dispatcher, supervisor).

4. The location management server sends the restrict location information dissemination response to the location management client 1 to confirm the status of the restrict location information dissemination request.

5. The location management server may inform all the subscribed users (in accordance with local policies and local requirements) that the location information from this particular user will be provided or not by sending the restrict location information dissemination notification upon successfully applying restrictions on location dissemination as described in step 3 above.

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, emergency alert cancel, entering emergency alert area and leaving emergency alert area that are utilised by the following MC services:

- MCPTT
- MCVideo
- MCData

10.10.1.1A Information flows

10.10.1.1A.1 MC service emergency alert request

Table 10.10.1.1A.1-1 describes the information flow MC service emergency alert request from the MC service client to the MC service server and from the MC service server to the MC service client.

Table 10.10.1.1A.1-1: MC service emergency alert request information elements

Information Element	Status	Description
MC service ID	M	The identity of the alerting party
Functional alias	O	The functional alias of the alerting party
MC service group ID (see NOTE 1)	O	The target MC service group ID with which the alert is associated
MC service ID (see NOTE 2)	O	The target MC service ID of the alert.
Organization name	O	The alerting MC service user's mission critical organization name
Location	O	The alerting MC service client's location
NOTE 1: This information shall be present if the message is requesting an MC service emergency alert associated with a group. NOTE 2: This information shall be present if the message is requesting an MC service emergency alert associated with an individual.		

10.10.1.1A.2 MC service emergency alert response

Table 10.10.1.1A.2-1 describes the information flow MC service emergency alert response from the MC service client to the MC service server and from the MC service server to the MC service client.

Table 10.10.1.1A.2-1: MC service emergency alert response information elements

Information Element	Status	Description
MC service ID	M	The identity of the alerting party
MC service group ID (see NOTE 1)	O	The target MC service group ID with which the alert is associated
MC service ID (see NOTE 2)	O	The target MC service ID of the alert.
NOTE 1: This information shall be present if the message is requesting an MC service emergency alert associated with a group. NOTE 2: This information shall be present if the message is requesting an MC service emergency alert associated with an individual.		

10.10.1.1A.3 MC service emergency alert cancel request

Table 10.10.1.1A.3-1 describes the information flow MC service emergency alert cancel request from the MC service client to the MC service server and from the MC service server to the MC service client.

Table 10.10.1.1A.3-1: MC service emergency alert cancel request information elements

Information Element	Status	Description
MC service ID	M	MC service user identity of the cancelling party
MC service ID (see NOTE 1)	O	MC service user identity whose emergency alert is to be cancelled
MC service group ID (see NOTE 2)	O	The MC service group ID to be informed about the alert cancellation
MC service ID (see NOTE 3)	O	MC service ID to be informed about the alert cancellation.
Group's in-progress emergency state cancel request	O	Requests cancellation of the in-progress emergency state of the group
NOTE 1: This information shall be present if the message is requesting cancellation of another MC service user's alert. If not present, then the alert of the MC service ID of the cancelling party is being cancelled NOTE 2: This information shall be present if the message is requesting cancellation of an MC service emergency alert associated with a group. NOTE 3: This information shall be present if the message is requesting cancellation of an MC service emergency alert associated with an individual.		

10.10.1.1A.4 MC service emergency alert cancel response

Table 10.10.1.1A.4-1 describes the information flow MC service emergency alert cancel response from the MC service client to the MC service server and from the MC service server to the MC service client.

Table 10.10.1.1A.4-1: MC service emergency alert cancel response information elements

Information Element	Status	Description
MC service ID	M	The identity of the cancelling party
MC service group ID (see NOTE)	O	The MC service group ID with which the alert is associated
NOTE: This information shall be present if the message is requesting cancellation of an MC service emergency alert associated with a group.		

10.10.1.1A.5 MC service emergency alert area notification

Table 10.10.1.1A.5-1 describes the information flow MC service emergency alert area notification from the MC service server to the MC service client.

Table 10.10.1.1A.5-1: MC service emergency alert area notification information elements

Information Element	Status	Description
MC service ID	M	MC service user identity of the party to be notified
Emergency Alert Area Indicator	M	An indicator that the MC service user is in an Emergency Alert Area or out of an Emergency Alert Area.

NOTE: Normally, the pre-defined area that triggers the emergency alert and the pre-defined area that triggers the out of MC service alert area notification is not the same.

10.10.1.2 MC service emergency alert

10.10.1.2.1 MC service emergency alert initiation

10.10.1.2.1.1 General

These procedures describe cases 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 an MC service group, or for communicating an alert to another MC service client. 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. These procedures will place the MC service client in the MC service emergency state if the MC service client is not already in that state.

10.10.1.2.1.2 MC service group emergency alert initiation

Figure 10.10.1.2.1.2-1 illustrates the procedure 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 to be used for emergency communications by MC service client 1 is previously defined on the group management server and MC service client 2 and MC service client 3 are affiliated to that MC service group.

NOTE 2: Alternatively, the client could have been provisioned for emergency behaviour on the currently selected 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 may not have carried out an explicit affiliation procedure with the MC service group designated as the MC service emergency group.

5. Optionally, MC service client 1 may use an activated functional alias for the group communication.

6. The MC service server may have subscribed to the MC service functional alias controlling server within the MC system for functional alias activation/de-activation updates.

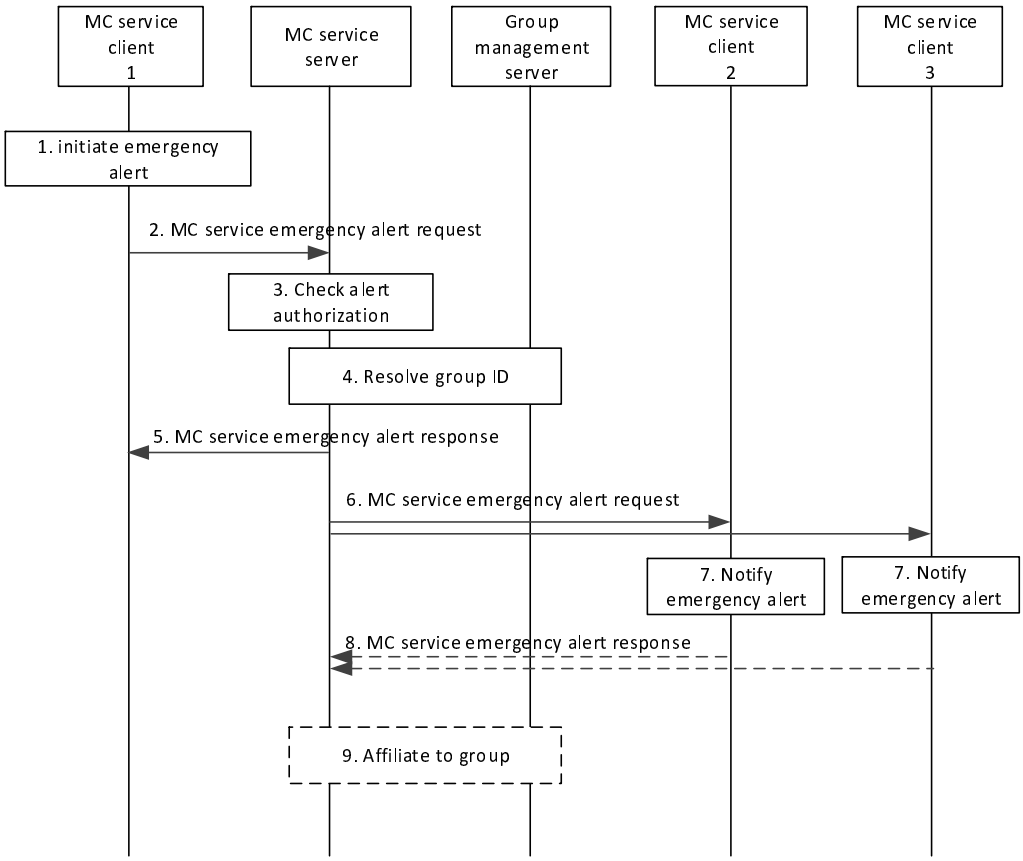

Figure 10.10.1.2.1.2-1 MC service group emergency alert

1. The MC service 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 user at MC service client 1 may select a functional alias used for the MC service group emergency alert. The MC service emergency state is retained by the MC service client 1 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 group emergency alerts for the indicated MC service group. The MC service server checks whether the provided functional alias, if present, can be used and has been activated for the user.

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. All MC service group calls made by the MC service client 1 will be sent as emergency calls until the emergency state on the MC service client 1 is cancelled. All MC service private calls made 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 user profile configuration) and the MC service user's mission critical organization name. If in step 2, the MC service client 1 does not include the location information in the MC service emergency alert request to the MC service server, the MC service server acquires the location information of the MC service user at the MC service client 1 from the location management server. If the location information is included in step 2, then the MC service server uses the location information from MC service client 1.

7. MC service users are notified of the MC service emergency alert. The functional alias of the group call initiating MC service user may be displayed.

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 in-progress emergency state.

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.

NOTE 6: It is configured whether MC service client 1 automatically triggers a subsequent MC service emergency group call.

NOTE 7: How the emergency alert is synchronized between MC services is out of scope of the present document.

10.10.1.2.1.3 MC service individual emergency alert initiation

Figure 10.10.1.2.1.3-1 illustrates the procedure for the MC service client initiating an MC service individual emergency alert. This emergency alert can be sent at the time of emergency private call initiation as specified in subclause 10.7.2.4.1 of TS 23.379 [16], or it can also be sent standalone as described below.

Pre-conditions:

1. The MC service ID of MC service client 2 is previously defined to be used for emergency communications by MC service client 1.

2. Optionally, MC service client 1 may use an activated functional alias for individual communication.

3. The MC service server may have subscribed to the MC service functional alias controlling server within the MC system for functional alias activation/de-activation updates.

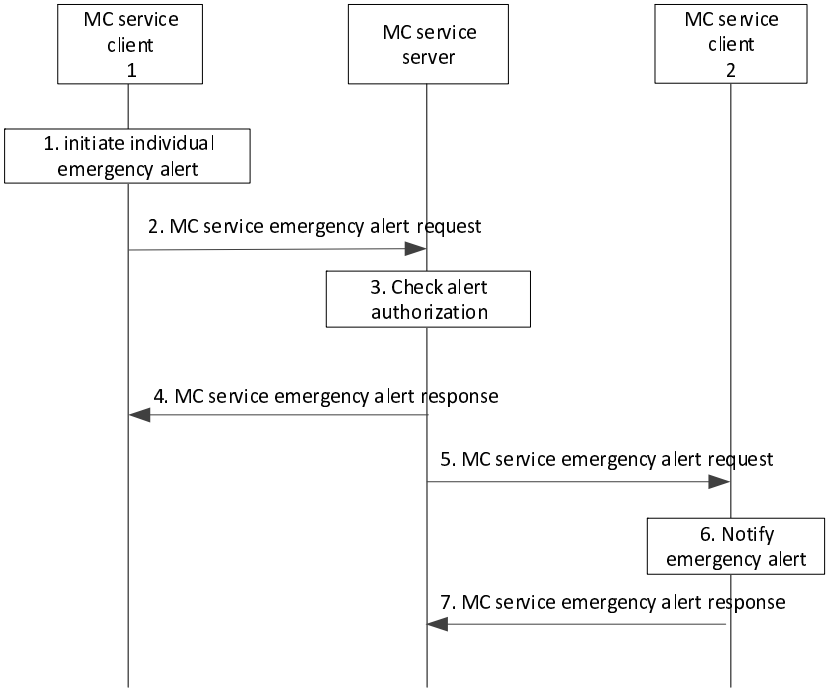

Figure 10.10.1.2.1.3-1 MC service individual emergency alert

1. The MC service user at the MC service client 1 initiates an MC service individual emergency alert. MC service client 1 sets its MC service emergency state. The MC service user at MC service client 1 may select a functional alias to be used for the MC service individual emergency alert. MCPTT client 1 retains the MC service emergency state until explicitly cancelled by the user of MC service client 1.

2. MC service client 1 requests the MC service server to send an MC service emergency alert request to MC service client 2 that has been designated as the target of MC service emergency communication by MC service client 1.

3. MC service server checks whether the MC service user of MC service client 1 is authorized for initiation of an MC service individual emergency alerts. The MC service server checks whether the provided functional alias, if present, can be used and has been activated for the user.

4. 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.

NOTE 1: While MC service client 1 is in the emergency state, all MC service group and private calls initiated by MC service client 1 are initiated as MC service emergency calls.

5. The MC service server sends an MC service emergency alert request toward MC service client 2. The MC service emergency alert request message shall contain the following information: Location, MC service ID, and the MC service user's mission critical organization name. If in step 2, the MC service client 1 does not include the location information in the MC service emergency alert request to the MC service server, the MC service server acquires the location information of the MC service user at the MC service client 1 from the location management server. If the location information is included in step 2, then the MC service server uses the location information from MC service client 1.

6. MC service user of MC service client 2 is notified of the MC service emergency alert. The functional alias of the initiating MC service user may be displayed.

NOTE 2: MC service client 2 does not set its emergency state as a result of receiving the MC service emergency alert.

7. The receiving MC service client 2 sends the MC service emergency alert response to the MC service server to acknowledge the MC service emergency alert.

NOTE 3: The MC service client 1 need not initiate a private call to MC service client 2.

10.10.1.2.2 MC service emergency alert cancel

10.10.1.2.2.1 General

These procedures describe cases where an MC service client has initiated an MC service emergency alert and entered the emergency state, and wishes to cancel the alert. For group-based alerts the cancellation informs 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 in-progress emergency state of the group. For individual-based alerts the cancellation informs the MC service server and the MC service user designated as the target of MC service emergency communication.

In both cases the cancellation of the MC service emergency alert clears the emergency state of the MC service client.

For group-based emergency alerts, the emergency state of the MC service user can alternatively be cancelled using the MC service in-progress emergency group state cancellation procedures in 3GPP TS 23.379 [16], TS 23.281[12], and TS 23.282 [13].

10.10.1.2.2.2 MC service group emergency alert cancel

Figure 10.10.1.2.2.2-1 illustrates the procedure for the MC service client cancelling 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 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 targeted to a group.
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.

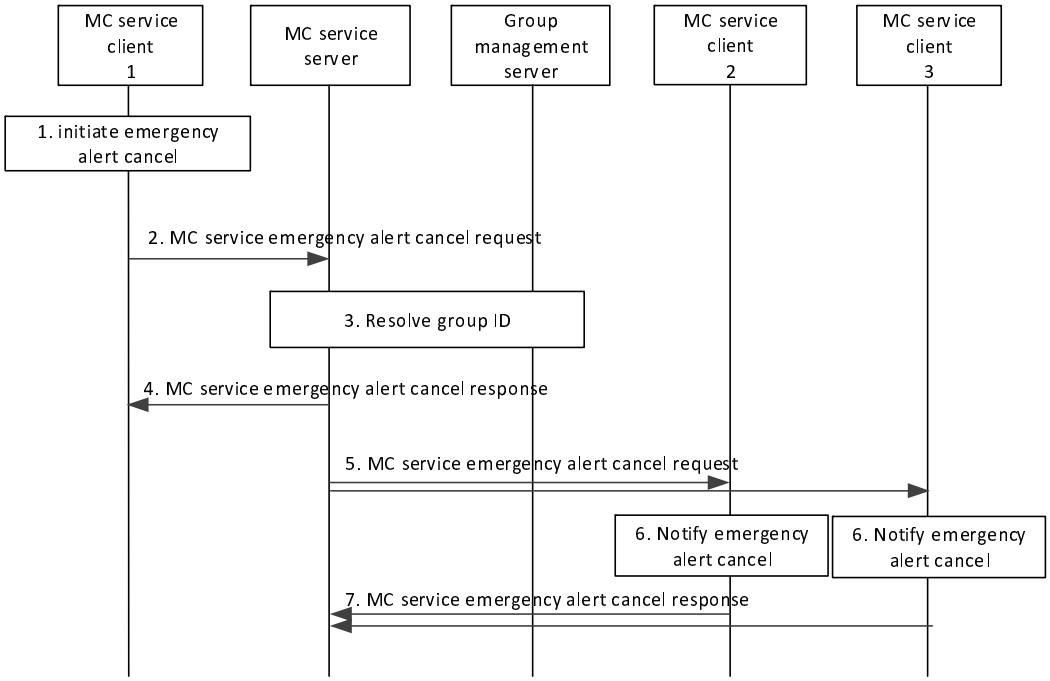

Figure 10.10.1.2.2.2-1 MC service group emergency alert cancel

1. The MC service user at the MC service client 1 initiates an MC service emergency alert cancel to inform the server that MC service client 1 is no longer in the emergency state.

NOTE 2: The MC service emergency alert cancel request can carry an indication to also request that the in-progress emergency of the group is to be cancelled. The MC service server can accept or deny the request to cancel the in-progress emergency state of the group as a whole, separately from accepting or denying the request to cancel the emergency alert at MC service client 1. An authorized user (e.g. dispatcher, supervisor) can cancel either or both the in-progress emergency state of the group and the MC service emergency alert of another user. A MC service user is always authorized to cancel the emergency state of their own client. Determination of authorized users is implementation dependent.

2. MC service client 1 requests the MC service server to send an MC service emergency alert 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 alert cancel response to the MC service client 1 to confirm the MC service emergency alert cancel request. MC service client 1 clears its emergency state.

5. The MC service server sends an MC service emergency alert 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 alert cancellation of MC service client 1.

7. For a unicast MC service emergency alert cancel, the receiving MC service clients send the MC service emergency alert cancel response to the MC service server to acknowledge the MC service emergency alert cancel. For a multicast MC service emergency alert cancel, these acknowledgements are not sent unless the MC service clients have been configured to do so.

10.10.1.2.2.3 MC service individual emergency alert cancel

Figure 10.10.1.2.2.3-1 illustrates the procedure for the MC service client cancelling an individual MC service emergency alert (i.e. without an associated MC service group).

Pre-conditions:

1. The MC service client 1 had previously successfully initiated an individual MC service emergency alert targeted to MC service client 2.

2. The MC service client 1 is still in the emergency state.

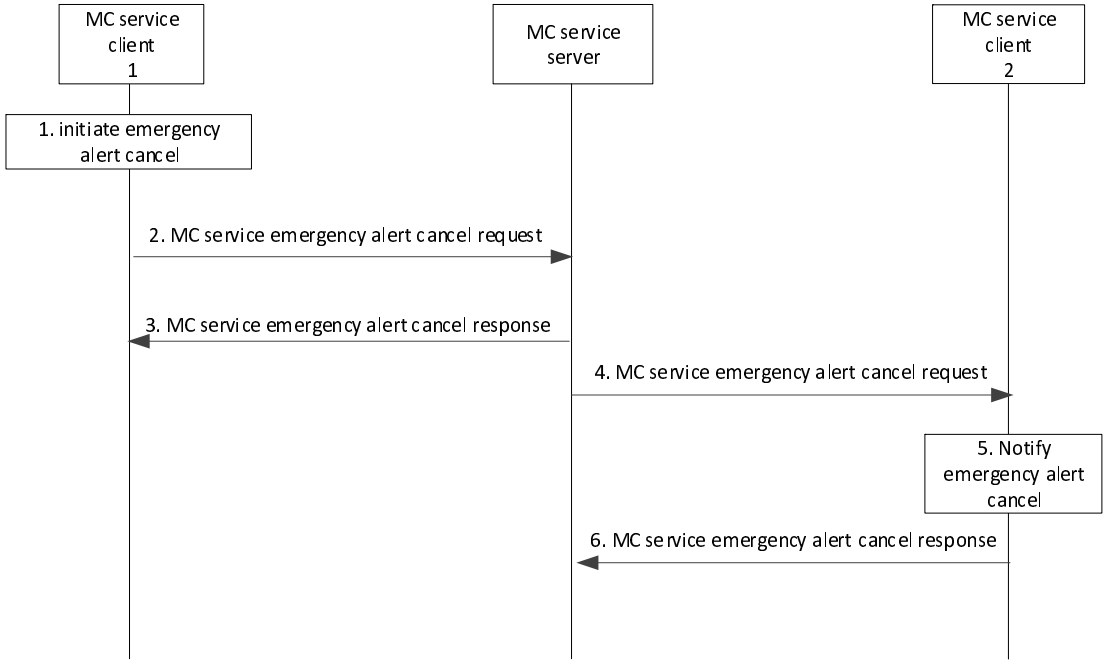

Figure 10.10.1.2.2.3-1 MC service individual emergency alert cancel

1. The MC service user at the MC service client 1 initiates an MC service individual emergency alert cancel for an individual emergency alert.

2. MC service client 1 sends the MC service emergency alert cancel request to the MC service server to inform the server that MC service client 1 is no longer in the emergency state. The emergency alert cancel request contains the MC service ID of MC service client 2.

3. The MC service server sends the MC service emergency alert cancel response to the MC service client 1 to confirm the MC service emergency alert cancel request. MC service client 1 clears its emergency state.

4. The MC service server sends an MC service emergency alert cancel request towards MC service client 2.

5. The MC service user of MC service client 2 is notified of the MC service emergency alert cancellation of MC service client 1.

6. MC service client 2 sends the MC service emergency alert cancel response to the MC service server to acknowledge the MC service emergency alert cancel.

10.10.1.2.3 Entering MC service emergency alert area

The procedure focuses on the case where an MC service emergency alert to be triggered when an MC service UE moves into a pre-defined area. 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 10.10.1.2.3-1 are the signalling control plane procedures for the MC service server triggering 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 MC service group management server. 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.

NOTE: 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. An area in which the MC service client should send emergency alert is pre-defined in MC service server.

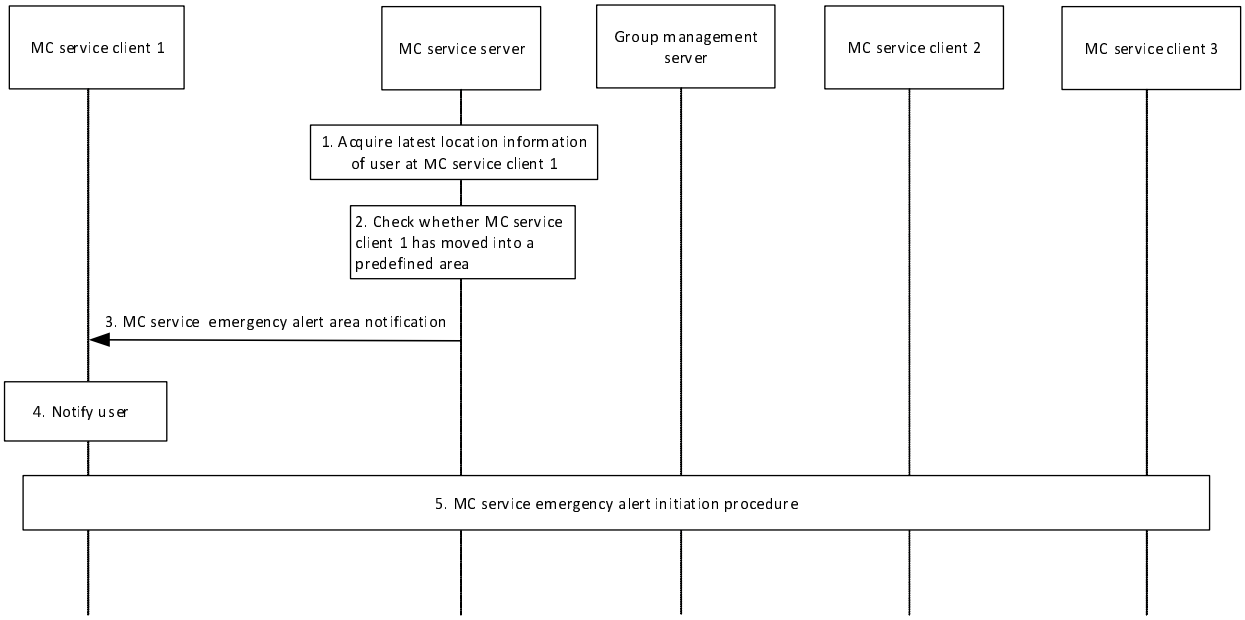

Figure 10.10.1.2.3-1 Entering MC service emergency alert area

1. MC service server acquires the latest location information of user at MC service client 1 from location management server as described in 10.9.3.6.
2. MC service server checks whether MC service client 1 has moved into a pre-defined area.
3. If so, MC service server sends an MC service emergency alert area notification to MC service client 1 to notify that it has moved into the area in potential danger.
4. MC service client 1 notifies the MC service user about the MC service emergency alert area.
5. MC service client 1 initiates MC service emergency alert procedure as described in 10.10.1.2.1.

10.10.1.2.4 Leaving MC service emergency alert area

This procedure focuses on the case where a notification is sent when an MC service UE moves out of a pre-defined area. This procedure will notify the MC service client that it is now out of the pre-defined emergency alert area. It is up to the MC service user at that MC service client to determine if the emergency state is to be cleared or not.

Procedures in figure 10.10.1.2.4-1 are the signalling control plane procedures for the MC service server sends an MC service emergency alert area notification. It is optional if the MC service user wants to initiate the MC service emergency alert cancel procedure to inform the members in the MC service group that its emergency condition is over.

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. This MC service group has been pre-defined for communicating the emergency alert in the user profile.
2. All members of the MC service group belong to the same MC system.

3. An area in which the emergency alert for the MC service client should remain active is pre-defined in MC service server.

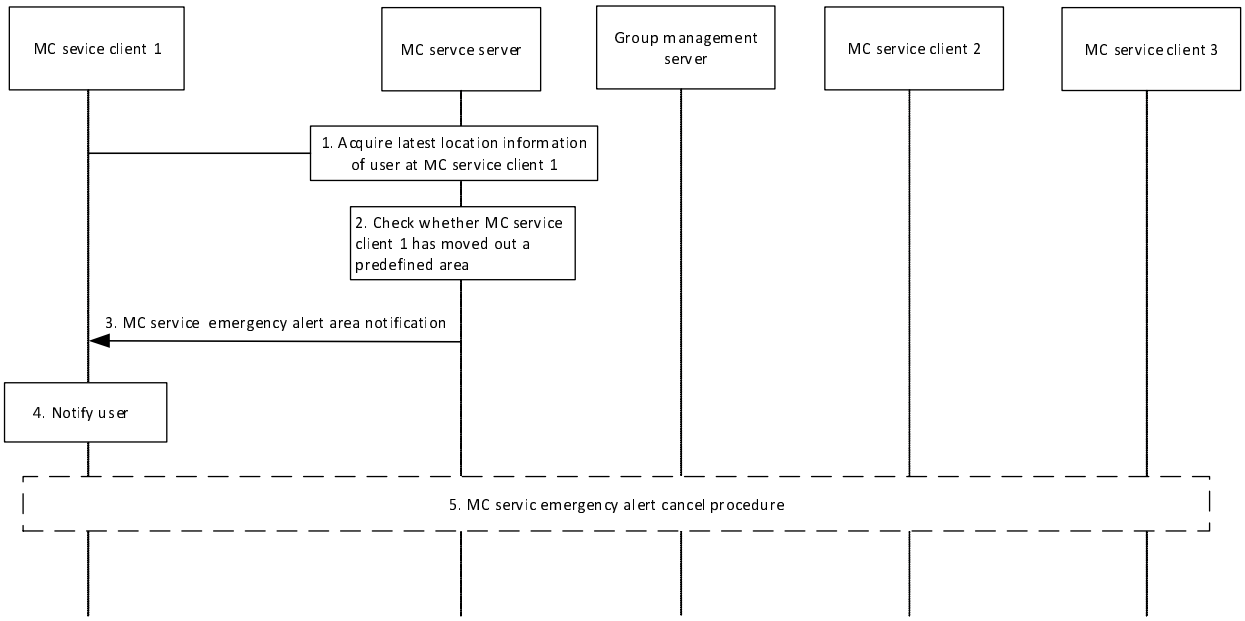

Figure 10.10.1.2.4-1 Leaving MC service emergency alert area

1. MC service server acquires the latest location information of user at MC service client 1 from location management server as described in subclause 10.9.3.6.

2. MC service server checks whether MC service client 1 has moved out a pre-defined area.

3. If so, MC service server sends an MC service emergency alert area notification to MC service client 1 to notify that it has moved out of the area in potential danger.

4. MC service client 1 notifies the MC service user about the MC service emergency alert area cancel. It is up to the MC service user at the MC service client 1 to determine if the emergency state is clear.

5. Optionally, the MC service user of MC service client 1 initiates MC service emergency alert cancel procedure as described in 10.10.1.2.2.

NOTE 2: It is up to the MC service user to clear the local emergency state on the client after the MC service UE has moved out of the emergency alert area, the MC service server cannot clear the client's local emergency state.

10.10.2 Off-network emergency alert

10.10.2.1 General

The following subclauses specify the procedures for emergency alert initiation and emergency alert cancel that are utilised by the following MC services:

- MCPTT
- MCVideo
- MCData

10.10.2.1A Information flows

10.10.2.1A.1 MC service emergency alert announcement

Table 10.10.2.1A.1-1 describes the information flow for the MC service emergency alert announcement from the MC service client to the other MC service clients.

Table 10.10.2.1A.1-1: MC service emergency alert announcement information elements

Information Element	Status	Description
MC service ID	M	The identity of the alerting MC service user
MC service group ID	M	The MC service group ID with which the alert is associated
Location	O	The alerting client's location, if known
Organization name	M	The alerting user's mission critical organization name

10.10.2.1A.2 MC service emergency alert cancel announcement

Table 10.10.2.1A.2-1 describes the information flow for the MC service emergency alert cancel announcement from the MC service client to other MC service clients.

Table 10.10.2.1A.2-1: MC service emergency alert cancel announcement information elements

Information Element	Status	Description
MC service ID	M	The identity of the cancelling MC service user
MC service group ID	M	The MC service group ID with which the alert is associated

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 clients 2 and 3 belong to and are ready for off-network communications on the MC service group.

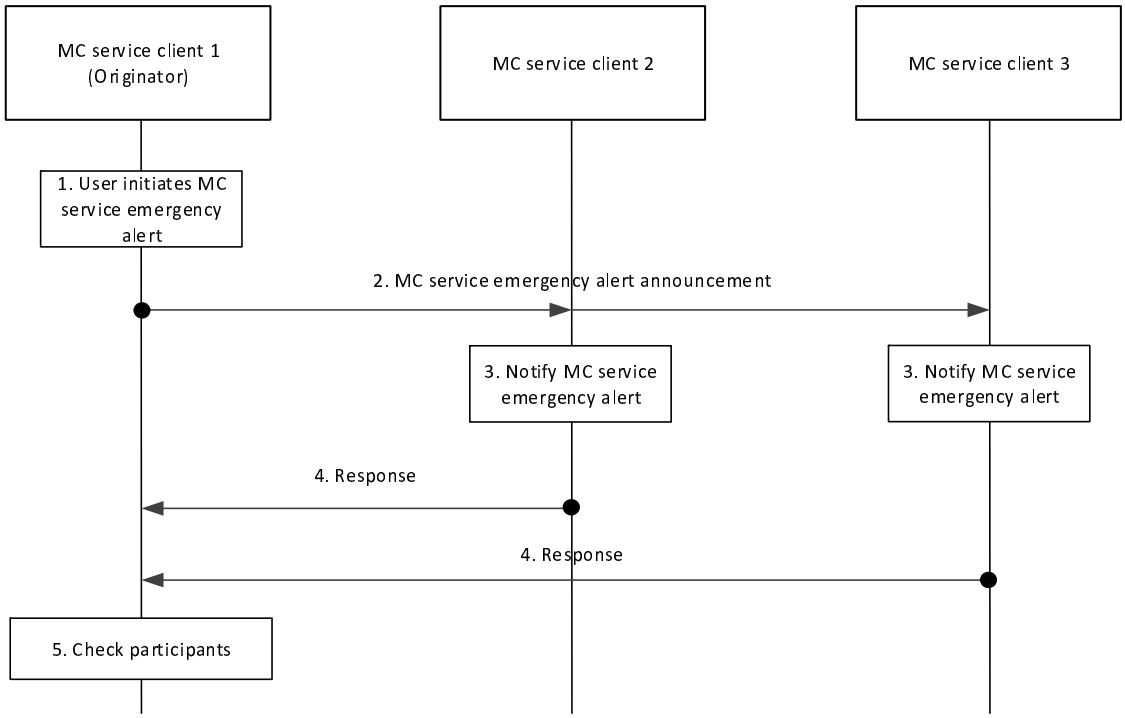

Figure 10.10.2.2.1-1: Emergency alert initiation

1. 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.

2. MC service client 1 sends an MC service emergency alert announcement to the other participants on the MC service emergency group. 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 state.

3. MC service users are notified of the MC service emergency state of the originating MC service user.

4. 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: Sending the emergency alert without making a request to also start an emergency call does not put the group into the in-progress emergency state.

NOTE 4: The MC service client 1 needs 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 5: MC service clients need to respond only to the first emergency alert announcement message that is received.

NOTE 6: It is configured if MC service client 1 will automatically trigger a subsequent MC service emergency group call.

5. 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 alert cancel

An MC service client has initiated an MC service emergency alert, has entered the MC service emergency state and wishes to cancel the alert, 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 state 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 alert.

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. The initiating MC service client 1 and MC service clients 2 and 3 are still in off-network contact via the MC service group provisioned to MC service client 1 as for the MC service emergency group.

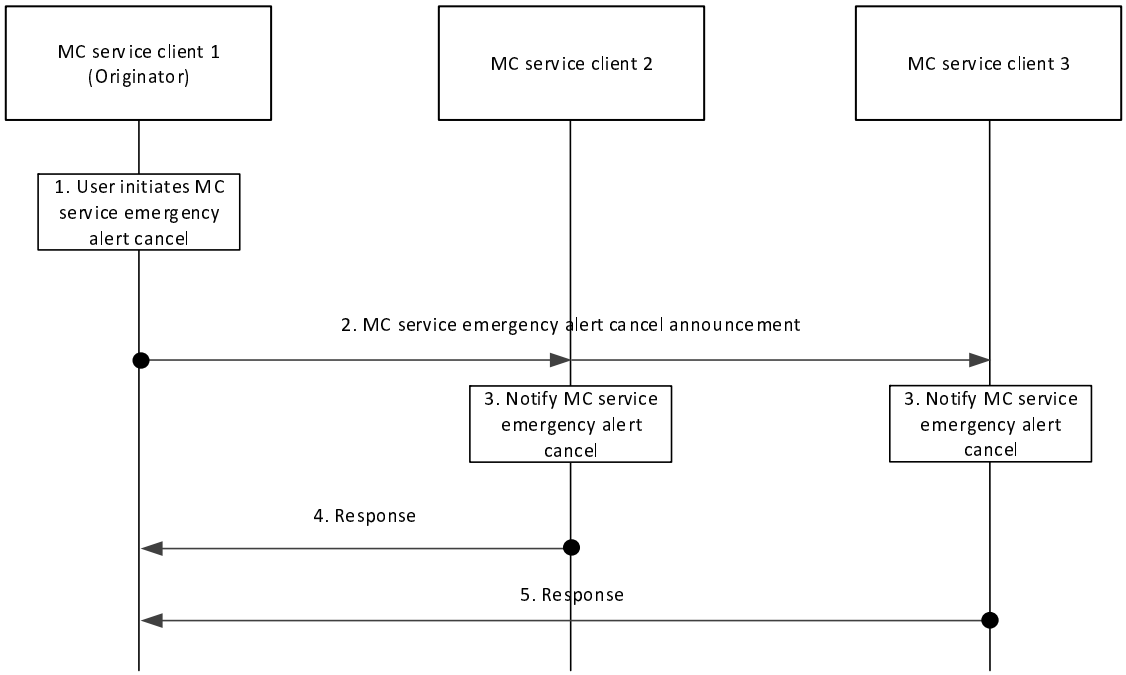

Figure 10.10.2.2.2-1 Emergency alert cancel

1. The user at the MC service client 1 initiates an MC service emergency alert cancel.
2. MC service client 1 sends an MC service emergency alert cancel announcement to the MC service group to which MC service client 1 had previously sent the emergency alert announcement message.
3. MC service users are notified of the MC service emergency alert cancellation by MC service client 1.
4. The receiving MC service clients acknowledge the MC service emergency alert 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.

10.10.3 Ad hoc group emergency alert

10.10.3.1 General

The following subclauses specify the procedures for ad hoc group emergency alert initiation, ad hoc group emergency alert cancel, entering an ongoing ad hoc group emergency alert and leaving an ad hoc group emergency alert that are utilised by the following MC services:

- MCPTT
- MCVideo
- MCData

10.10.3.2 Information flows

10.10.3.2.1 Ad hoc group emergency alert request (MC service client – MC service server)

Table 10.10.3.2.1-1 describes the information flow ad hoc group emergency alert request from the MC service client to the MC service server.

Table 10.10.3.2.1-1 Ad hoc group emergency alert request information elements

Information Element	Status	Description
MC service ID	M	The identity of the alerting party
Functional alias	O	The functional alias of the alerting party
Ad hoc group ID (see NOTE)	O	The group ID which is generated by the MC service user to be used for the ad hoc group alert
Organization name	O	The alerting MC service user's mission critical organization name
Location information	O	The alerting MC service client's location
Criteria for determining the participants	M	Carries the details of criteria or meaningful label identifying the criteria or the combination of both which will be used by the MC service server for determining the participants e.g., it can be a location-based criteria to invite participants in a particular area
Additional information	O	The alerting party may provide additional information related to the alert, e.g., medical help needed or reason for the alert
NOTE: If this information element is not included, then the MC service server shall assign one to be used for the ad hoc group emergency alert and shall return it to the alerting party.		

10.10.3.2.2 Ad hoc group emergency alert request (MC service server – MC service client)

Table 10.10.3.2.2-1 describes the information flow ad hoc group emergency alert request from the MC service server to the MC service client.

Table 10.10.3.2.2-1 Ad hoc group emergency alert request information elements

Information Element	Status	Description
MC service ID	M	The identity of the alerting party
Functional alias	O	The functional alias of the alerting party
Ad hoc group ID	M	The target group ID associated with the alert
Organization name	O	The alerting MC service user's mission critical organization name
Location information	O	The alerting MC service client's location
Additional information	O	The alerting party may provide additional information related to the alert, e.g., medical help needed or reason for the alert

10.10.3.2.2a Ad hoc group emergency alert request return

Table 10.10.3.2.2a-1 describes the information flow ad hoc group emergency alert request return from the MC service server to the MC service client.

Table 10.10.3.2.2a-1 Ad hoc group emergency alert request return information elements

Information Element	Status	Description
MC service ID	M	The identity of the alerting party
Functional alias	O	The functional alias of the alerting party
Authorization result	M	Indicate if authorization is success or failure

10.10.3.2.3 Ad hoc group emergency alert response

Table 10.10.3.2.3-1 describes the information flow ad hoc group emergency alert response from the MC service client to the MC service server and from the MC service server to the MC service client.

Table 10.10.3.2.3-1 Ad hoc group emergency alert response information elements

Information Element	Status	Description
MC service ID	M	The identity of the target party
Functional alias	O	The functional alias of the target party
Ad hoc group ID	M	The target group ID associated with the alert

10.10.3.2.4 Ad hoc group emergency alert cancel request

Table 10.10.3.2.4-1 describes the information flow ad hoc group emergency alert cancel request from the MC service client to the MC service server and from the MC service server to the MC service client.

Table 10.10.3.2.4-1 Ad hoc group emergency alert cancel request information elements

Information Element	Status	Description
MC service ID	M	MC service user identity of the cancelling party
Functional alias	O	The functional alias of the cancelling party
MC service ID (see NOTE)	O	MC service user identity whose emergency alert is requested to be cancelled
Ad hoc group ID	M	The ad hoc group ID with which the alert is associated
Group's in-progress emergency state cancel request	O	Requests cancellation of the in-progress emergency state of the group
NOTE: This information shall only be present if the message is requesting cancellation of another MC service user's alert. If not present, then the alert of the MC service ID of the cancelling party is being cancelled.		

10.10.3.2.4a Ad hoc group emergency alert cancel request return

Table 10.10.3.2.4a-1 describes the information flow ad hoc group emergency alert cancel request return from the MC service server to the MC service client.

Table 10.10.3.2.4a-1 Ad hoc group emergency alert cancel request return information elements

Information Element	Status	Description
MC service ID	M	The identity of the cancelled party
Functional alias	O	The functional alias of the cancelled party
Authorization result	M	Indicate if authorization is success or failure

10.10.3.2.5 Ad hoc group emergency alert cancel response

Table 10.10.3.2.5-1 describes the information flow ad hoc group emergency alert cancel response from the MC service client to the MC service server and from the MC service server to the MC service client.

Table 10.10.3.2.5-1 Ad hoc group emergency alert cancel response information elements

Information Element	Status	Description
MC service ID	M	The identity of the cancelled party
Functional alias	O	The functional alias of the cancelled party
Ad hoc group ID	M	The ad hoc group ID associated with the alert

10.10.3.2.6 Ad hoc group emergency alert participants list notification

Table 10.10.3.2.6-1 describes the information flow ad hoc group emergency alert participants list notification from the MC service server to the MC service client.

Table 10.10.3.2.6-1 Ad hoc group emergency alert participants list notification information elements

Information Element	Status	Description
MC service ID	M	The identity of the notified participant
Functional alias	O	The functional alias of the notified participant
Ad hoc group ID	M	The group ID associated with the ad hoc group emergency alert
MC service user ID list	O	The total list of MC service users who belong to the ad hoc group irrespective of having acknowledged the ad hoc group emergency alert or not
MC service user ID list	O	The list of MC service users who belong to the ad hoc group but have not acknowledged the ad hoc group emergency alert

10.10.3.2.7 Ad hoc group emergency alert get userlist request

Table 10.10.3.2.7-1 describes the information flow of an ad hoc group emergency alert get userlist request sent from an MC service server at a primary MC system to another MC service server at a partner MC system.

Table 10.10.3.2.7-1 Ad hoc group emergency alert get userlist request

Information Element	Status	Description
Criteria for determining the participants	M	Carries the details of criteria or meaningful label identifying the criteria or the combination of both which will be used by the MC service server for determining the participants, e.g., it can be a location-based criteria to invite participants in a particular area
MC group ID	M	The identity of the ad hoc group associated with the emergency alert

10.10.3.2.8 Ad hoc group emergency alert get userlist response

Table 10.10.3.2.8-1 describes the information flow of an ad hoc group emergency alert get userlist response sent from an MC service server at a partner MC system to the MC service server at the primary MC system, whose MC service user has initiated the ad hoc group emergency alert.

Table 10.10.3.2.8-1 Ad hoc group emergency alert get userlist response

Information Element	Status	Description
MC service ID list	M	List of MC service IDs meeting the criteria specified in the ad hoc group emergency alert get userlist request
MC group ID	M	The identity of the ad hoc group associated with the emergency alert

10.10.3.2.9 Ad hoc group emergency alert user add notification

Table 10.10.3.2.9-1 describes the information flow of an ad hoc group emergency alert user add notification sent from an MC service server at a partner MC system to the MC service server at the primary MC system, whose MC service user has initiated the ad hoc group emergency alert.

Table 10.10.3.2.9-1 Ad hoc group emergency alert user add notification

Information Element	Status	Description
MC service ID	M	The identity of an MC service client to be added to an ongoing ad hoc group emergency alert
MC group ID	M	The identity of the ad hoc group associated with the emergency alert

10.10.3.2.10 Ad hoc group emergency alert user remove notification

Table 10.10.3.2.10-1 describes the information flow of an ad hoc group emergency alert user remove notification sent from an MC service server at a partner MC system to the MC service server at the primary MC system, whose MC service user has initiated the ad hoc group emergency alert.

Table 10.10.3.2.10-1 Ad hoc group emergency alert user remove notification

Information Element	Status	Description
MC service ID	M	The identity of an MC service client to be removed from an ongoing ad hoc group emergency alert
MC group ID	M	The identity of the ad hoc group associated with the emergency alert

10.10.3.2.11 Ad hoc group emergency alert notify

Table 10.10.3.2.11-1 describes the information flow for an ad hoc group emergency alert notify sent from MC service server to MC service client.

Table 10.10.3.2.11-1: Ad hoc group emergency alert notify

Information element	Status	Description
MC service ID	M	The identity of the MC service client participating in the ad hoc group emergency alert
Functional alias	O	The associated functional alias of the MC service user of the ad hoc group emergency alert participant
MC group ID	M	The ad hoc MC group ID associated with the emergency alert
MC service ID list	O	The list of the invited MC service users who acknowledge the ad hoc group emergency alert request, when MC service users join or leave the ad hoc group emergency alert. Or the list of the participating MC service users in the terminated ad hoc group emergency alert.

10.10.3.3 Procedures within single MC system

10.10.3.3.1 Ad hoc group emergency alert initiation

Figure 10.10.3.3.1-1 illustrates the procedure for the MC service client initiating an ad hoc group emergency alert initiated by an authorized MC service user.

Pre-conditions:

1. The MC service user at MC service client 1 wants to send an ad hoc group emergency alert to the MC service users who are satisfying certain criteria.
2. All MC service clients belong to the same MC system.
3. The MC service user on MC service client 3 is authorized to receive ad hoc group participants information.

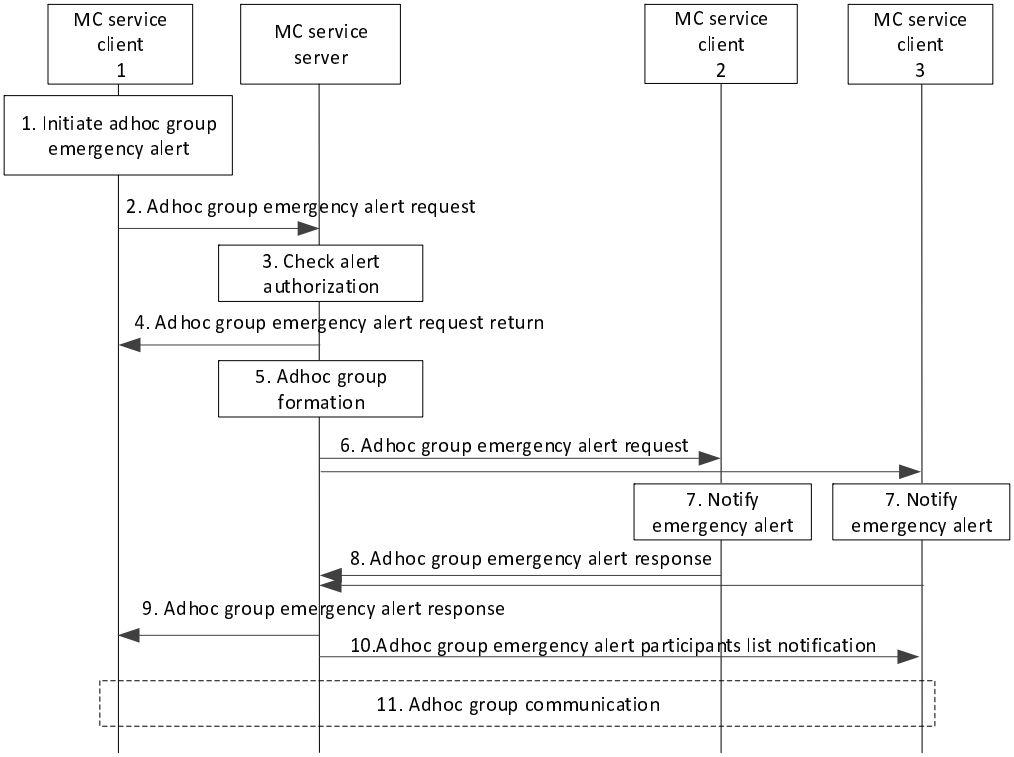

Figure 10.10.3.3.1-1: Ad hoc group emergency alert initiation

1. The MC service user at the MC service client 1 initiates an ad hoc group emergency alert to an ad hoc group with participants satisfying specific criteria. The MC service user may add additional information describing the reason for sending the alert.
2. MC service client 1 initiates the ad hoc group emergency alert by sending the ad hoc group emergency alert request containing the details of the criteria to be applied by the MC service server for determining the participants list or the list of participants. MC service client 1 may set its MC service emergency state. The MC service user at MC service client 1 may select a functional alias used for the MC service group emergency alert. If MC service client 1 is in MC service emergency state, the MC service emergency state is retained by the MC service client 1 until explicitly cancelled.
3. MC service server checks whether the MC service user of MC service client 1 is authorized for initiation of ad hoc group emergency alerts and whether the request is supported. The MC service server checks whether the provided functional alias, if present, can be used and has been activated for the user.
4. The MC service server sends the ad hoc group emergency alert request return to the MC service user 1 containing the result of whether the ad hoc group call is authorized or not. If the ad hoc group emergency alert

request is not authorized, the MC service server and the MC service client 1 shall not proceed with the rest of the steps.

5. The MC service server determines the list of participants to be invited for the ad hoc group emergency alert based on the information present in the information element Criteria for determining the participants. This information element could carry either criteria or indicator identifying the criteria or combination of both. The MC service server stores the ad hoc group ID together with the list of participants for the duration of the ad hoc group emergency alert. The MC service server considers the alerted participants as implicitly affiliated to the ad hoc group.

6. The MC service server sends an ad hoc group emergency alert request including the ad hoc group ID towards the MC service clients 2 and 3.

7. MC service users are notified of the ad hoc group emergency alert. The functional alias of the MC service user initiating the ad hoc group emergency alert and additional information related to the alert may be displayed.

8. The receiving MC service clients send the ad hoc group emergency alert response to the MC service server to acknowledge the ad hoc group emergency alert.

9. The MC service server sends the ad hoc group emergency alert response to MC service client 1 to inform about successful alert establishment, containing the ad hoc group ID (generated by the MC service server in the case where the MC service ad hoc group ID created by the MC service client 1 is not acceptable or the case where the MC service ad hoc group ID was not provided by MC service client 1).

10. The authorized user on MC service client 3 is notified with the total list of MC service IDs of those MC service users who belong to the ad hoc group and a separate list of MC service IDs of MC service users who belong to the ad hoc group that have not acknowledged the ad hoc group emergency alert.

11. If configured, an MC service client may setup a subsequent ad hoc group emergency communication, using the ad hoc group ID from the ad hoc group emergency alert, according to 3GPP TS 23.379 [16], 3GPP TS 23.281 [12] or 3GPP TS 23.282 [13].

NOTE 1: MC service client 1 may start the subsequent ad hoc group emergency communication after step 5.

NOTE 2: Sending the ad hoc group emergency alert without making a request to also start an ad hoc group emergency communication does not put the group into the in-progress emergency state.

NOTE 3: Sending the ad hoc group emergency alert does not put the other participants in the group into an MC service emergency state.

The MC service server shall resend an ad hoc group emergency alert request towards MC service client(s) who still satisfy the criteria but did not acknowledge the ad hoc group emergency alert.

The MC service server continuously checks whether other MC service clients meet or if participating MC service clients no longer meet the criteria for the ad hoc group emergency alert.

10.10.3.3.2 Ad hoc group emergency alert cancel

Figure 10.10.3.3.2-1 illustrates the procedure for the MC service client cancelling an ad hoc group emergency alert associated with an ad hoc group i.e., MC service users on MC service client 1, MC service client 2 and MC service client 3 belong to the same ad hoc group.

Pre-conditions:

1. The MC service client 1 is authorised to cancel the ad hoc group emergency alert (as configured in the user profile data according to 3GPP TS 23.379 [16], 3GPP TS 23.281 [4] or 3GPP TS 23.282 [5]).

2. The initiating MC service client 1 is a participant of the ad hoc group associated with the ongoing emergency alert.

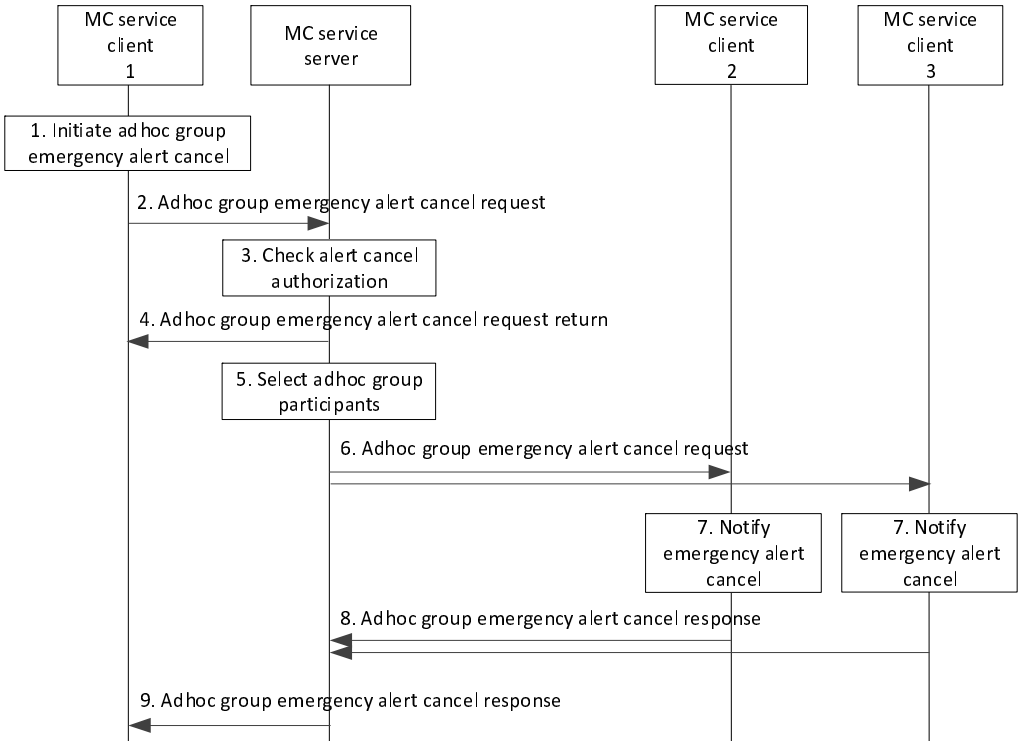

Figure 10.10.3.3.2-1: Ad hoc group emergency alert cancel

1. The MC service user at the MC service client 1 initiates an ad hoc group emergency alert cancel to inform the MC service server that alert is to be cancelled.

NOTE 1: The ad hoc group emergency alert cancel request can carry an indication to also request that the in-progress emergency of the group is to be cancelled. The MC service server can accept or deny the request to cancel the in-progress emergency state of the group, separately from accepting or denying the request to cancel the emergency alert at MC service client 1.

2. MC service client 1 sends an ad hoc group emergency alert cancel request to the MC service server. If the cancel request is for another MC service user that initiated this emergency alert, that user's MC service ID shall be included in the request.

3. MC service server checks whether the MC service user of MC service client 1 is authorized for cancellation of ad hoc group emergency alerts and whether the request is supported.

4. The MC service server sends the ad hoc group emergency alert cancel request return to the MC service client 1 containing the result of whether the ad hoc group emergency alert cancel is authorized or not. If the ad hoc group emergency alert cancel is not authorized, the MC service server and the MC service client 1 shall not proceed with the rest of the steps.

5. MC service server uses the ad hoc group ID to select the participants of that ad hoc group. If MC service client 1 has initiated the ad hoc group emergency alert and its MC service emergency state is set, then the MC service emergency state is cleared.NOTE 2: If MC service client 1 has not initiated the ad hoc group emergency alert, the MC service emergency state on the MC service client which initiated the ad hoc group emergency alert is retained locally by the MC service client until explicitly manually cancelled by the MC service user.

NOTE 3: The MC service emergency state of an MC service client due to an ad hoc group emergency alert or an ad hoc group communication is considered as a different state as from an MC service emergency state set by an MC service emergency group call or an MC service group emergency alert.

6. The MC service server sends an ad hoc group emergency alert cancel request towards the participants of the ad hoc group associated with the ad hoc group emergency alert.

7. MC service users are notified of the ad hoc group emergency alert cancellation and the MC service emergency state is cleared.

8. The receiving MC service clients send the ad hoc group emergency alert cancel response to the MC service server to acknowledge the ad hoc group emergency alert cancel.

9. The MC service server sends the ad hoc group emergency alert cancel response to MC service client 1 to inform about successful alert cancellation.

NOTE 4: If there is no ongoing communication in the ad hoc group or once the ongoing communication in the ad hoc group is terminated, the MC service server removes the ad hoc group.

10.10.3.3.3 Entering an ongoing ad hoc group emergency alert

During an ongoing ad hoc group emergency alert, the MC service server continuously checks if additional MC service users meet the conditions of the ad hoc group emergency alert.

As illustrated in Figure 10.10.3.3.3-1 MC service client is added to the ad hoc group as the MC service client meets the criteria for receiving an ongoing ad hoc group emergency alert.

Pre-conditions:

1. An ad hoc group emergency alert has been initiated and the related ad hoc group exists.

2. The criteria for entering an ad hoc group emergency alert are known to the MC service server.

3. The MC service user on MC service client 2 is authorized to receive ad hoc group participants information.

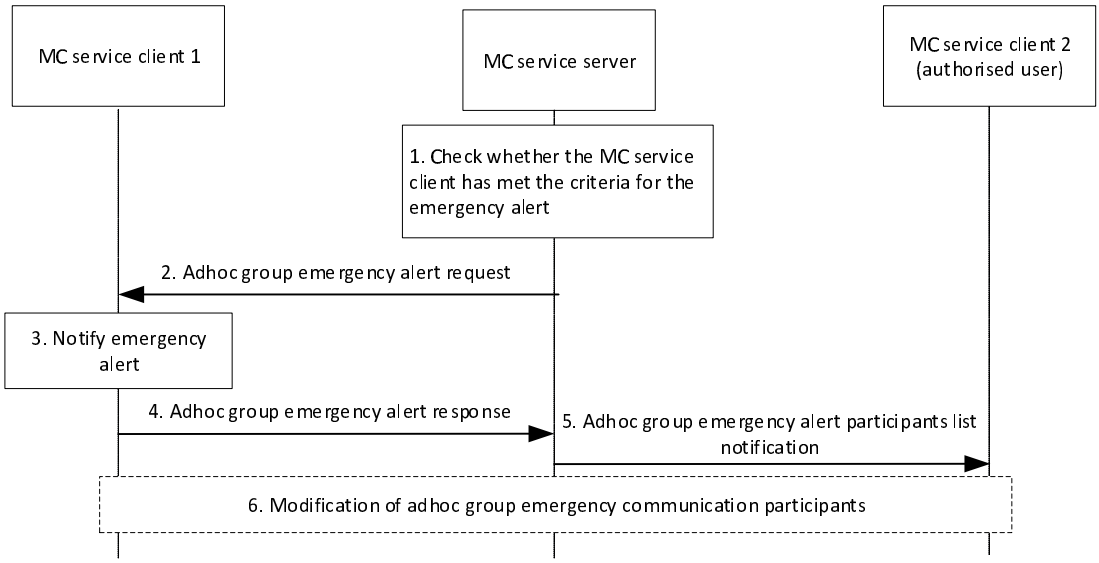

Figure 10.10.3.3.3-1: Entering an ongoing ad hoc group emergency alert

1. MC service server acquires the latest information of the MC service user at the MC service client and checks whether the criteria for initiating an ad hoc group emergency alert to the MC service client are met. The MC service server considers the MC service client 1 to be implicitly affiliated to the ad hoc group associated to the emergency alert.

2. The MC service server sends an ad hoc group emergency alert request notification to MC service client 1 to notify that it has moved into potential danger. The MC service client 1 is added to the emergency ad hoc group.

3. MC service client 1 notifies the MC service user about the ad hoc group emergency alert.

4. The receiving MC service client 1 sends the ad hoc group emergency alert response to the MC service server to acknowledge the ad hoc group emergency alert.

5. The authorized user on MC service client 2 is notified with the total list of MC service IDs of those MC service users who belong to the ad hoc group including the newly added MC service client 1, and a separate list of MC service IDs of MC service users who belong to the ad hoc group that have not acknowledged the ad hoc group emergency alert.

6. If there is an ongoing ad hoc group emergency communication ongoing, the MC service server adds the MC service client to the list of ad hoc group emergency communication participants according to 3GPP TS 23.379 [16], 3GPP TS 23.281 [12] or 3GPP TS 23.282 [13].

10.10.3.3.4 Leaving an ad hoc group emergency alert

During an ongoing ad hoc group emergency alert, the MC service server continuously checks if MC service users still meet the conditions of the emergency alert.

As illustrated in Figure 10.10.3.3.4-1 MC service client is removed from the ad hoc group associated with an ongoing ad hoc group emergency alert as the MC service client does not meet the criteria for the alert any longer and the emergency alert is removed from the MC service client.

Pre-conditions:

1. An ad hoc group emergency alert has been initiated and the related ad hoc group exists.
2. The MC service server is aware of the criteria for leaving an ad hoc emergency alert.
3. The MC service user on MC service client 2 is authorized to receive ad hoc group participants information.

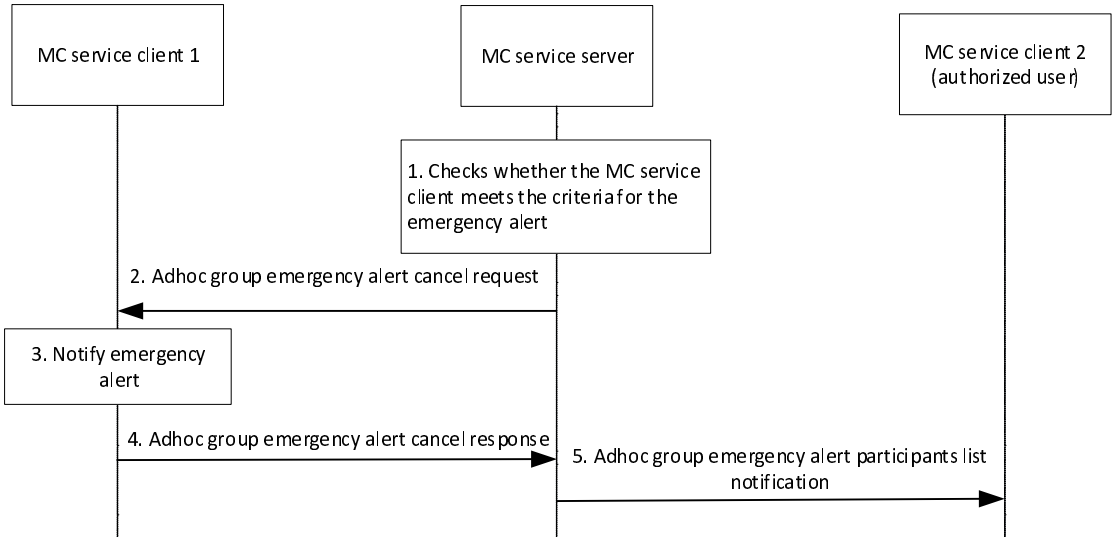

Figure 10.10.3.3.4-1: Leaving an ad hoc group emergency alert

1. MC service server acquires the latest information of the MC service user at the MC service client 1 and checks whether the criteria for the ad hoc group emergency alert are still met. The MC service server deaffiliates the MC service client 1 from the ad hoc group associated to the emergency alert.
2. The MC service server sends an ad hoc group emergency alert cancel request to MC service client 1. The MC service client 1 is removed from the ad hoc group.
3. MC service client 1 notifies the MC service user that the emergency alert is cancelled.
4. The receiving MC service client 1 sends the ad hoc group emergency alert cancel response to the MC service server to acknowledge that the ad hoc group emergency alert is cancelled for this MC service user.
5. The authorized user on MC service client 2 is notified with the MC service IDs of those MC service users who are currently in the ad hoc group after removing MC service client 1 from the list.

NOTE: If a communication is ongoing in the ad hoc group for the MC service user, the MC service server will wait to remove the MC service user from the ad hoc group until the communication is terminated.

10.10.3.4 Procedures within multiple MC systems

10.10.3.4.1 Ad hoc group emergency alert initiation

Figure 10.10.3.4.1-1 illustrates the procedure for initiating of ad hoc emergency alert within multiple MC systems.

Preconditions:

- The MC service user 1 belonging to MC system A initiates an ad hoc group emergency alert that involves MC service users from MC system A and MC system B.
- The MC system A and MC system B are interconnected.

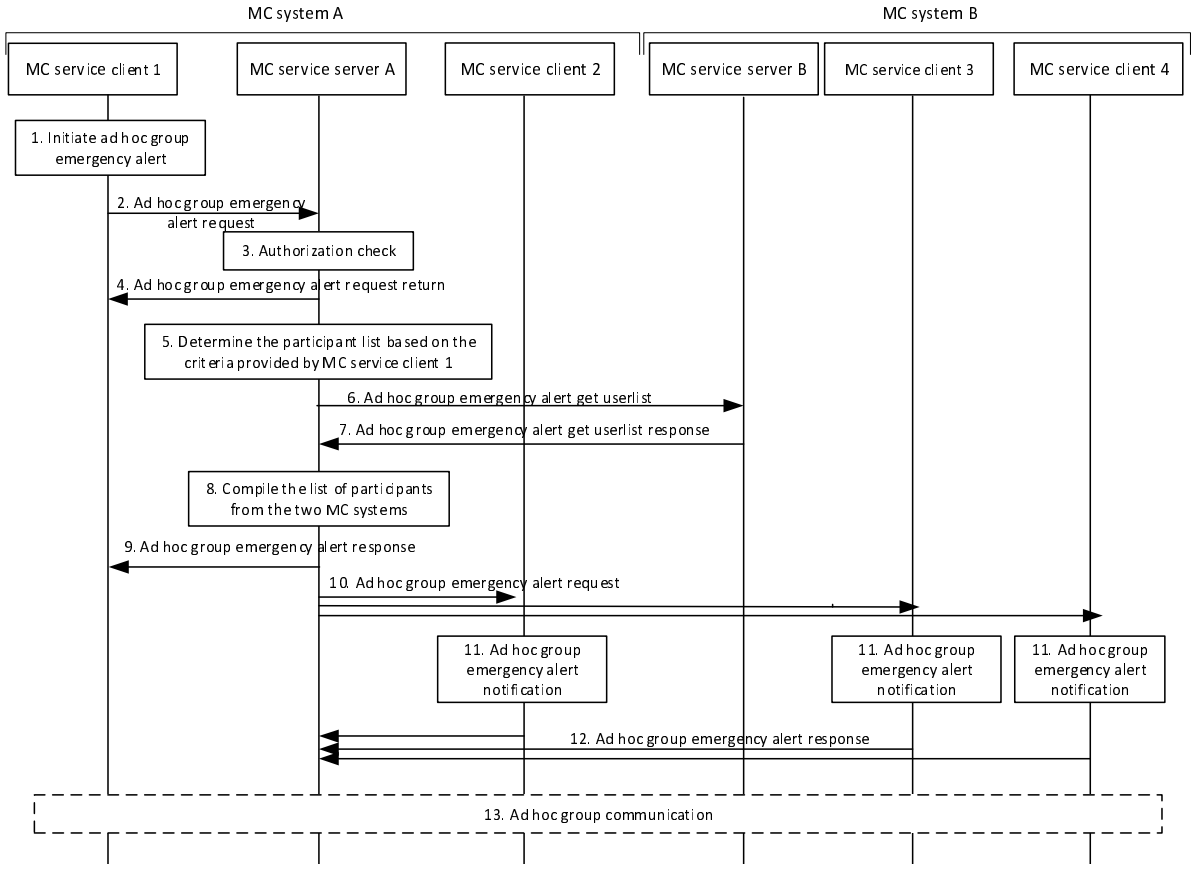

Figure 10.10.3.4.1-1: Ad hoc group emergency alert initiation between multiple MC systems

1. The MC service user 1 at the MC service client 1 initiates an ad hoc group emergency alert to an ad hoc group with participants satisfying specific criteria. The MC service user may add additional information describing the reason for sending the alert.

2. The MC service client 1 sends an ad hoc group emergency alert request containing the details of the criteria to be applied by the MC service server A for determining the participants list. The MC service client 1 may set its MC service emergency state. The MC service user at the MC service client 1 may select a functional alias used for the MC service group emergency alert. If the MC service client 1 is in an MC service emergency state, the MC service emergency state is retained by the MC service client 1 until explicitly cancelled.

3. The MC service server A checks whether the MC service user of MC service client 1 is authorized for initiation of ad hoc group emergency alert and whether the request is supported. The MC service server checks whether the provided functional alias, if present, can be used and has been activated for the user.

4. The MC service server A sends the ad hoc group emergency alert request return to the MC service user 1 containing the result of whether the ad hoc group emergency alert is authorized or not. If the ad hoc group emergency alert request is not authorized, the MC service server and the MC service client 1 shall not proceed with the rest of the steps.

5. The MC service server A determines that the partner MC system B is to be involved in the initiated ad hoc group emergency alert based on the information elements provided by the MC service client 1. The MC service server A determines the list of participants within MC system A to be invited for the ad hoc group emergency alert based on the information elements provided by the MC service client 1. This information element could carry either criteria or indicator identifying the pre-defined criteria or combination of both. Furthermore, The MC service server A adds the ad hoc group ID (generated by the MC service server A in the case when the MC service ad hoc group ID created by the MC service client 1 is not acceptable or the case where the MC service ad hoc group ID was not provided by the MC service client 1) to be associated with the ad hoc group emergency alert. The MC service sever A stores the ad hoc group ID together with the list of participants for the duration of the ad hoc group emergency alert.

NOTE 1: The content of the Criteria for determining the participants information element, the details of the pre-defined criteria, and the way how their MC service server determines the list of participants are left to implementation.

6. The MC service server A sends an ad hoc group emergency alert get userlist request to MC service server B including the criteria to determine the list of participants from the MC system B.

7. The MC service server B sends an ad hoc group emergency alert get userlist response to MC service server A including the list of participants within MC system B. The MC service server B may apply local policies if any while determining the participants satisfying the criteria.

8. The MC service server A compiles the list of participants from both MC system A and the partner MC system B to be involved in the ad hoc group emergency alert. The MC service server A considers MC service client 2, MC service client 3 and MC service client 4 implicitly affiliated to the ad hoc group associated to the emergency alert.

9. The MC service server A sends the MC service client 1 an ad hoc group emergency alert response to confirm that the request is granted.

10. The MC service server A sends an ad hoc group emergency alert request towards MC service client 2 within the partner MC system A and, MC service client 3, MC service client 4 within the partner MC system B.

11. The MC service user 2, MC service user 3 and MC service user 4 are notified of the ad hoc group emergency alert.

12. The MC service client 2, MC service client 3 and MC service client 4 send an ad hoc group emergency alert response back to MC service server A.

13. It is configured, whether any MC service client may setup a subsequent ad hoc group communication, using the ad hoc group ID from the ad hoc group emergency alert, according to 3GPP TS 23.379 [16], 3GPP TS 23.281 [12] or 3GPP TS 23.282 [13].

NOTE 2: MC service client 1 may start the subsequent ad hoc group call after step 9.

NOTE 3: Sending the emergency alert without making a request to also start an emergency call does not put the group into the in-progress emergency state.

NOTE 4: Sending the emergency alert does not put the other participants in the group into an MC service emergency state.

The MC service server continuously checks whether other MC service clients meet or if participating MC service clients no longer meet the criteria for the ad hoc group emergency alert.

10.10.3.4.2 Updating the participant list of an ongoing ad hoc group emergency alert

Figure 10.10.3.4.2-1 illustrates updating the participant list of an ongoing ad hoc group emergency alert within multiple MC systems. This includes scenario of MC service users entering and leaving an ongoing ad hoc emergency alert.

Preconditions:

- An ad hoc group emergency alert has been initiated by MC service user 1 within MC system A, and a related ad hoc group exists.

- The MC service server A and MC service server B are aware of the criteria sent by MC service client 1 related to the ongoing ad hoc group emergency alert.
- MC system A and MC system B are interconnected.

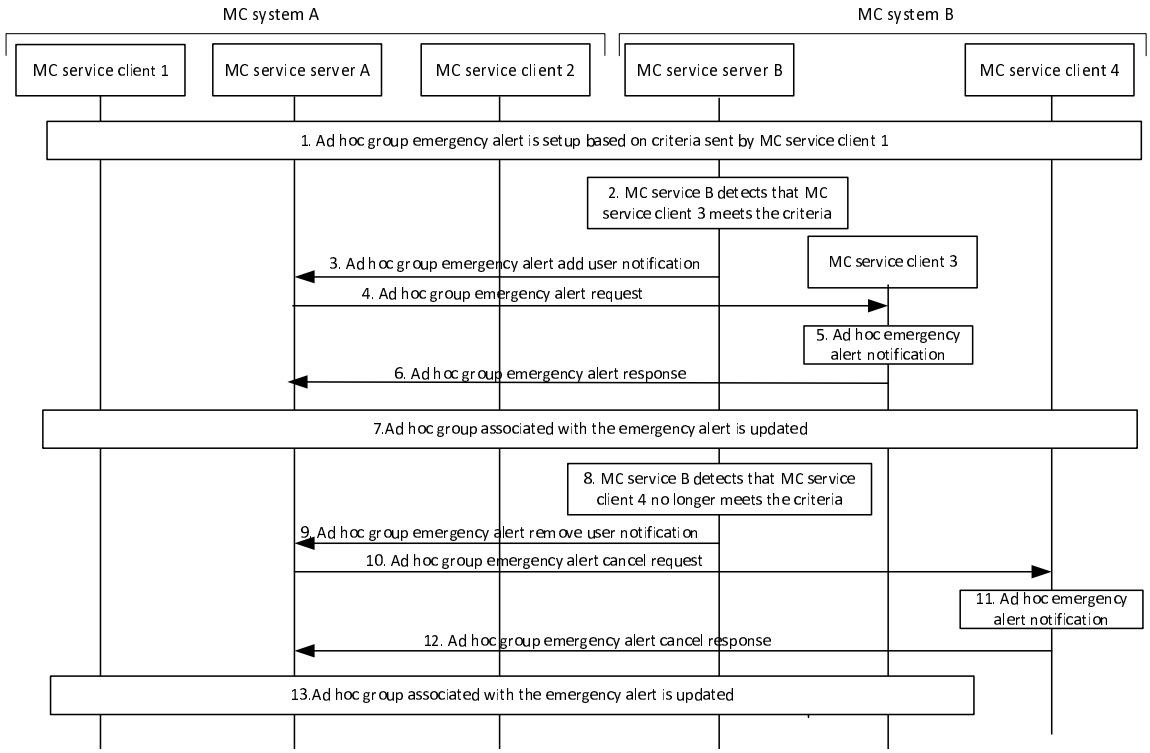

Figure 10.10.3.4.2-1: Updating the participant list of an ongoing ad hoc group emergency alert between multiple MC systems

1. An ad hoc group emergency alert has been established based on a set of criteria sent by MC service client 1 upon initiating the ad hoc emergency alert. The MC service server A considers MC service client 3 implicitly affiliated to the ad hoc group associate to the emergency alert.
2. MC service server B detects that MC service client 3 meets the criteria of the ongoing ad hoc group emergency alert initiated at MC system A.
3. MC service server B sends an ad hoc group emergency alert add user notification including the identity of MC service client 3 to be added to the ad hoc group associated to the ongoing emergency alert.
4. The MC service server A sends an ad hoc group emergency alert request to MC service client 3.
5. The MC service user 3 is notified of entering an ongoing ad hoc group emergency alert.
6. The MC service client 3 sends the MC service server A an ad hoc group emergency alert response.
7. The MC service server A updates the participant list of the MC service group associated with the ongoing ad hoc group emergency alert. The MC service server A may send a notification to authorized users indicating the addition of MC service client 3 to the ad hoc group.
8. The MC service server B detects that MC service client 4 no longer meets the criteria of the ongoing ad hoc group emergency alert. The MC service server A deaffiliates the MC service client 4 from the ad hoc group associated to the emergency alert.
9. The MC service server B sends the MC service server A an ad hoc group emergency remove user notification.
10. MC service server A sends the MC service client 4 an ad hoc group emergency alert cancel request.
11. The MC service user 4 is notified of leaving an ad hoc group emergency alert.

12. The MC service client 4 sends the MC service server A an ad hoc emergency alert cancel response.

13. The ad hoc group associated with the ongoing ad hoc emergency alert is updated. The MC service server A may send a notification to authorized users indicating the removal of the MC service client 4.

10.10.3.4.3 Ad hoc group emergency alert cancel

Figure 10.10.3.4.3-1 illustrates the procedure once an MC service client cancels an ongoing ad hoc group emergency alert.

Preconditions:

- An ad hoc group emergency alert is ongoing with participants within MC system A and MC system B.
- MC system A and MC system B are interconnected.

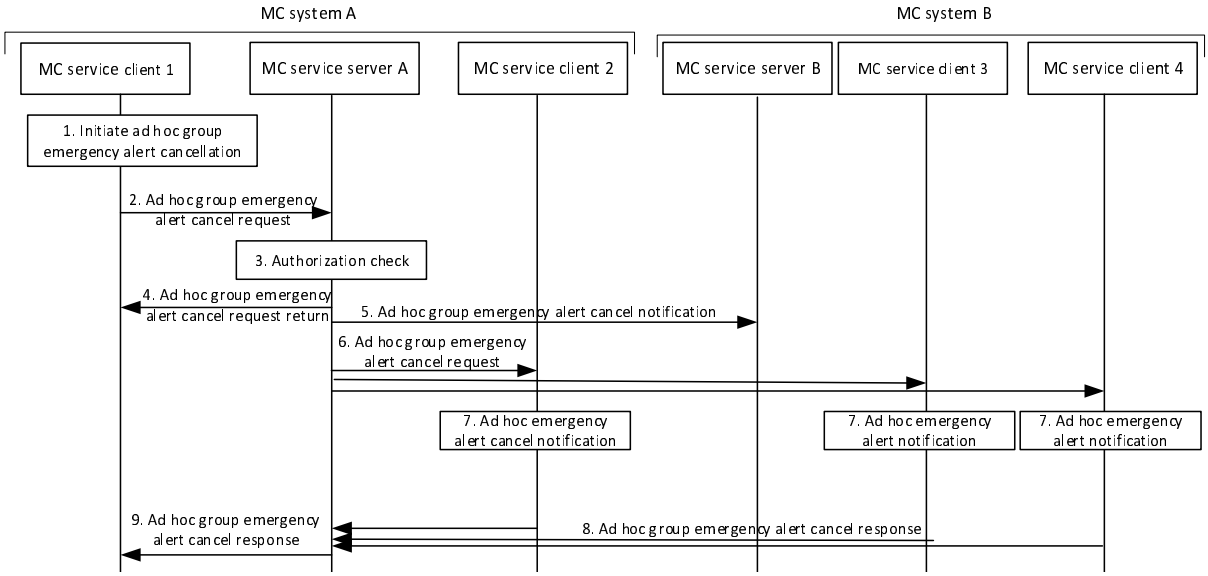

Figure 10.10.3.4.3-1: Ad hoc group emergency alert cancel between multiple MC systems

1. The MC service user 1 decides to cancel an ongoing ad hoc group emergency alert.

2. MC service client 1 sends the MC service server A an ad hoc group emergency alert cancel request. If the cancel request is sent for another MC service user that initiated this emergency alert, that user`s MC service ID shall be included in the cancel request.

3. MC service server A checks whether the MC service client 1 is authorized to cancel an ongoing ad hoc group emergency alert. The MC service server A checks whether the provided functional alias, if present, can be used and has been activated for the user.

4. The MC service server A sends the ad hoc group emergency alert cancel request return to the MC service user 1 containing the result of whether the ad hoc group emergency alert cancel request is authorized or not. If the ad hoc group emergency alert cancel request is not authorized, the MC service server and the MC service client 1 shall not proceed with the rest of the steps.5. The MC service server A sends an ad hoc emergency alert cancel notification to the MC service server B at the partner MC system B.

6. The MC service server A sends MC service client 2, MC service client 3 and MC service client 4 ad hoc group emergency alert cancel request.

7. The MC service user 2, MC service user 3 and MC service user 4 are notified of the ad hoc group emergency alert cancellation.

8. The MC service client 2, MC service client 3 and MC service client 4 sends ad hoc group emergency alert cancel response to the MC service server A. If there is no other communication in the ad hoc group or once the communication in the ad hoc group is terminated, the ad hoc group ceases to exist.

9. The MC service server A sends an ad hoc group emergency alert cancel response to MC service client 1.

10.11 MC service resource management (on-network)

10.11.1 General

The following subclauses specify the procedures for resource management for mission critical services. The procedures 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]).

The MC service server sets up media bearers and may need to modify the bearers for an already established MC communication.

Media characteristics that may need to be modified include:

- activation and deactivation of the bearer;
- modification of the QoS characteristics of the bearer (e.g. bearer priority adjustment); and
- modification of GBR due to media codec change

NOTE 1: A group call can consist of both unicast and multicast bearers which can all need modification due to the same event.

NOTE 2: The MC service server can retry the establishment of a media bearer upon failure based on information received, or other conditions.

10.11.2 Request for unicast resources at session establishment

The procedure defined in this subclause specifies how network resources are requested at session establishment. If concurrent sessions are used the MC service server may utilize the capability of resource sharing specified in 3GPP TS 23.203 [8]. The request for resources is sent to the PCRF on the Rx reference point and includes media type, bandwidth, priority, application identifier and resource sharing information.

The procedure is generic to any type of session establishment that requires requests for network resources.

Procedures in figure 10.11.2-1 are the signalling procedures for the requesting resource at session establishment.

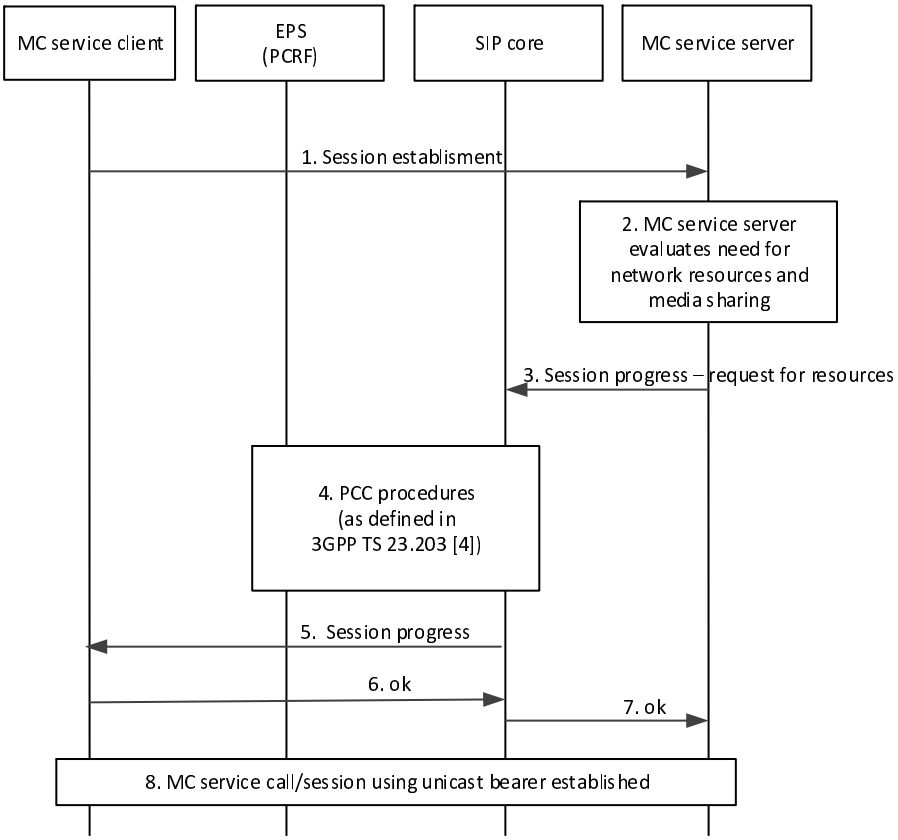

Figure 10.11.2-1: Resource request at session establishment

1. MC service client sends a call/session establishment request.
2. MC service server receives evaluates the need network resources and use of media resource sharing.
3. MC service server send a session progress request containing request for resources.
4. PCC procedures (as defined in 3GPP TS 23.203 [8]) initiated from SIP core local inbound/outbound proxy over Rx.
5. The SIP core local inbound / outbound proxy forwards the call control protocol request to the MC service client.
6. The MC service client acknowledges the session progress request with an OK message.
7. The SIP core local inbound / outbound proxy forwards the OK message to the MC service server.
8. The MC service call/session is established and resources have been allocated.

10.11.2a Request for unicast resources at session establishment from MC service server

10.11.2a.1 General

The procedure defined in this clause specifies how network resources are requested at session establishment from the MC service server. The request for resources is sent to the PCRF via the Rx reference point from the MC service server and includes media type, bandwidth, priority, application identifier and resource sharing information. If concurrent sessions are used, the MC service server may utilize the capability of resource sharing specified in 3GPP TS 23.203 [8].

For the request of network resources by the MC service server via the Rx reference point, the MC service client provides to the MC service server the final access resource details (e.g. IP addresses and ports) of the MC service client and the media anchoring points.

This procedure is generic to any type of session establishment with the MC service server requesting network resources.

10.11.2a.2 Procedure

Figure 10.11.2a.2-1 describes the procedure for the request of resources at session establishment from the MC service server.

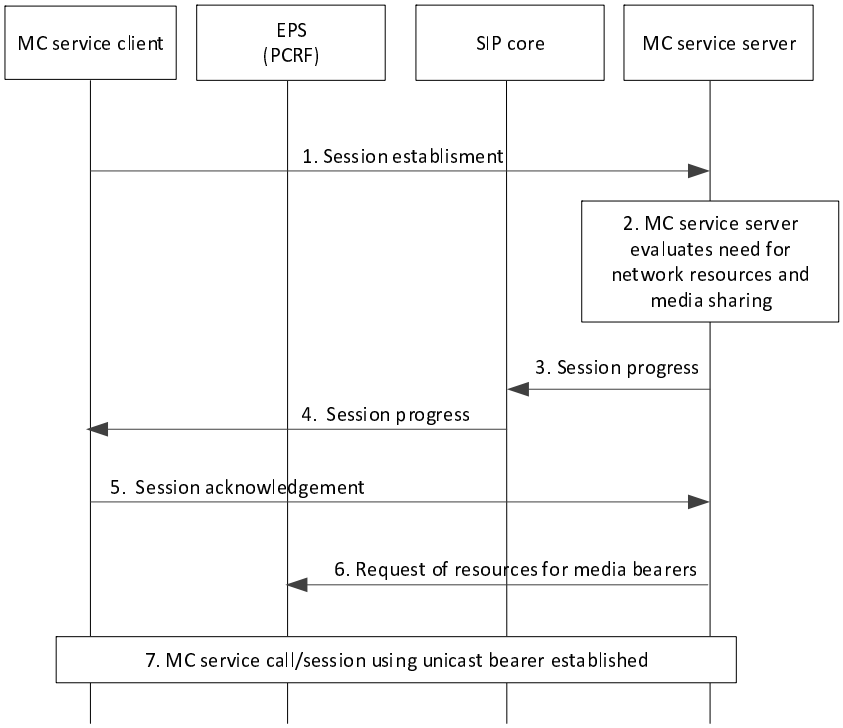

Figure 10.11.2a.2-1: Resource request at session establishment from the MC service server

1. The MC service client sends a call/session establishment request. The request includes, apart from the SDP offer, access resource details, e.g. IP addresses and ports of the MC service client related to the media session.
2. The MC service server evaluates the need of network resources and use of media resource sharing.
3. The MC service server sends a session progress request to the SIP core.

NOTE: The session progress request does not include a request for network resources to be performed by the SIP core.

4. The SIP core local inbound / outbound proxy forwards the session progress request to the MC service client.
5. The MC service client acknowledges the session establishment to the MC service server. This message contains the final negotiated media access parameters, e.g. IP addresses and ports related to the media anchoring points received in the SDP answer from the SIP core.
6. The MC service server sends a request for resources to the PCRF over Rx (as defined in 3GPP TS 23.203 [8]).
7. The MC service call/session is established, and resources have been allocated.

10.11.3 Request for modification of unicast resources

To modify unicast media bearers, the MC service server shall send a resource modification request containing the parameters to be modified, using the call control protocol via the SIP core to the UE.

Possible scenarios when this procedure may be used are:

- Modify the allocation and retention priority for unicast resources;
- Release and resume resources in-between MC service calls when using the chat model; or
- Release and resume resources when a UE is able to receive the MC service call over multicast transmission

Releasing resources for the media plane should give the option to allow the SIP session to either be torn down or continue.

Procedures in figure 10.11.3-1 are the signalling procedures for the modification of a unicast:

Pre-conditions:

- An MC service call or session is already in progress;

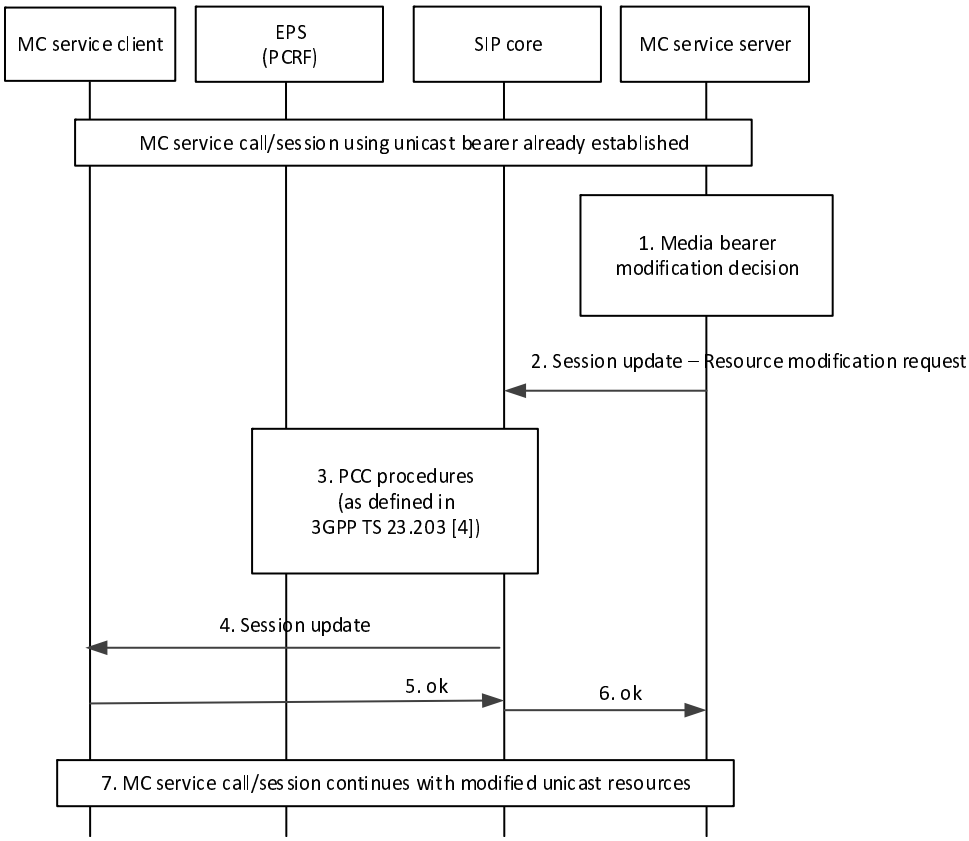

Figure 10.11.3-1: Bearer modification request

1. MC service server decides to modify the parameters of a unicast bearer (e.g. a request to upgrade the existing MC service call to an MC service emergency or imminent threat call).
2. MC service server sends a session update which includes a resource modification request containing the modified parameters of the unicast bearer.
3. PCC procedures (as defined in 3GPP TS 23.203 [8]) initiated from SIP core local inbound/outbound proxy over Rx.
4. The SIP core local inbound / outbound proxy forwards the session update request to the MC service client.
5. The MC service client acknowledges the call control protocol request with an OK message.
6. The SIP core local inbound / outbound proxy forwards the OK message to the MC service server.
7. The MC service call continues with the modified unicast resources.

NOTE 1: If the MC service call is transferred to multicast transmission, the unicast resources could be temporarily be released.

NOTE 2: If multiple audio streams are sent to the UE, additional bearer resources could be required during an established session. Pre-allocation of additional bearer resources already at session establishment could be useful.

10.11.4 Management of multicast media bearers

To activate the multicast media bearers the MC service server shall use the Activate MBMS Bearer procedure specified in 3GPP TS 23.468 [18] with the MC service server performing the GCS AS function. The MC service server shall activate MBMS bearers in broadcast areas where eMBMS capable UEs are or are expected to be located. For that, the MC service server shall use the MBMS SAI(s) and/or cell id(s) information to construct the MBMS broadcast area parameter in the Activate MBMS Bearer procedure.

To deactivate the multicast media bearers the MC service server shall use the Deactivate MBMS Bearer procedure specified in 3GPP TS 23.468 [18] with the MC service server performing the GCS AS function.

To modify multicast media bearers the MC service server shall use the Modify MBMS Bearer procedure specified in 3GPP TS 23.468 [18] with the MC service server performing the GCS AS function.

10.11.5 Request for resources with shared priority

10.11.5.1 General

An MC service server that supports simultaneous sessions may need to share a common priority on the EPS bearer for several MC service group calls that may use different priorities on the application level. This is achieved by including information for priority sharing on the request of resources over Rx reference point to PCRF. All sessions associated with the same priority sharing information will be handled by one EPS bearer, which will have a priority based on the highest requested priority among the sessions.

The use of the procedure defined in subclause 10.11.5.2 is dependent on operator policy.

10.11.5.2 Procedure

Pre-conditions:

- All previous resource requests from the MC service have included a priority sharing information.

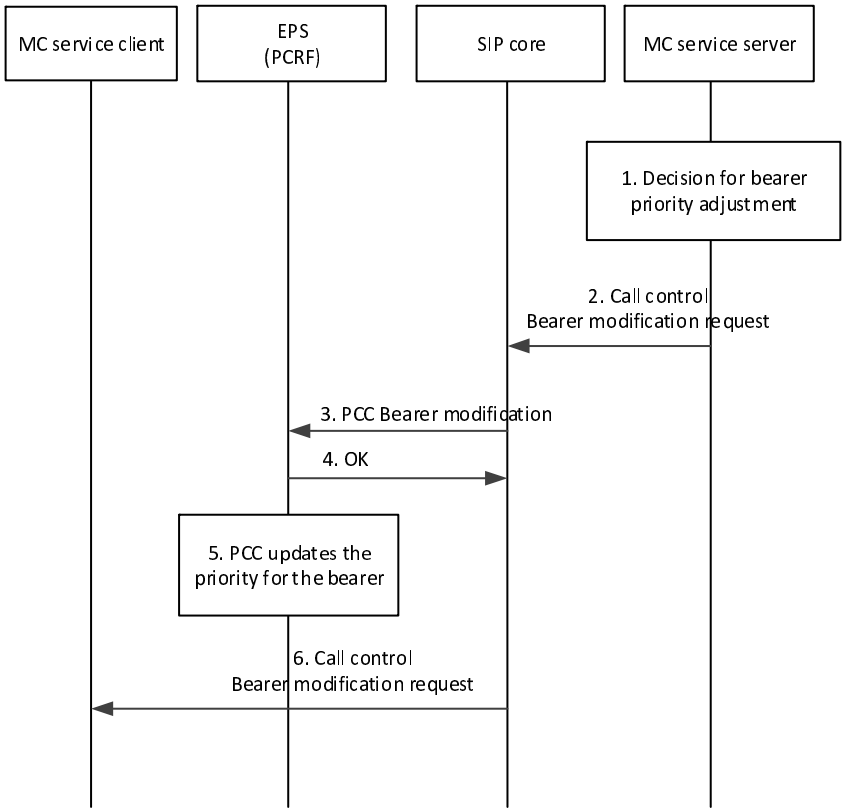

Figure 10.11.5.2-1: Resource request including priority sharing information

1. The MC service server decides based on a request from the MC service client that the priority of an ongoing call must be adjusted.
2. The MC service server requests a session update to the SIP core. This request will contain information of priority sharing.
3. The proxy function in the SIP core sends a request to the PCRF over Rx to request for modified priority. The request will include the priority sharing information over Rx.
4. The PCRF acknowledges the request.
5. PCC updates the bearer priority for the bearer that contains the SDFs associated with the same priority sharing information. The priority is set to highest priority (lowest ARP) among those SDFs. No additional bearer is created. Also the default bearer priority is updated accordingly.
6. The session update is forwarded to the MC service client.

NOTE 1: The procedure defined above requires a PCC enhancement and is subject to implementation in EPC and IMS and can therefore only be used if supported by EPC and IMS.

NOTE 2: If the EPC and IMS does not support the priority sharing from MC system, no shared priority treatment applies, and a new EPS bearer will be setup based on QCI/ARP combination.

10.11.6 Request for media resources from MC service server

10.11.6.1 General

The procedure in this sub clause specify how request for resource for floor control (or transmission control in MCVideo and MCData) and for the media plane can be handled independently. This procedure utilizes the Rx reference point both between from the MC service server to the PCRF and from the SIP core to the PCRF.

Resource for the transmission control is requested at session establishment, in this case the IMS standard procedures as specified in 3GPP TS 23.228 [9] are used. The session description shall in this procedure include bandwidth information applicable for the transmission control traffic requirement. At group call setup the request for resources for the media plane is triggered. This request is sent directly from the MC service server to the PCRF.

The procedure is optional and is suitable when the procedures for pre-established sessions are used, it may also be used to setup and tear down the media plane used by between consecutive group calls in one communication session using the chat call model.

10.11.6.2 Procedure

The figure below illustrates the procedure for resource reservation

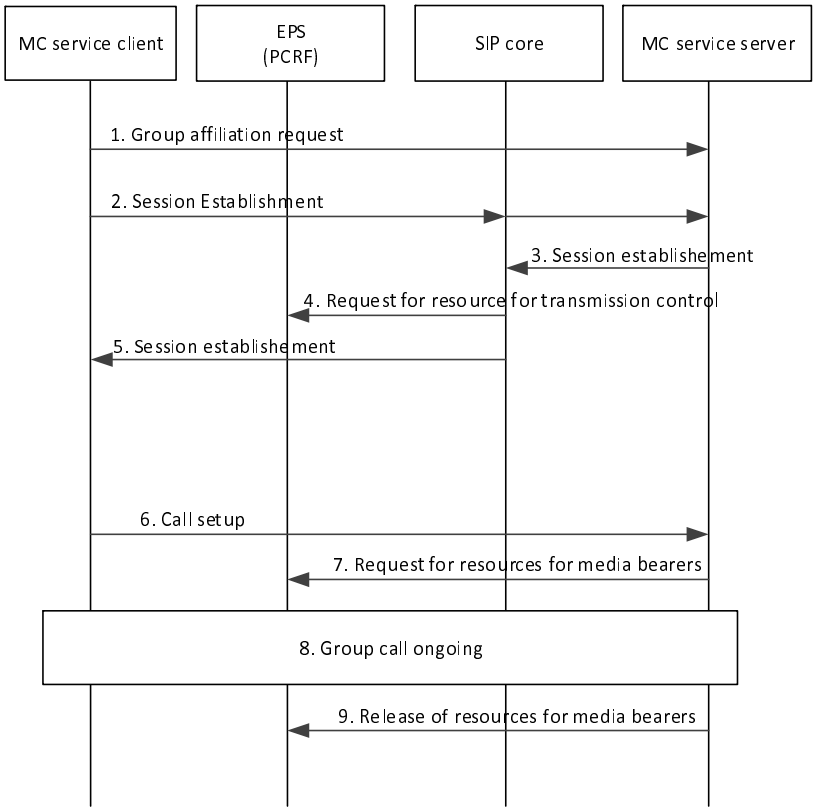

Figure 10.11.6.2-1: Request for resources for transmission control and media plane

1. The MC service client sends a request for group affiliation.
2. The MC service client sends a request to the MC service server for establishment of a communication session.
3. The MC service server answer the session establishment request and adjust the bandwidth information in the session description. The requested bandwidth shall be minimized to cover the bandwidth requirements for floor control signaling (or transmission control for MCVideo or MCData).
4. The SIP core request resources towards the PCRF according to the session establishment request.5.The session establishment request is completed and a response is sent towards the MC service client.
6. The MC service client sends a cell setup message according to existing procedures.
7. The MC service server sends a request for resources for the media plane to PCRF, and the media plane is by that established. This request includes media description relevant for the media plane.
8. Group call is ongoing on the group communication session.
9. The MC service serve sends a release of media resources to PCRF, and the media plane is by that terminated.

NOTE 1: The resources for transmission control are retained.

NOTE 2: Step 6-9 can be repeated several times within the life cycle of one communication session.

10.12 Priority Management

10.12.1 General

Mission critical priority and QoS management is situational. The MC Services provides a real-time priority and QoS experience for the MC users, who have significant dynamic operational requirements that determine their priority. For example, the type of incident a responder is serving or the responder's overall shift role needs to strongly influence a user's ability to obtain resources from the LTE system.

Priority treatment applies on both application layer as well as on transport layer. The details on how the priority level is evaluated and used is outside the scope of this specification. What is specified is the necessary mechanisms to apply the priority and QoS and map different priority parameters between different entities, for example to map application layer priority to transport layer priority.

One of the requirements for MC communication services is to coordinate the use of priority levels between the different MC service servers. This priority coordination is used to mitigate and manage the risk for network congestion situations.

10.12.2 Information flows

10.12.2.1 MC priority request

Table 10.12.1.1-1 describes the information flow MC priority request from one MC service server to an MC service server taking the priority arbitration role.

Table 10.12.1.1-1: MC priority request

Information element	Status	Description
Priority	M	Requested priority
Priority area	M	The geographical area for which the requested priority is required.
Type of service	O	The MC service type e.g. MCVideo, MCPTT or MCData

10.12.3 Procedure for priority coordination between multiple MC service servers

In deployment scenarios with multiple MC service servers of different or the same type it is required to coordinate the priorities used by the different servers. The procedure defined below provides the necessary coordination between MC service servers to manage high priority levels. One of the involved MC service servers is assigned the role of being a priority arbitrator among a group of MC service servers serving the same geographical area. The priority arbitrator may also compete for the same limited network resources. Prior to using this procedure all MC service servers need to be configured with information about which MC service server will act as the priority arbitrator and under what conditions (e.g. priority level) the priority arbitrator should be used. The use of this procedure is not mandated. MC systems that support priority coordination between multiple MC service servers should support this procedure.

Pre-condition:

1. One of the MC service servers is assigned the role of the priority arbitrator.
2. It is assumed that all MC service servers are part of the same trusted domain.
3. A MC communication session is ongoing or is about to commence. The operational situation together with static and dynamic attributes requires the use of elevated priority for network resources.

NOTE 1: Whether enforcement of the granted priority can be applied to MC service servers outside of the same trusted domain is out of scope of the present document.

NOTE 2: How the MC service server 2 (priority arbitrator) knows about ongoing traffic is out of scope of the present document.

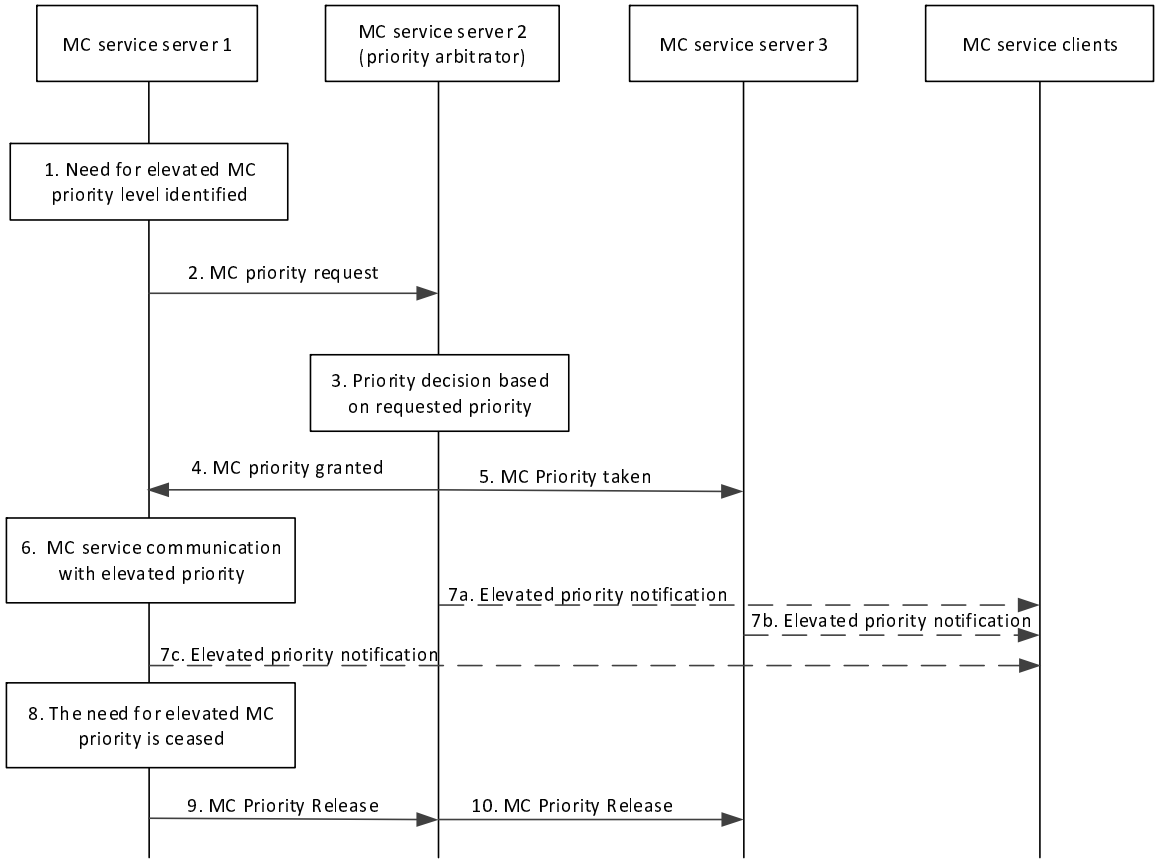

Figure 10.12.3-1: Priority arbitration between multiple MC service servers

1. A need for high priority level is identified by the MC service server 1. The priority level identified is above the level of priority that the MC service server 1 can utilise without centralized priority arbitration.

2. The MC service server 1 sends a MC priority request to the MC service server being assigned the priority arbitrator role. The request includes the geographical area, duration, the priority level, service type and needed capacity.

3. The priority arbitrator determines whether to grant, reject or queue the request for elevated priority.

NOTE 3: How the priority arbitrator makes this determination is out of scope of the present document.

NOTE 4: One source of information for the priority arbitrator to evaluate the priority request, could be information received at the resource reservations over the Rx reference point. Example of such information is resource request failure and Retry-Interval AVP which could be an indication of RAN user plane congestion, see reference 3GPP TS 29.214 [27].

4. The priority arbitrator grants MC service server 1 the elevated priority

5. The priority arbitrator notifies other MC service servers about the elevated priority granted to other services.

NOTE 5: The behaviour of the MC service servers that receive this information is implementation specific. The MC service server may take this information into account when performing priority evaluations for the MC service clients managed by this MC service server.

6. The MC service server utilizes the elevated priority when requesting resources for new or existing MC service communication.

NOTE 6: The priority level granted to the MC service server 1 can be mapped to an applicable SIP priority header or a reservation priority AVP (when the MC service server use the Rx reference point directly).

7a-c. A priority notification may be sent to the MC service clients in the geographical area in which the priority was granted. Messages to MC service clients need to be sent from the MC service server serving each MC user. This message is preferably sent over a multicast bearer.

NOTE 7: How the clients could utilize such notifications is out of scope of the present document.

8. The MC service server 1 identifies that the elevated priority is not needed.

9. The requested MC Priority is released from the MC service server 1.

10. The MC service server 2 (priority arbitrator) informs other MC servers that the elevated priority is released.

NOTE 8: The procedure for MC priority revoking is out of scope of the present document.

NOTE 9: The procedure for MC priority queueing is out of scope of the present document.

10.13 Functional alias management (on-network)

10.13.1 General

Functional alias management procedures apply to on-network MC service only.

10.13.2 Information flows for functional alias management

10.13.2.1 Active functional alias information user query request

Table 10.13.2.1-1 describes the information flow for the active functional alias information user query request from the MC service client to the MC service server.

Table 10.13.2.1-1: Active functional alias information user query request

Information element	Status	Description
MC service ID	M	The identity of the MC service user who performs the query.
MC service ID(s)	M	The identity of the MC service user(s) to be queried.

10.13.2.1a Active functional alias information usage query request

Table 10.13.2.1a-1 describes the information flow for the active functional alias information usage query request from the MC service client to the MC service server.

Table 10.13.2.1a-1: Active functional alias information usage query request

Information element	Status	Description
MC service ID	M	The identity of the MC service user who performs the query.
Functional alias(es)	M	A list of functional alias(es) to be queried.

10.13.2.2 Active functional alias information user query response

Table 10.13.2.2-1 describes the information flow for the active functional alias information user query response from the MC service server to the MC service client. This information flow is sent individually addressed on unicast or multicast.

Table 10.13.2.2-1: Active functional alias information user query response

Information element	Status	Description
MC service ID	M	The identity of the MC service user who performs the query.
MC service ID(s)	M	The identity of the MC service user(s) to be queried.
Query result	M	The active functional alias information retrieved from the MC service server for each of the MC service user(s) queried; or Null if no functional alias is active for the MC service user.

10.13.2.2a Active functional alias information usage query response

Table 10.13.2.2a-1 describes the information flow for the active functional alias information usage query response from the MC service server to the MC service client. This information flow is sent individually addressed on unicast or multicast.

Table 10.13.2.2a-1: Active functional alias information usage query response

Information element	Status	Description
MC service ID	M	The identity of the MC service user who performs the query.
Functional alias(es)	M	The functional alias(es) to be queried.
Query result	M	The list of MC service ID(s) of the MC service user(s) who have activated the functional alias being queried; or Null if this functional alias is not active for any user.

10.13.2.3 Functional alias activation request

Table 10.13.2.3-1 describes the information flow functional alias activation request from the MC service client to the MC service server.

Table 10.13.2.3-1: Functional alias activation request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias activation request.
Functional alias list	M	A list of one or more functional aliases which the originator intends to activate.

10.13.2.4 Functional alias activation response

Table 10.13.2.4-1 describes the information flow functional alias activation response from the MC service server to the MC service client. This information flow is sent individually addressed on unicast or multicast.

Table 10.13.2.4-1: Functional alias activation response

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias activation request.
Functional alias list	M	A list of one or more functional aliases which the originator intends to activate.
Activation status per functional alias	M	Indicates the activation result for each functional alias in the list (activated, rejected, can be taken over).

10.13.2.5 Functional alias de-activation request

Table 10.13.2.5-1 describes the information flow functional alias de-activation request from the MC service client to the MC service server.

Table 10.13.2.5-1: Functional alias de-activation request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias de-activation request.
Functional alias list	M	A list of one or more functional aliases which the originator intends to de-activate.

10.13.2.6 Functional alias de-activation response

Table 10.13.2.6-1 describes the information flow functional alias de-activation response from the MC service server to the MC service client. This information flow is sent individually addressed on unicast or multicast.

Table 10.13.2.6-1: Functional alias de-activation response

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias de-activation request.
Functional alias list	M	A list of one or more functional aliases which the originator intends to de-activate.
De-activation status per functional alias	M	Indicates the de-activation result for every functional alias in the list.

10.13.2.7 Functional alias status notification

Table 10.13.2.7-1 describes the information flow functional alias notification from the MC service server to the MC service client. This information flow may be sent individually addressed or group addressed on unicast or multicast (see subclause 10.7.3.4.1).

Table 10.13.2.7-1: Functional alias status notification

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias activation, de-activation or take over request.
Functional alias list	M	A list of one or more functional aliases.
Operations	M	Activation, de-activation or take over status per functional alias.

10.13.2.8 Functional alias take over request

Table 10.13.2.8-1 describes the information flow functional alias take over request from the MC service client to the MC service server.

Table 10.13.2.8-1: Functional alias take over request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias take over request.
Functional alias list	M	A list of one or more functional alias which the originator intends to take over.

10.13.2.9 Functional alias take over response

Table 10.13.2.9-1 describes the information flow functional alias take over response from the MC service server to the MC service client. This information flow is sent individually addressed on unicast or multicast.

Table 10.13.2.9-1: Functional alias take over response

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias take over request.
Functional alias list	M	A list of one or more functional alias which the originator intends to take over.
Take over status per functional alias	M	Indicates the take over request result (accepted, rejected).

10.13.2.10 Functional alias revoke notification

Table 10.13.2.10-1 describes the information flow functional revoke notification from the MC service server to the MC service client. This information flow is sent individually addressed on unicast or multicast.

Table 10.13.2.10-1: Functional alias revoke notification

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias take over request.
Functional alias	M	The functional alias which is revoked.

10.13.2.11 Subscribe functional alias request

Table 10.13.2.11-1 describes the information flow subscribe functional alias request from the MC service server to the functional alias controlling MC service server, and from the location management server to the functional alias controlling MC service server.

Table 10.13.2.11-1: Subscribe functional alias request

Information element	Status	Description
Functional alias	M	The functional alias for which subscription is requested.
Subscription type	M	Indicates the subscription is for one-time notification or continuous notification.

10.13.2.12 Subscribe functional alias response

Table 10.13.2.12-1 describes the information flow subscribe functional alias response from the functional alias controlling MC service server to the MC service server, and from the functional alias controlling MC service server to the location management server.

Table 10.13.2.12-1: Subscribe functional alias response

Information element	Status	Description
Functional alias	M	The functional alias for which subscription is requested.
Status	M	Success or failure of the request

10.13.2.13 Notify functional alias request

Table 10.13.2.13-1 describes the information flow notify functional alias request from the functional alias controlling MC service server to the MC service server, and from the functional alias controlling MC service server to the location management server.

Table 10.13.2.13-1: Notify functional alias request

Information element	Status	Description
Functional alias	M	The functional alias for which subscription is requested.
List of MC service IDs (see NOTE)	M	The list of MC service IDs that is activated for the functional alias
NOTE: The MC service ID list can be an empty list.		

10.13.2.14 Notify functional alias response

Table 10.13.2.14-1 describes the information flow notify functional alias response from the MC service server to the functional alias controlling MC service server, and from the location management server to the functional alias controlling MC service server.

Table 10.13.2.14-1: Notify functional alias response

Information element	Status	Description
Functional alias	M	The functional alias for which a list of MC service users who activate the functional alias is requested.

10.13.2.15 Unsubscribe functional alias request

Table 10.13.2.15-1 describes the information flow unsubscribe functional alias request from the MC service server to the functional alias controlling MC service server, and from the location management server to the functional alias controlling MC service server.

Table 10.13.2.15-1: Unsubscribe functional alias request

Information element	Status	Description
Functional alias	M	The functional alias for which subscription is requested to be cancelled.

10.13.2.16 Unsubscribe functional alias response

Table 10.13.2.16-1 describes the information flow subscribe functional alias response from the functional alias controlling MC service server to the MC service server, and from the functional alias controlling MC service server to the location management server.

Table 10.13.2.16-1: Unsubscribe functional alias response

Information element	Status	Description
Functional alias	M	The functional alias for which subscription is requested to be cancelled.
Status	M	Success or failure of the request

10.13.2.17 Functional alias to group binding request

Table 10.13.2.17-1 describes the information flow functional alias to group binding request from the MC service client to the MC service server.

Table 10.13.2.17-1: Functional alias to group binding request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias to group binding request.
MC service group ID to functional alias bindings	M	A list of MC service group IDs to functional alias bindings. One MC service group ID can be bound only to one functional alias. The same functional alias can be bound to multiple MC service group IDs.

10.13.2.18 Functional alias to group binding response

Table 10.13.2.18-1 describes the information flow functional alias to group binding response from the MC service client to the MC service server.

Table 10.13.2.18-1: Functional alias to group binding response

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias to group binding request.
Result	M	Indicates the success or failure for the result

10.13.2.19 Functional alias to group unbinding request

Table 10.13.2.19-1 describes the information flow functional alias to group unbinding request from the MC service client to the MC service server.

Table 10.13.2.19-1: Functional alias to group unbinding request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias to group unbinding request.
MC service group ID list	M	A list of MC service group IDs to which the originator requests the functional alias to group unbinding.

10.13.2.20 Functional alias to group unbinding response

Table 10.13.2.20-1 describes the information flow functional alias to group unbinding response from the MC service client to the MC service server.

Table 10.13.2.20-1: Functional alias to group unbinding response

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the functional alias to group unbinding request.
Result	M	Indicates the success or failure for the result

10.13.3 Authorised MC service user retrieves active functional alias(es) for certain MC service user(s)

An authorised MC service user can request the active functional alias(es) for one or more MC service users.

Figure 10.13.3-1 below illustrates the active functional alias list query for the MC service user(s).

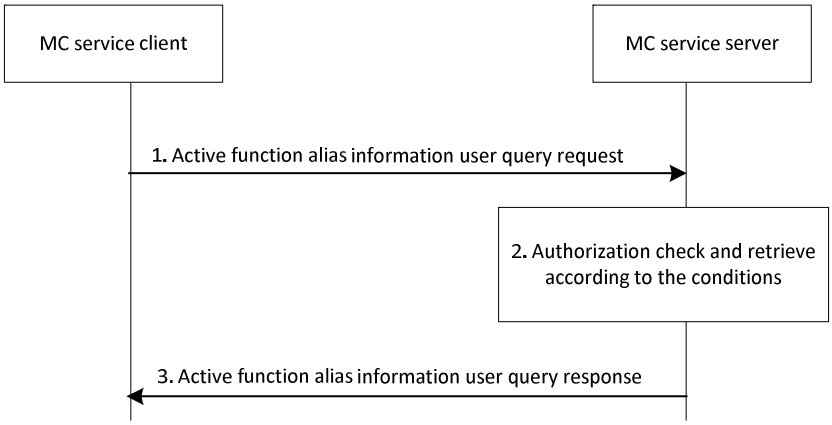

Figure 10.13.3-1: Active functional alias list query for the user

1. The MC service client of the MC service user requests the list(s) of active functional aliases for each MC service user(s) from the MC service server by sending an active functional alias information user query request. The MC service ID(s) to be queried is included.
2. The MC service server checks whether the MC service user is authorized to perform the query. If authorized, then the MC service server retrieves the requested active functional alias information based on the MC service ID(s).
3. The MC service server sends an active functional alias information user query response including the functional alias information to the MC service client.

10.13.4 MC service user activates functional alias(es) within an MC system

The procedure for MC service user activates functional alias(es) within an MC system is illustrated in figure 10.13.4-1.

Pre-conditions:

1. MC service client has already been provisioned (statically or dynamically) with the functional alias(es) information that the MC service client is allowed to activate.
2. MC service server may have retrieved the user profile and functional alias policy from the functional alias configuration e.g. which user(s) are authorized to activate to what functional alias, priority, and other configuration data.
3. MC service client may have indicated to the functional alias management server that it wishes to receive updates of functional alias data for the functional aliases for which it is authorized.
4. The MC service client triggers the functional alias activation procedure. This is an explicit activation 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 a functional alias.

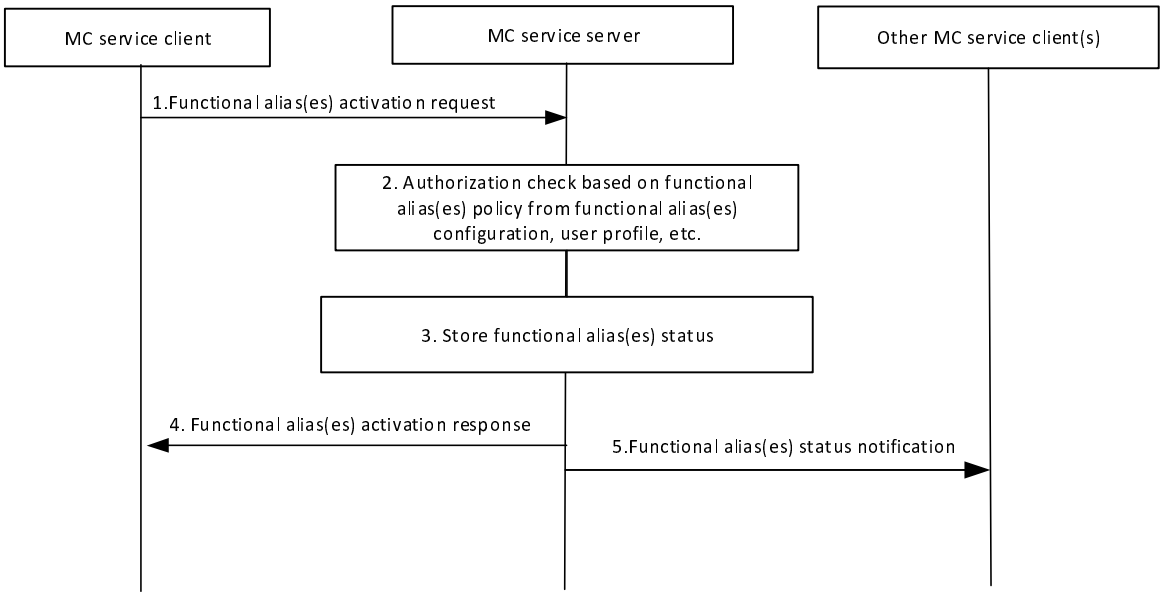

Figure 10.13.4-1: Functional alias activation procedure within an MC system

1. MC service client of the MC service user requests the MC service server to activate a functional alias or a set of functional aliases.

NOTE 1: If the MC service server is not the one that performs the functional alias controlling role, the MC service server will forward the request to the MC service server that performs the functional alias controlling role.

2. The MC service server checks if there are any conflicts with active functional alias(es).

3. If the user of the MC service client is authorised to activate the requested functional alias(es) then the MC service server stores the functional alias(es) status of the requested functional alias(es).

   If a certain functional alias(es) can be simultaneously active for multiple MC service users and the upper limit of number of simultaneous MC service users is not reached, the MC service shall activate the functional alias(es) for the MC service user and inform all other MC service user(s) with sharing the same functional alias(es) (step 5). If the limit of number of simultaneous MC service users is reached or the functional alias is not allowed to be shared, the request is rejected and the MC service user is notified (step 4).

   If the functional alias(es) is (are) already used by another MC service user(s), an authorized MC service user gets an offer to take over the functional alias from the MC service user currently using the functional alias(es).

NOTE 2: The functional alias status is notified to other servers (e.g. MC service servers) within the MC system that have subscribed to functional alias status.

4. MC service server sends a functional alias(es) activation response to the MC service client.

5. The MC service server informs all other MC service user(s) sharing the same functional alias(es).

10.13.5 MC service user de-activates functional alias(es) within an MC system

The procedure for MC service user de-activates functional alias(es) within an MC system is illustrated in figure 10.13.5-1.

When an MC service user does not want to use a functional alias(es) anymore, then the MC service user can de-activate functional alias(es).

Pre-conditions:

1. MC service server has already subscribed to the functional alias(es) information from the functional alias management server and has stored the data of the functional alias(es) a MC service user has activated.

2. The MC service client triggers the functional alias(es) de-activation procedure. This is an explicit de-activation request 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 a functional alias.

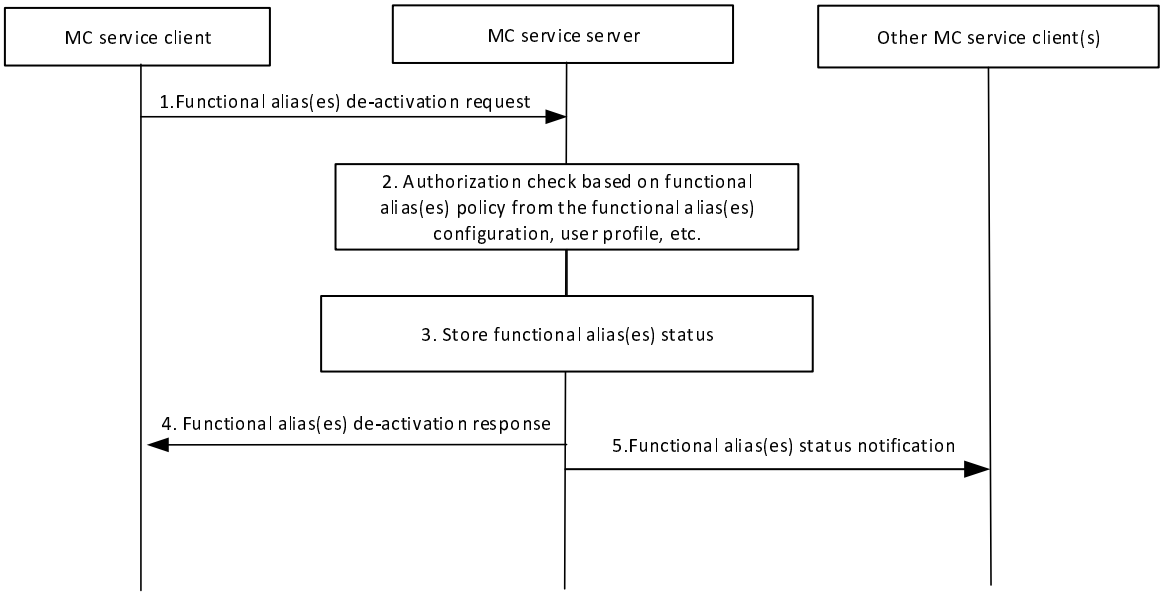

Figure 10.13.5-1: Functional alias de-activation procedure within an MC system

1. MC service client requests the MC service server to de-activate a functional alias or a set of functional aliases.

NOTE 1: If the MC service server is not the one that performs the functional alias controlling role, the MC service server will forward the request to the MC service server that performs the functional alias controlling role.

2. Based on the MC service user profile and stored functional alias policy from the functional alias configuration, the MC service server checks if the MC service user of the MC service client is authorized to de-activate from the requested functional alias(es) and if the MC service user of the MC service client has activated to the requested functional alias(es).

3. If the MC service user is authorized to de-activate from the requested functional alias(es) then the MC service server updates the functional alias activation status of the MC service user.

NOTE 2: The functional alias status is notified to other servers (e.g. MC service servers) within the MC system that have subscribed to functional alias status.

4. MC service server provides to the MC service client the functional alias de-activation response.

5. The MC service server informs all other MC service user(s) sharing the same functional alias(es).

10.13.6 Authorised MC service user takes over functional alias(es) within an MC system

The procedure for MC service user takes over functional alias(es) within an MC system is illustrated in figure 10.13.6-1.

During functional alias(es) activation, if the functional alias(es) is (are) already used by another MC service user(s), an authorized MC service user may get an offer to take over the functional alias(es) from the MC service user currently using the functional alias(es).

Pre-conditions:

1. MC service client 1 has performed the functional alias(es) activation procedure as described in subclause 10.13.4.

2. As result of the functional alias(es) activation procedure, the MC service user of MC service client 1 is aware which functional alias(es) are already used but can be taken over.

3. The MC service user of MC service client 1 decides to take over a functional alias.

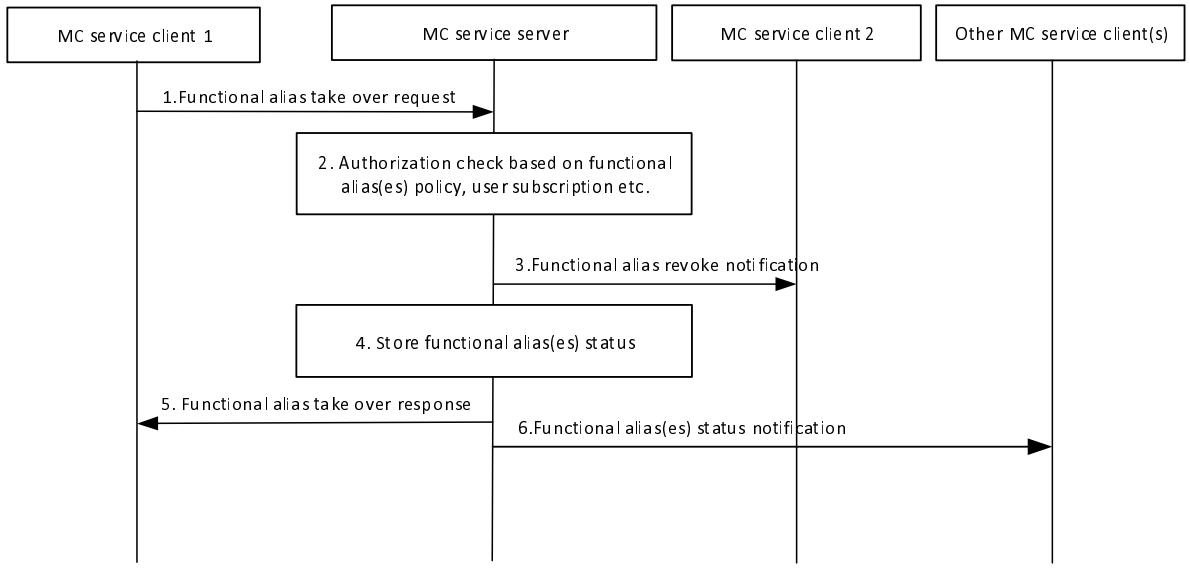

Figure 10.13.6-1: Functional alias taking over procedure within an MC system

1. MC service client 1 of the MC service user 1 requests the MC service server to take over a functional alias by sending a functional alias take over request.

NOTE 1: If the MC service server is not the one that performs the functional alias controlling role, the MC service server will forward the request to the MC service server that performs the functional alias controlling role.

NOTE 2: For the sake of brevity takeover of single functional alias is shown in this procedure. If MC service user 1 decides to take over multiple functional aliases, then the Functional alias take over request in step 1 carries a list of those functional aliases.

2. The MC service server checks if there are any conflicts taking over the functional alias.

3. If the user of the MC service client 1 is authorised to take over the requested functional alias then the MC service server sends a functional alias revoke notification to inform MC service client 2 that the functional alias has been revoked and is not any longer active for the user of MC service client 2.

4. The MC service server stores the functional alias status of the requested functional alias.

NOTE 3: The functional alias status is notified to other servers (e.g. MC service servers) within the MC system that have subscribed to functional alias status.

5. MC service server sends a functional alias take over response to the MC service client.

6. The MC service server informs all other MC service user(s) sharing the same functional alias.

10.13.7 Authorised MC service user retrieves MC service user(s) for certain active functional alias(es)

An authorised MC service user can request the MC service user(s) who have activated the functional alias being queried, for one or more functional aliases.

Figure 10.13.7-1 below illustrates the query of usage of the active functional alias(es) procedure.

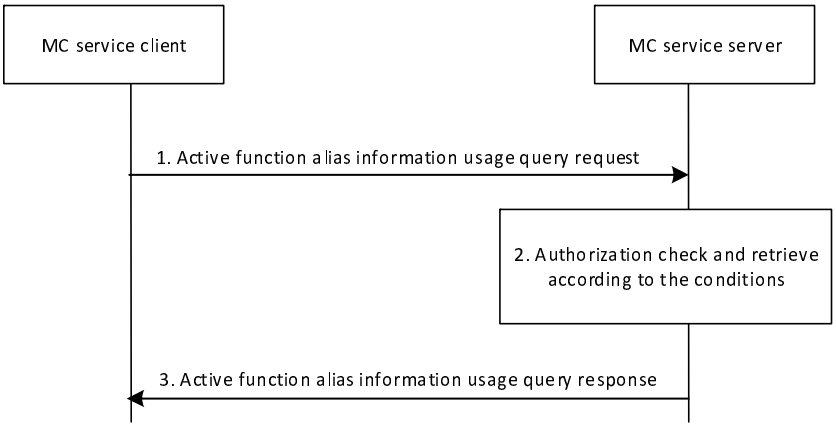

Figure 10.13.7-1: Query of usage of the active functional alias(es)

1. The MC service client of the MC service user requests the list(s) of MC service user(s) who have actived the functional alias being queried, by sending an active functional alias information usage query request. The functional alias(es) to be queried are included.

2. The MC service server checks whether the MC service user is authorized to perform the query. If authorized, then the MC service server retrieves the requested MC service user(s) information for those MC service users who have actived the functional alias being queried.

3. The MC service server sends an active functional alias information usage query response including the MC service user information to the MC service client.

10.13.8 Automatic activation of functional alias(es) within an MC system

The MC Service Server can automatically activate functional aliases that can be specified by internal or external triggers such as location dependency, schedule, or timer.

The procedure for automatic activation of functional alias(es) within an MC system is illustrated in figure 10.13.8-1. The MC service client(s) get(s) notified by the MC service server at the time when a functional alias has been activated by the MC service server.

Pre-conditions:

1. MC service server may have retrieved the MC service user profile and functional alias policy from the functional alias configuration, for example, which MC service user(s) are authorized to activate which functional alias(es), to use corresponding priorities and other configuration data associated with the functional alias.

2. MC service server has already been provisioned with the functional alias(es) information that the MC service client is allowed to activate.

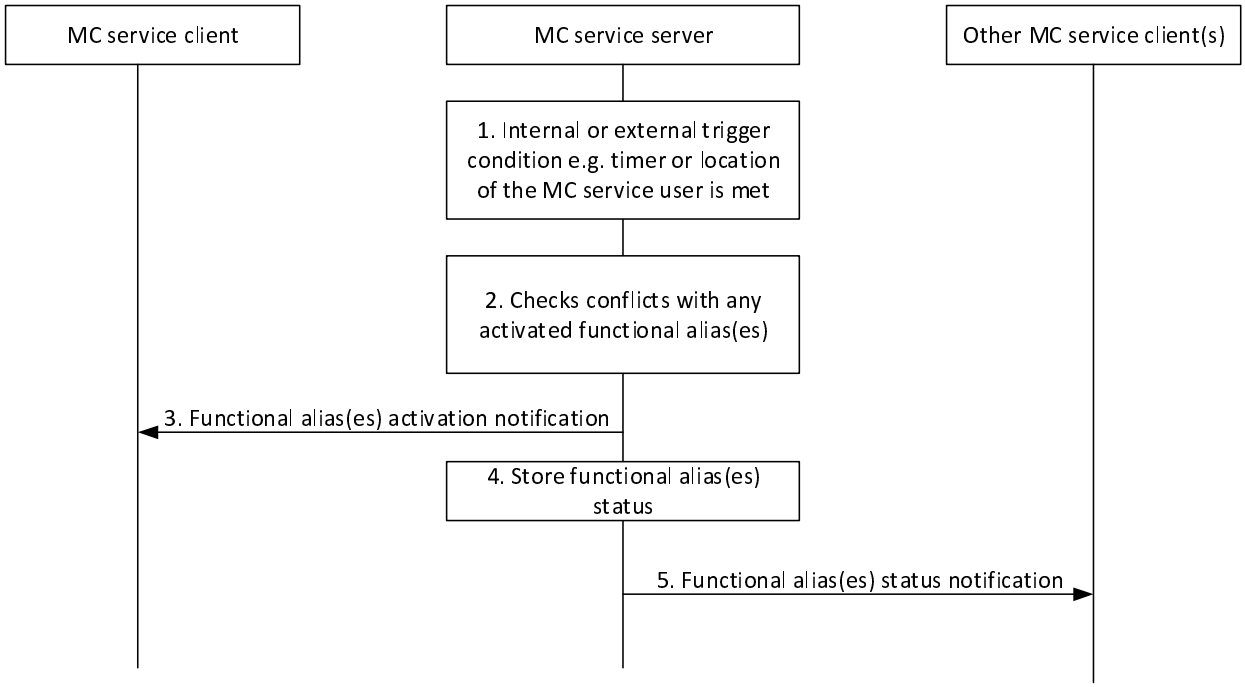

Figure 10.13.8-1: Automatic functional alias activation within an MC system

1. The condition e.g. timer or current location of the MC service user for automatic functional alias(es) activation is met.

2. The MC service server checks if there are any conflicts with current active functional alias(es).

   a.) If a certain functional alias(es) can be simultaneously active for multiple MC service users and the upper limit of simultaneous MC service users is not reached, the MC service server shall activate the functional alias(es) for the corresponding MC service user and inform all other MC service user(s) that are sharing the same functional alias(es) (step 5).

   b.) If the limit of simultaneous MC service users is reached or the functional alias is not allowed to be shared then the MC service server does not proceed with the functional alias(es) activation procedure or the MC service server can reassign the functional alias, i.e. takeover, from the MC service user currently using the functional alias(es) to the new MC service client.

3. MC service server notifies the MC service client about the activation of the functional alias(es).

4. The MC service server stores the functional alias(es) status for the functional alias(es), including date and time of activation.

5. The MC service server informs all other MC service user(s) sharing the same functional alias(es).

10.13.9 Automatic deactivation of functional alias(es) within an MC system

The MC Service Server can automatically activate functional aliases that can be specified by internal or external triggers such as location dependency, schedule, or timer.

The procedure for automatic deactivation of functional alias(es) within an MC system is illustrated in figure 10.13.9-1. The MC service client(s) get(s) notified by the MC service server at the time when a functional alias has been deactivated by the MC service server.

Pre-conditions:

1. MC service server has already retrieved the relevant functional alias(es) information from the configuration (functional alias) management server and has stored the data of the concerning functional alias(es) a MC service user has activated.

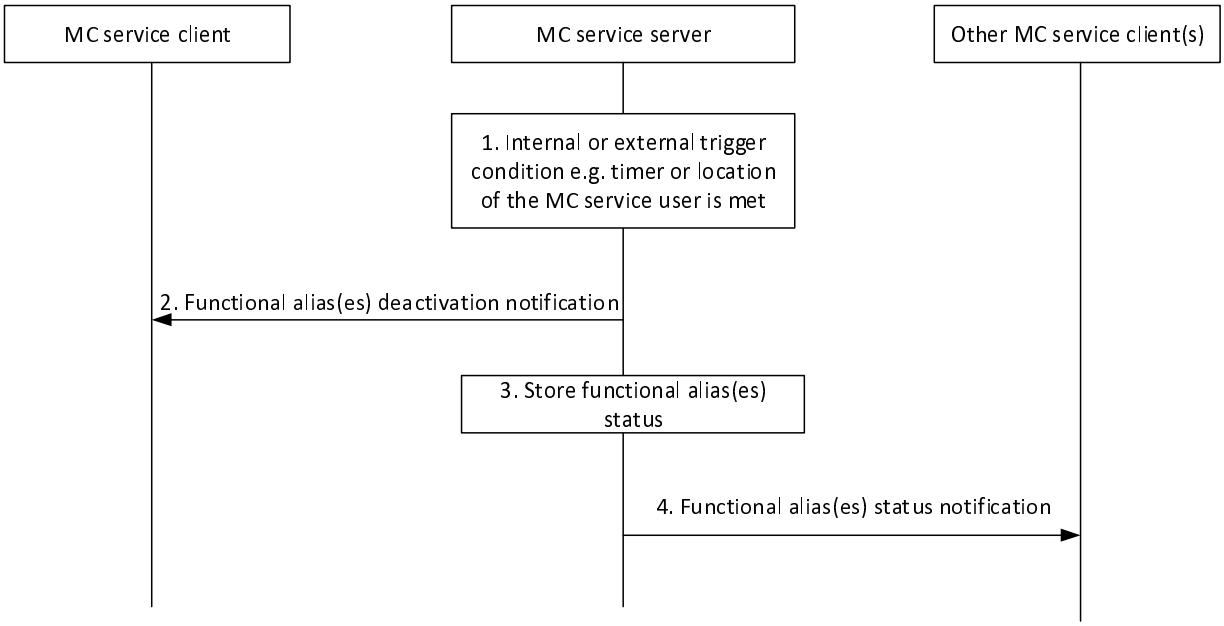

Figure 10.13.9-1: Automatic functional alias deactivation within an MC system

1. The condition e.g. timer or current location of the MC service user for automatic functional alias(es) deactivation is met. The trigger for deactivation may be done by the MC system or by an authorized external system attached to the MC system.
2. MC service server notifies the MC service client about the deactivation of the functional alias(es).
3. The MC service server stores the status, e.g. deactivated, of the concerned functional alias(es) and the corresponding MC service ID(s).
4. The MC service server informs all other MC service user(s) sharing the same functional alias(es).

10.13.10 Subscription and notification for functional alias

10.13.10.1 General

The subscriber (e.g. MC service server, location management server) obtains the list of MC service users who have activated a functional alias from the functional alias controlling MC service server via subscription and notification mechanisms.

10.13.10.2 Subscription for functional alias procedure

The procedure for subscription for functional alias is described in figure 10.13.10.2-1.

Pre-conditions:

- The functional alias controlling MC service server holds a list of MC service users who has activated the functional alias.

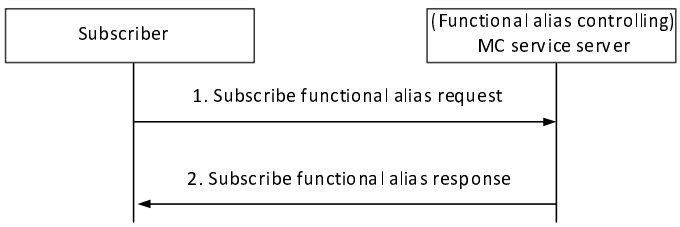

Figure 10.13.10.2-1: Subscription for functional alias

1. The subscriber sends a subscribe functional alias request to the functional alias controlling MC service server in order to receive notifications about the list of MC service users who has activated the function alias.

2. The functional alias controlling MC service server provides a subscribe functional alias response to the subscriber indicating success or failure of the request.

10.13.10.3 Notification for functional alias procedure

The procedure for notification for functional alias as shown in figure 10.13.10.3-1 is used by the functional alias controlling MC service server to inform the subscriber about MC service users who has activated the functional alias.

Pre-conditions:

- The subscriber has subscribed to the functional alias

- The list of MC service users who has activated the functional alias is changed at functional alias controlling MC service server due to activation, deactivation or taken over.

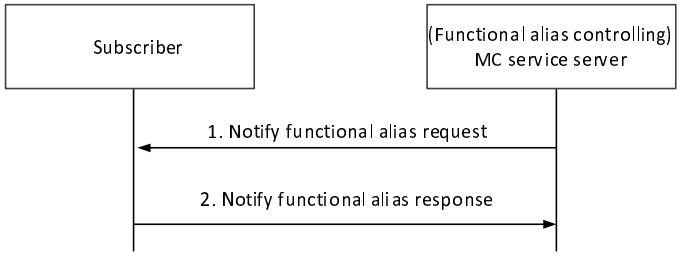

Figure 10.13.10.3-1: Notification for the functional alias

1. The functional alias controlling MC service server provides the list of MC service users who has activated the functional alias in the notify functional alias request to the subscriber.

2. The subscriber provides a notify functional alias response to the functional alias controlling MC service server.

10.13.10.4 Unsubscription for functional alias procedure

The procedure for unsubscription for functional alias is described in figure 10.13.10.4-1.

Pre-conditions:

- The functional alias controlling MC service server holds a list of MC service users who has activated the functional alias.

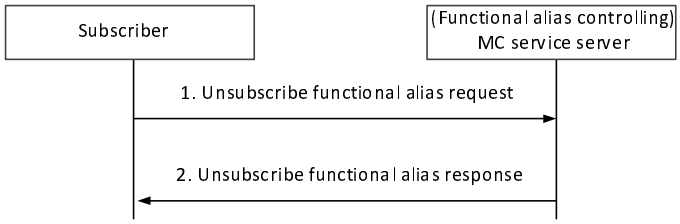

Figure 10.13.10.4-1: Unsubscription for functional alias

1. The subscriber sends a unsubscribe functional alias request to the functional alias controlling MC service server in order to stop receiving notifications about the list of MC service IDs who has activated the function alias.

2. The functional alias controlling MC service server provides a subscribe functional alias response to the subscriber indicating success or failure of the request.

10.13.11 Functional alias to group binding

10.13.11.1 General

The MC service client creates a functional alias to group binding association to be stored within the group controlling MC server. Once a functional alias is bound to a group it is bound till the functional alias is unbound to the group. After an MC service log-off the user's functional alias to group bindings are deleted.

NOTE: Affiliation and de-affiliation procedures do not change the functional alias to group binding.

10.13.11.2 Functional alias to group binding

The procedure for binding a functional alias with a group is described in figure 10.13.11.2-1.

Pre-conditions:

- The MC service server has subscribed to the MC service functional alias controlling server within the MC system for functional alias activation/de-activation updates.

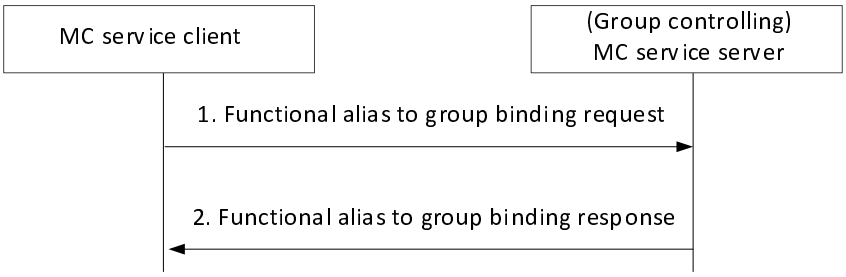

Figure 10.13.11.2-1: Functional alias to group binding procedure

1. The MC service client sends a functional alias to group binding request to the group controlling MC service server to bind functional aliases to groups to be used for communications within those groups.

2. The group controlling MC service server provides a functional alias to group binding response to the MC service client indicating success or failure of the request.

10.13.11.3 Functional alias to group unbinding

The procedure for unbinding a functional alias with a group is described in figure 10.13.11.3-1.

Pre-conditions:

- The MC service server has subscribed to the MC service functional alias controlling server within the MC system for functional alias activation/de-activation updates.

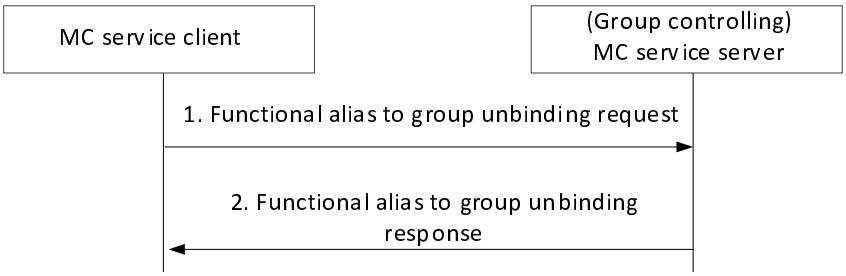

Figure 10.13.11.3-1: Functional alias to group unbinding procedure

1. The MC service client sends a functional alias to group unbinding request to the group controlling MC service server to unbind functional aliases from groups which are not used for communications within those groups anymore.

2. The group controlling MC service server provides a functional alias to group unbinding response to the MC service client indicating success or failure of the request. The MC service server also checks whether the MC service client is the last client who has bound a certain functional alias to a group which may prevent unbinding that functional alias from the group.

10.14 Generic procedures for interconnection

10.14.1 General

Interconnection provides a means for communication between different MC systems with differing levels of trust between those MC systems. This subclause describes generic procedures for interconnection which are variations of specific procedures detailed in 3GPP TS 23.379 [16] and 3GPP TS 23.281 [12]. These procedures should be read in conjunction with specific procedures in those specifications.

10.14.2 Generic call procedure with topology hiding

10.14.2.1 General

The procedure in this subclause applies to MC service group calls and private calls made between multiple MC systems where topology hiding is required. An MC gateway server in an MC system is used to route calls to and from partner MC systems, and by doing so hides the topology of the MC system.

10.14.2.2 Procedure for calls with topology hiding

Figure 10.14.2.2-1 shows the procedure where an MC service client initiates an MC service group call to an MC service group where the primary MC system of that MC service group is an interconnected MC system, or where an MC service client initiates an MC service private call to an MC service user where the primary MC system of that MC service user is an interconnected partner MC system. In this procedure, both MC systems make use of topology hiding.

NOTE 1: This procedure does not illustrate the case where the target MC service client has migrated, and where further forwarding of the call request is required.

Pre-conditions:

1. MC service client 1 is receiving MC service in a different MC system to the primary MC system of the target MC service group or MC service user, and the MC systems are interconnected.

NOTE 2: MC service client 1 may be receiving service in the primary MC system of MC service client 1, or may have successfully migrated to a partner MC system.

2. If the call to be originated by MC service client 1 is an MC service group call, MC service client 1 has affiliated to the MC service group.

3. If the call to be originated by MC service client 1 is an MC service private call, the target MC service client, MC service client 2, is receiving service from the primary MC system of that MC service client.

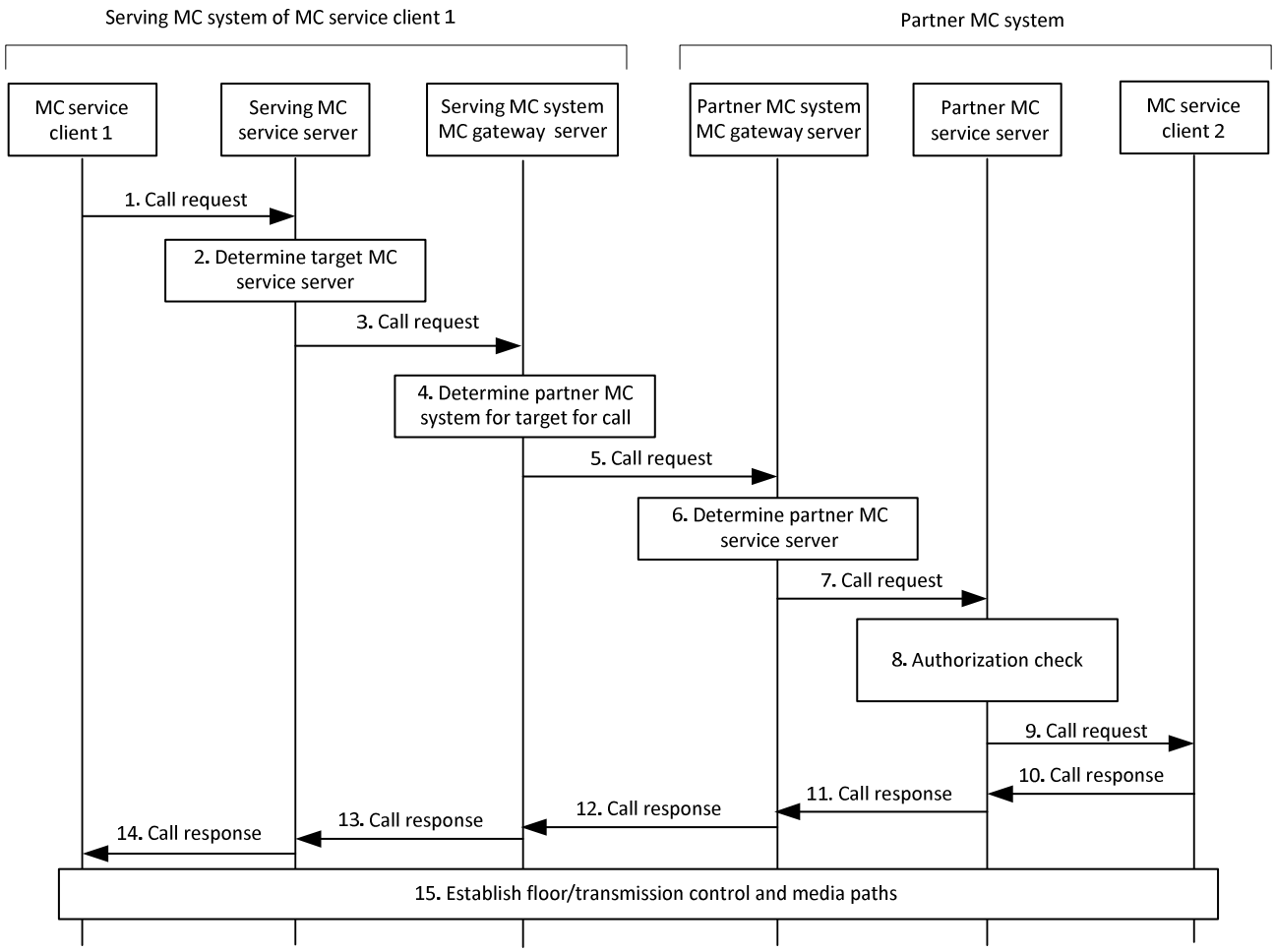

Figure 10.14.2.2-1: Call to target in interconnected MC system

1. MC service client 1 initiates a call request to a target MC service user or MC service group, where the primary MC system of that MC service user or MC service group is an interconnected partner MC system.

2. The serving MC service server of MC service client 1 determines that the call has a target in a different MC system, and that the MC gateway server is the correct next hop for the call.

3. The serving MC service server of MC service client 1 forwards the call request to the MC gateway server of the serving MC system.

4. The MC gateway server identifies the correct partner MC system which is the primary MC system for the target of the call.

NOTE 3: The MC gateway server of the serving MC system of MC service client 1 will contain configuration to allow it to route the call request over the signalling plane to the MC gateway server in the partner MC system.

5. The MC gateway server of the primary MC system of MC service client 1 forwards the call request to the MC gateway server of the partner MC system.

6. The MC gateway server of the partner MC system determines the MC service server which is the primary MC service server for the target MC service user or MC service group.

NOTE 4: The MC gateway server of the partner MC system will contain configuration allowing it to make use of the target MC service ID or MC service group ID to identify the primary MC service server of the target MC service user or MC service group.

7. The call request is forwarded to the partner MC service server which is the primary MC service server of the target MC service user or MC service group.

8. The partner MC service server which is the primary MC service server of the target MC service user or MC service group checks that the call is authorized to be made. The authorization process checks that the call origin is permissible (i.e. from the serving MC system of calling MC service user, and from that calling MC service user) for a call to the target MC service user or MC service group.

9. Providing that the authorization in step 8 is successful, the call request is sent to MC service client 2.

10. MC service client 2 sends a call response to the call request.

11. The partner MC service server, which is the primary MC service server of the target MC service user or MC service group, sends a call response to the MC gateway server in the partner MC system.

12. The MC gateway server in the partner MC system sends the call response to the MC gateway server in the primary MC system of MC service client 1.

13. The MC gateway server in the primary MC system sends the call response to the serving MC service server of MC service client 1.

14. The serving MC service server sends the call response to MC service client 1.

NOTE 5. Steps 9 and 10 may occur at any time after step 8 and prior to step 15, provided that step 9 always take place before step 10. If the authorization in step 8 has failed, then steps 9 and 10 do not occur.

15.If the call response was successful, floor control and media paths are established for the call.

10.14.3 Generic call procedure for enforcement of local MC service group configuration

10.14.3.1 General

The procedure in the following subclauses apply to MC service group calls made between multiple MC systems where the partner MC system applies local configuration to the MC service group configuration which has been provided by the primary MC system of the MC service group. The serving MC server of the MC service group members, that is a participating server for the MC service group, applies enforcement of local MC service group configuration.

10.14.3.2 MC service group call initiated in the partner MC system of the MC service group

Figure 10.14.3.2-1 shows the procedure where an MC service group call is initiated by an MC service client receiving MC service in the partner MC system of the MC service group.

NOTE 1: Any topology hiding by the primary or partner MC system of the MC service group is not shown within this procedure.

Pre-conditions:

1. MC service client 1 is receiving MC service in a partner MC system of the MC service group, and the MC systems are interconnected.

NOTE 2: MC service client 1 can be receiving service in the primary MC system of MC service client 1, or can have successfully migrated to a partner MC system.

2. MC service client 1 has affiliated to the MC service group.

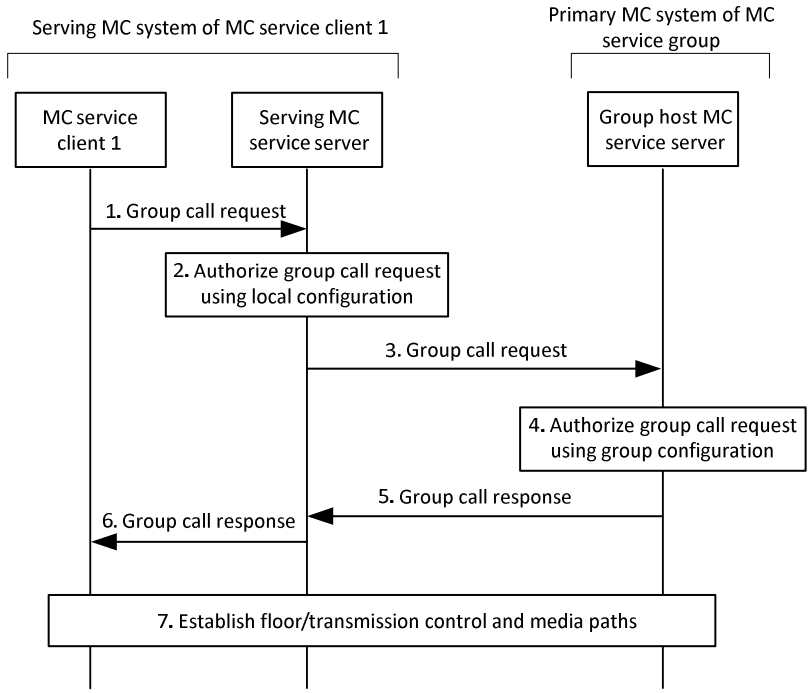

Figure 10.14.3.2-1: Enforcement of local configuration with call originated in partner MC system of MC service group

1. MC service client 1 initiates a group call request to the MC service group, where the primary MC system of that MC service group is an interconnected partner MC system.
2. The serving MC service server of MC service client 1 authorizes the group call request using local group configuration information.
3. If the group call request authorization by the serving MC service server of MC service client 1 is successful, the serving MC service server forwards the group call request to the group host MC service server in the primary MC system of the MC service group.
4. The primary MC service server of the MC service group checks that the call is authorized to be made. The authorization process checks that the call origin is permissible (i.e. from the serving MC system of calling MC service user, and from that calling MC service user) for a call to that MC service group.
5. Providing that authorization in step 4 is successful, the group call response is sent to the serving MC service server of MC service client 1.
6. The serving MC service server sends the MC service group call response to MC service client 1.
7. Floor control or transmission control and media paths are established for the MC service group call.

10.14.3.3 MC service group call request received from the primary MC system of the MC service group

Figure 10.14.3.3-1 shows the procedure where an MC service group call request is received from the primary MC system of the MC service group, which includes an MC service group member MC service client 1 that is receiving service within the partner MC system of the MC service group. Any topology hiding by the primary or partner MC system of the MC service group is not shown within this procedure.

Pre-conditions:

1. MC service client 1 is receiving MC service in a partner MC system of the MC service group, and the MC systems are interconnected.

NOTE: MC service client 1 can be receiving service in the primary MC system of MC service client 1, or can have successfully migrated to a partner MC system.

2. MC service client 1 has affiliated to the MC service group.

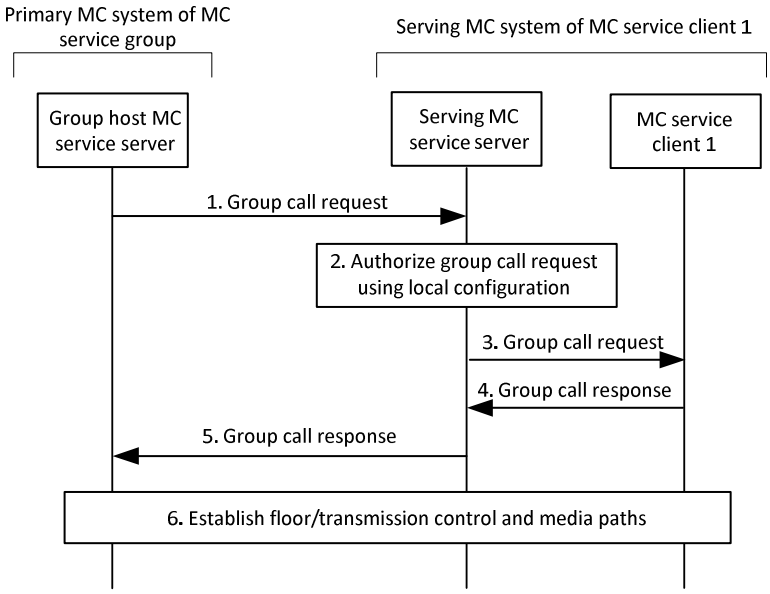

Figure 10.14.3.3-1: Enforcement of local configuration where group call request is received from primary MC system of MC service group

1. A group call request is received from the group host MC service server in the primary MC system of the MC service group.
2. The serving MC service server of MC service client 1 authorizes the group call request using local group configuration information.
3. If the group call request authorization by the serving MC service server of MC service client 1 is successful, the serving MC service server sends the group call request to MC service client 1.
4. MC service client 1 responds to the group call request with a group call response.
5. The group call response is sent to the group host MC service server of the MC service group.
6. Floor control or transmission control and media paths are established for the MC service group call.

10.14.4 Generic call procedure for media replication in participating MC system in MC service group calls

10.14.4.1 General

The procedure in the following subclause applies to MC service group calls made between multiple MC systems where the partner MC system carries out media replication to served MC service group members.

10.14.4.2 Media replication in the partner MC system of the MC service group

Figure 10.14.4.2-1 shows the procedure where an MC service group call is initiated by an MC service client receiving MC service in the primary MC system of the MC service group, and media replication takes place in the partner MC system.

NOTE 1: Any topology hiding by the primary or partner MC system of the MC service group is not shown within this procedure.

Pre-conditions:

1. MC service client 1 is receiving MC service in the primary MC system of the MC service group, and the MC systems are interconnected.

2. MC service clients 2, 3 and n are receiving MC service in the partner MC system of the MC service group.

NOTE 2: MC service clients 2,3 and n can be receiving MC service in the primary MC system of MC clients 2, 3 and n, or one or more of MC service clients 2, 3 and n can have successfully migrated to a partner MC system.

3. MC service clients 1, 2, 3 and n have affiliated to the MC service group.

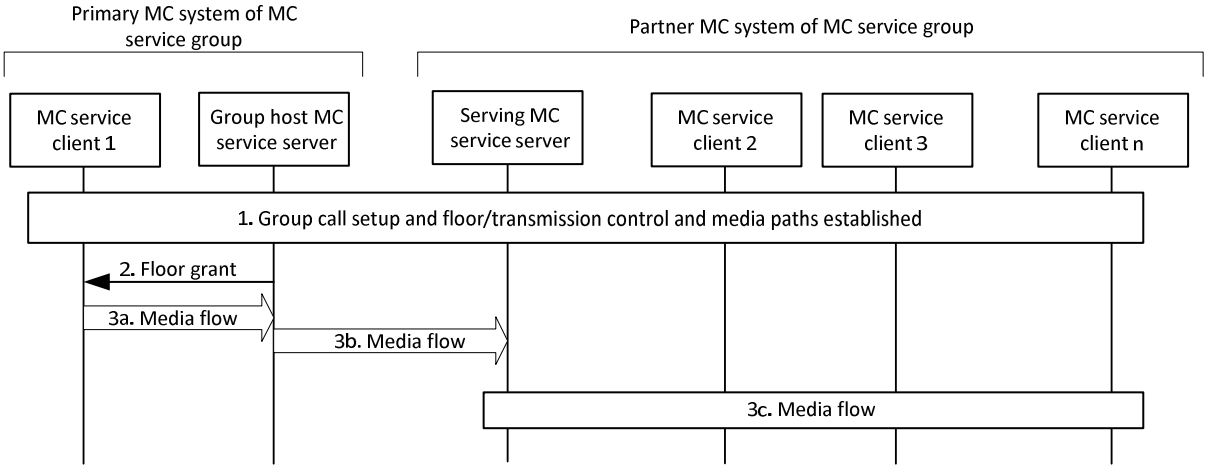

Figure 10.14.4.2-1: Media replication in partner MC system of MC service group

1. An MC service group call is set up and floor or transmission control and media paths are established, and MC service client 1 requests permission to transmit media to the MC service group.

2. The group host MC service server grants the requested floor or transmission permission to MC service client 1.

3a. MC service client 1 transmits a media stream to the group host MC service server.

3b. The group host MC service server sends a single media stream to the serving MC service server of MC service clients 2, 3 and n in the partner MC system of the MC service group.

3c. The serving MC service server of MC service clients 2, 3 and n replicates and distributes the media to MC service clients 2, 3 and n.

NOTE 3: Media distribution to MC service clients 2, 3 and n may be using unicast or multicast bearers.

10.15 Preconfigured regrouping

10.15.1 General

The following subclauses specify the information flows and procedures for group and user regrouping using preconfigured groups for a single MC service, and which are utilised by the following MC services:

- MCVideo (as specified in 3GPP TS 23.281 [12])
- MCData (as specified in 3GPP TS 23.282 [13])

NOTE: The information flows and procedures for group and user regrouping using preconfigured groups for MCPTT are specified in 3GPP TS 23.379 [16].

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.

10.15.2 Information flows for preconfigured regrouping

10.15.2.1 Preconfigured regroup request (MC service client – MC service server)

Table 10.15.2.1-1 describes the information flow preconfigured regroup request from the MC service client to the MC service server.

Table 10.15.2.1-1 Preconfigured regroup request information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the requester
MC service group ID	O	MC service group ID of the regroup group
MC service group ID	M	MC service group ID of the MC service group from which configuration is to be taken
MC service group ID list	O (see NOTE 1)	List of MC service groups to be regrouped into the group regroup group
MC service user ID list	O (see NOTE 1)	List of MC service users to be regrouped into the user regroup group
MC service user criteria	O (see NOTE 1, NOTE 2)	Carries the details of criteria which will be used by the MC service server for determining the participants. For example, it can be a location based criteria to determine the MC service user ID list in a particular area, or it could be tags (e.g. "fire", "medical", "police", etc.), or a combination of tags and location, which is left to implementation.
NOTE 1: One and only one of these shall be present. NOTE 2: This information element is used only for the user regroup procedures		

10.15.2.2 Preconfigured regroup request (MC service server – MC service client)

Table 10.15.2.2-1 describes the information flow preconfigured regroup request from the MC service server to the MC service client.

Table 10.15.2.2-1 Preconfigured regroup request information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the target MC service group member
MC service group ID	M	MC service group ID of the regroup group
MC service group ID	M	MC service group ID of the MC service group from which configuration is to be taken

10.15.2.3 Preconfigured regroup request (MC service server – MC service server)

Table 10.15.2.3-1 describes the information flow preconfigured regroup request from the MC service server to the MC service server.

Table 10.15.2.3-1 Preconfigured regroup request information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the requester
MC service group ID	M	MC service group ID of the regroup group
MC service group ID	M	MC service group ID of the MC service group from which configuration is to be taken
MC service group ID list	O	List of MC service groups to be regrouped into the group regroup group

10.15.2.4 Preconfigured regroup response (MC service client – MC service server)

Table 10.15.2.4-1 describes the information flow preconfigured regroup response from the MC service client to the MC service server.

Table 10.15.2.4-1 Preconfigured regroup response information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the responding MC service client
MC service group ID	M	MC service group ID of the regroup group
Result	M	Result of the regrouping operation

10.15.2.5 Preconfigured regroup response (MC service server – MC service client)

Table 10.15.2.5-1 describes the information flow preconfigured regroup response from the MC service server to the MC service client.

Table 10.15.2.5-1 Preconfigured regroup response information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the requester of the regrouping operation
MC service group ID	M	MC service group ID of the regroup group
Result	M	Result of the regrouping operation

10.15.2.6 Preconfigured regroup response (MC service server – MC service server)

Table 10.15.2.6-1 describes the information flow preconfigured regroup response from the MC service server to the MC service server.

Table 10.15.2.6-1 Preconfigured regroup response information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the responding MC service client
MC service group ID	M	MC service group ID of the regroup group
Result	M	Result of the regrouping operation

10.15.2.7 Preconfigured regroup cancel request (MC service client – MC service server)

Table 10.15.2.7-1 describes the information flow preconfigured regroup cancel request from the MC service client to the MC service server.

Table 10.15.2.7-1 Preconfigured regroup cancel request information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the requester
MC service group ID	M	MC service group ID of the regroup group

10.15.2.8 Preconfigured regroup cancel request (MC service server – MC service client)

Table 10.15.2.8-1 describes the information flow preconfigured regroup cancel request from the MC service server to the MC service client.

Table 10.15.2.8-1 Preconfigured regroup cancel request information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the target MC service user or MC service group member
MC service group ID	M	MC service group ID of the regroup group

10.15.2.9 Preconfigured regroup cancel request (MC service server – MC service server)

Table 10.15.2.9-1 describes the information flow preconfigured regroup cancel request from the MC service server to the MC service server.

Table 10.15.2.9-1 Preconfigured regroup cancel request information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the requester
MC service group ID	M	MC service group ID of the regroup group

10.15.2.10 Preconfigured regroup cancel response (MC service client – MC service server)

Table 10.15.2.10-1 describes the information flow preconfigured regroup cancel response from the MC service client to the MC service server.

Table 10.15.2.10-1 Preconfigured regroup cancel response information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the responding MC service client
MC service group ID	M	MC service group ID of the regroup group
Result	M	Result of the regrouping operation

10.15.2.11 Preconfigured regroup cancel response (MC service server – MC service client)

Table 10.15.2.11-1 describes the information flow preconfigured regroup cancel response from the MC service server to the MC service client.

Table 10.15.2.11-1 Preconfigured regroup cancel response information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the requester of the regroup removal
MC service group ID	M	MC service group ID of the regroup group
Result	M	Result of the regrouping operation

10.15.2.12 Preconfigured regroup cancel response (MC service server – MC service server)

Table 10.15.2.12-1 describes the information flow preconfigured regroup cancel response from the MC service server to the MC service server.

Table 10.15.2.12-1 Preconfigured regroup cancel response information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the requester of the regroup removal
MC service group ID	M	MC service group ID of the regroup group
Result	M	Result of the regroup removal operation

10.15.2.13 Preconfigured regroup reject (MC service server – MC service client)

Table 10.15.2.13-1 describes the information flow preconfigured regroup reject from the MC service server to the MC service client.

Table 10.15.2.13-1 Preconfigured regroup reject information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the requester of the regrouping
MC service group ID	M	MC service group ID of the regroup group
Reject reason	M	Reason for rejecting the regrouping operation

10.15.2.14 Preconfigured regroup reject (MC service server – MC service server)

Table 10.15.2.14-1 describes the information flow preconfigured regroup reject from the MC service server to the MC service server.

Table 10.15.2.14-1 Preconfigured regroup reject information elements

Information Element	Status	Description
MC service group ID	M	MC service group ID of the regroup group
Reject reason	M	Reason for rejecting the regrouping operation

10.15.2.15 Preconfigured user regroup remove request (MC service server – MC service client)

Table 10.15.2.15-1 describes the information flow preconfigured user regroup remove request from the MC service server to MC service client.

Table 10.15.2.15-1 Preconfigured user regroup remove request information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the MC service user to be removed from the regroup group
MC service group ID	M	MC service group ID of the regroup group from which the MC service user is to be removed

10.15.2.16 Preconfigured user regroup remove response (MC service client – MC service server)

Table 10.15.2.16-1 describes the information flow preconfigured user regroup remove response from the MC service client to the MC service server.

Table 10.15.2.16-1 Preconfigured user regroup remove response information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the MC service user to be removed from the preconfigured regroup
Result	M	Result of the preconfigured user regroup removal operation

10.15.3 Regroup with preconfigured group

10.15.3.1 General

A group regroup may be achieved by regrouping MC service groups into a new MC service regroup group which uses the configuration of a separate preconfigured MC service group. The MC service regroup group configuration needs to be provided to the relevant MC service group members of the MC service groups that will be regrouped in advance of the regrouping operation.

A user regroup may be achieved by regrouping MC service users into a new MC service regroup group which uses the configuration of a separate preconfigured MC service group. The MC service regroup group configuration needs to be provided to the relevant MC service users who will be regrouped in advance of the regrouping operation.

NOTE 1: A preconfigured group which is intended only to provide configuration for the preconfigured regroup process is identified by a parameter in group configuration described in this specification.

NOTE 2: The configuration may alternatively be taken from any MC service group that has been configured in the user profile of all the relevant MC service users who will be regrouped.

NOTE 3: Regroup groups may be defined according to the organizational structure of a mission critical organization, or by some other means which allows the MC service client of an authorized user to be aware of an appropriate regroup group for sets of MC service groups or MC service users that will be regrouped together.

The preconfigured MC service group that provides the configuration is not used as the MC service regroup group itself, it only provides configuration for one or more MC service regroup groups. The MC service group ID of the regroup group is provided by the authorized user when the preconfigured regrouping is carried out.

The MC service regroup group can be specified to be a broadcast or non-broadcast type according to the configuration of the MC service group whose configuration is specified by the regroup request. The broadcast type of regroup is used for one-way communication where only an authorized MC service user is allowed to transmit and all other regroup members are only allowed to receive the communication (e.g. a call from a dispatcher to all regroup members). The non-broadcast type is used for two-way communication where all regroup members can transmit and receive (i.e, the regroup group call behaves like a normal non-broadcast group call).

For group regrouping, if the MC service server has been notified by the group management server that one of the MC service groups that has been requested for regrouping by means of these procedures has already been regrouped, the MC service server shall reject the request for regrouping described in the following procedures.

10.15.3.2 Preconfigured regroup procedures in a single MC system

The following subclauses define group and user regroup procedures using preconfigured groups within a single MC system.

10.15.3.2.1 Preconfigured Group Regroup formation in a single MC system

Figure 10.15.3.2.1-1 illustrates the procedure to initiate a group regroup using a preconfigured MC service group. The procedure takes place prior to the establishment of a group call to the MC service regroup group.

Pre-conditions:

- MC service client 2 is an affiliated member of MC service group 1 and MC service client 3 is an affiliated member of MC service group 2.
- The MC service group identity and group configuration for the preconfigured MC service group have been preconfigured in MC service clients 2 and 3, and MC service clients 2 and 3 have received the relevant security related information to allow them to communicate in the MC service regroup group.
- MC service client 1 is authorized to initiate a preconfigured group regroup procedure.
- MC service client 1 is aware of a suitable MC service group whose configuration has been preconfigured in the MC service UEs of the group members who will be regrouped.
- In order to be aware whether a group is currently regrouped, the MC service server is subscribed to the group configuration in the GMS.
- The GMS has subscribed to group dynamic data from the MC service server using the procedures defined in subclause 10.1.5.6.

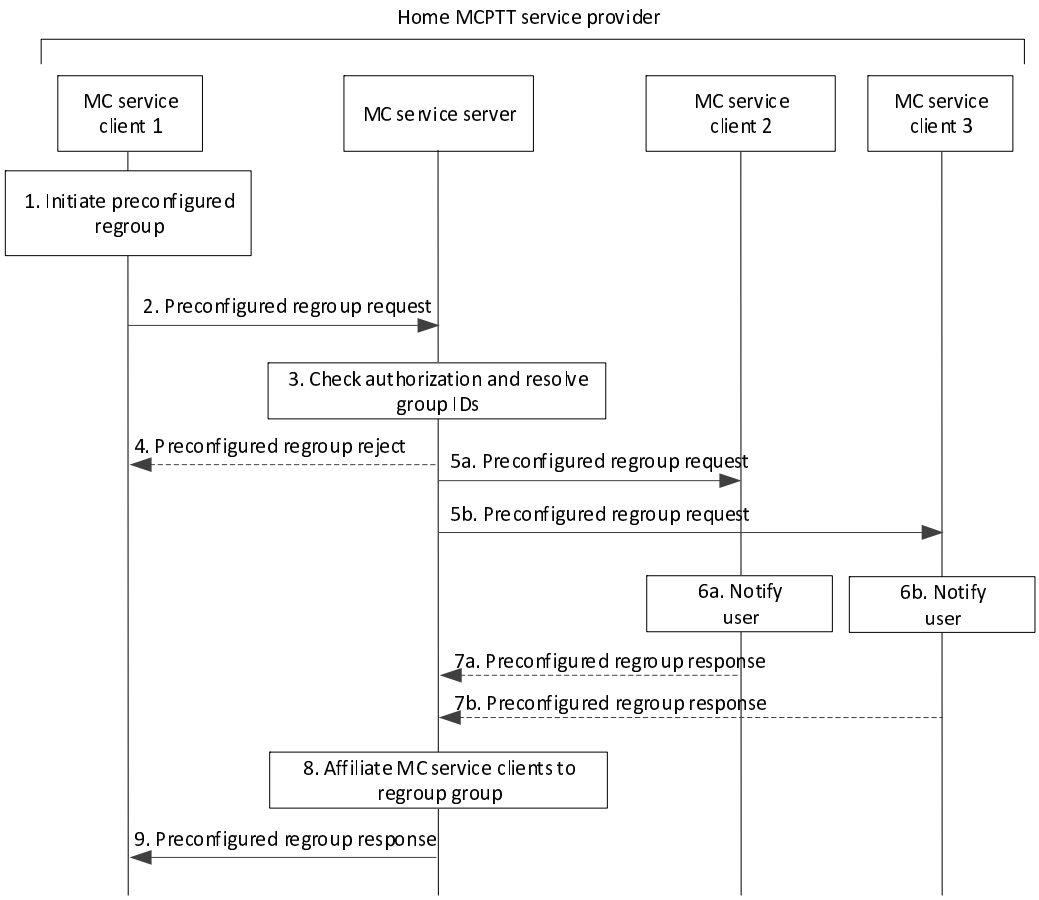

Figure 10.15.3.2.1-1: Regroup procedure using preconfigured group in a single MC system

1. The authorized user of MC service client 1 initiates the group regroup procedure, specifying the list of MC service groups to be regrouped (MC service groups 1 and 2), the MC service group ID of the regroup group and the MC service group ID of the group from which configuration information for the regroup group is to be taken.

2. MC service client 1 sends the preconfigured regroup request to the MC service server.

3. The MC service server checks that MC service client 1 is authorized to initiate a preconfigured group regroup procedure, and resolves the group identities of the MC service groups requested in step 1. The MC service server also checks which group members are affiliated to MC service groups 1 and 2. The MC service server may retrieve the configuration for the regroup group from the GMS if that configuration information is not already known to the MC service server. The MC service server also checks that none of the MC service groups that are requested for regrouping are already regrouped by any mechanism.

NOTE 1: This procedure does not require that that the authorized user of MC service client 1 is a group member of MC service groups 1 or 2, or that the authorized user of MC service client 1 is an affiliated group member of MC service groups 1 or 2.

NOTE 2: The list of groups included in the group regroup is held in dynamic data in the MC service server, and is not used to update group configuration information in the group management server.

4. If the MC service server determines that any of the groups requested for regrouping, including the regroup group, have been regrouped by other group regrouping procedures, the MC service server then sends a preconfigured regroup reject back to MC service client 1 with a reject reason indicating that one of the groups has already been regrouped, and this procedure terminates.

5. If the preconfigured regroup request is not rejected, the MC service server sends the preconfigured regroup requests to MC service clients 2 and 3 in steps 5a and 5b respectively.

NOTE 3: Only group members that are affiliated to the MC service groups that are to be regrouped are sent a preconfigured regroup request.

6. MC service clients 2 and 3 notify their users of the regrouping in steps 6a and 6b respectively.

7. MC service clients 2 and 3 may send the preconfigured regroup response to the MC service server to acknowledge the regrouping action. These acknowledgements are not sent in response to a multicast transmission of the preconfigured regroup request.

8. The MC service server affiliates the regrouped MC service clients to the regroup group.

9. The MC service server sends a preconfigured regroup response to MC service client 1.

After the group regrouping procedure, the regrouping remains in effect until explicitly cancelled by the procedure in 10.15.3.2.3.

MC service client participation in the ongoing regroup persists until the MC service client is no longer affiliated to any of the regrouped groups (group 1 or 2 in this procedure).

MC service client affiliation to the regroup group may cease when the UE's MC service ceases, e.g. when the UE is powered down, or by performing a log-off operation.

NOTE 4: Data persistence in the MC service client following a user log-off or power down is out of scope of the present document.

10.15.3.2.2 Preconfigured User Regroup formation in a single MC system

Figure 10.15.3.2.2-1 illustrates the procedure to initiate a user regroup procedure using a preconfigured MC service group. The procedure takes place prior to the establishment of a group call to the MC service regroup group.

Pre-conditions:

- MC service clients 2 and 3 are registered with the MC service server.

- The MC service group identity and group configuration for the preconfigured MC service group have been preconfigured in MC service clients 2 and 3, and MC service clients 2 and 3 have received the relevant security related information to allow them to communicate in the MC service regroup group.

- MC service client 1 is authorized to initiate a preconfigured user regroup procedure.

- MC service client 1 is aware of a suitable preconfigured group whose configuration has been preconfigured in the MC service UEs of the MC service users who will be regrouped.

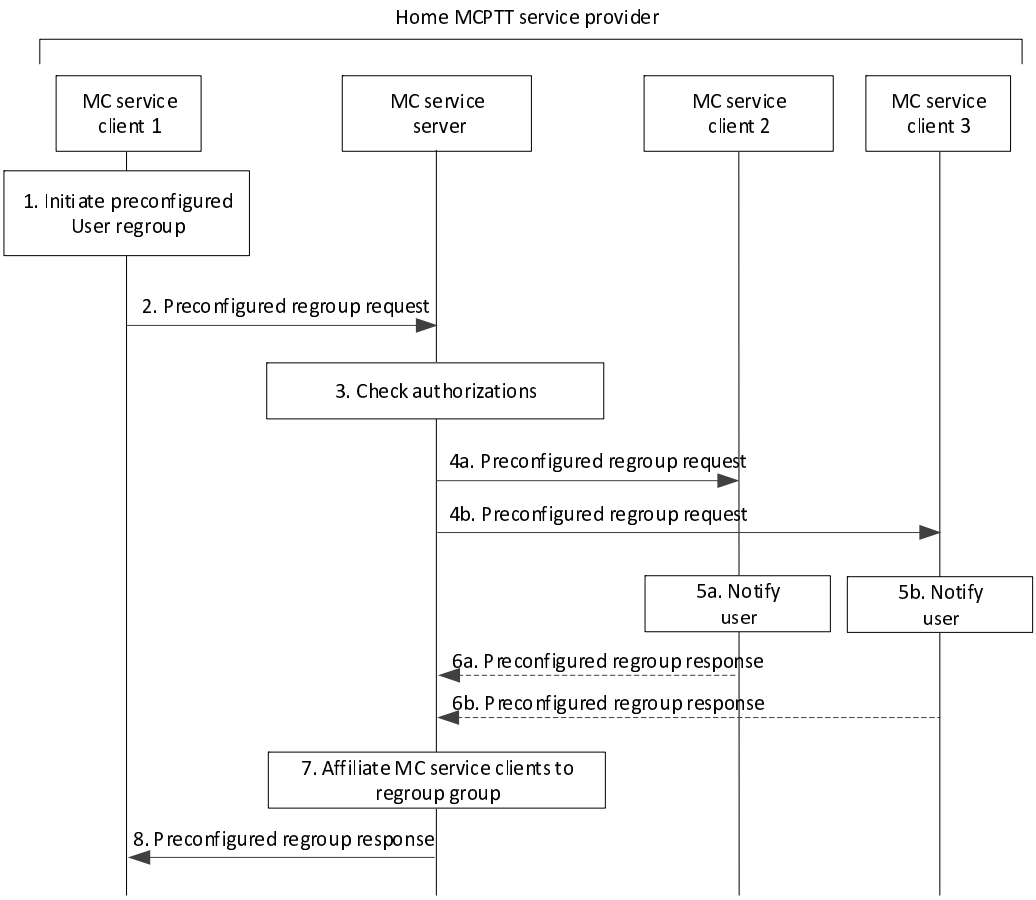

Figure 10.15.3.2.2-1: User regroup procedure using preconfigured group in a single MC system

1. The authorized user of MC service client 1 initiates the user regroup procedure, specifying the list of MC service users to be regrouped (MC service clients 2 and 3), the MC service group ID of the regroup group, and the MC service group ID of the group from which configuration information for the regroup group is to be taken. Alternatively, the MC service client 1 can provide the criteria which allows the MC service server to determine the list of MC service users to be regrouped.

2. MC service client 1 sends the preconfigured regroup request to the MC service server.

3. The MC service server checks that MC service client 1 is authorized to initiate a preconfigured user regroup procedure.

NOTE 1: MC service clients can be involved in multiple user and group regroups simultaneously.

4. The MC service server sends the preconfigured regroup requests to MC service clients 2 and 3 in steps 4a and 4b respectively.

NOTE 2: When using multicast, the MC service server can periodically rebroadcast the preconfigured regroup request.

5. MC service clients 2 and 3 notify their users of the regrouping in steps 5a and 5b respectively.

6. MC service clients 2 and 3 may send the preconfigured regroup response to the MC service server to acknowledge the regrouping action. These acknowledgements are not sent in response to a multicast transmission of the preconfigured regroup request.

7. The MC service server affiliates the regrouped MC service clients to the regroup group.

8. The MC service server sends a preconfigured regroup response to MC service client 1.

NOTE 3: After the user regrouping procedure, the regrouping remains in effect until explicitly cancelled by the procedure in 10.15.3.2.3.

10.15.3.2.3 Preconfigured regroup cancellation in a single MC system

Figure 10.15.3.2.3-1 illustrates the procedure to cancel a group or user regroup that uses a preconfigured MC service group.

Pre-conditions:

- MC service clients 2 and 3 have been regrouped into a MC service regroup group that uses the configuration of a preconfigured MC service group.
- MC service client 1 is authorized to cancel a group or user regroup that uses a preconfigured MC service group.
- The GMS has subscribed to group dynamic data from the MC service server using the procedures defined in subclause 10.1.5.6.

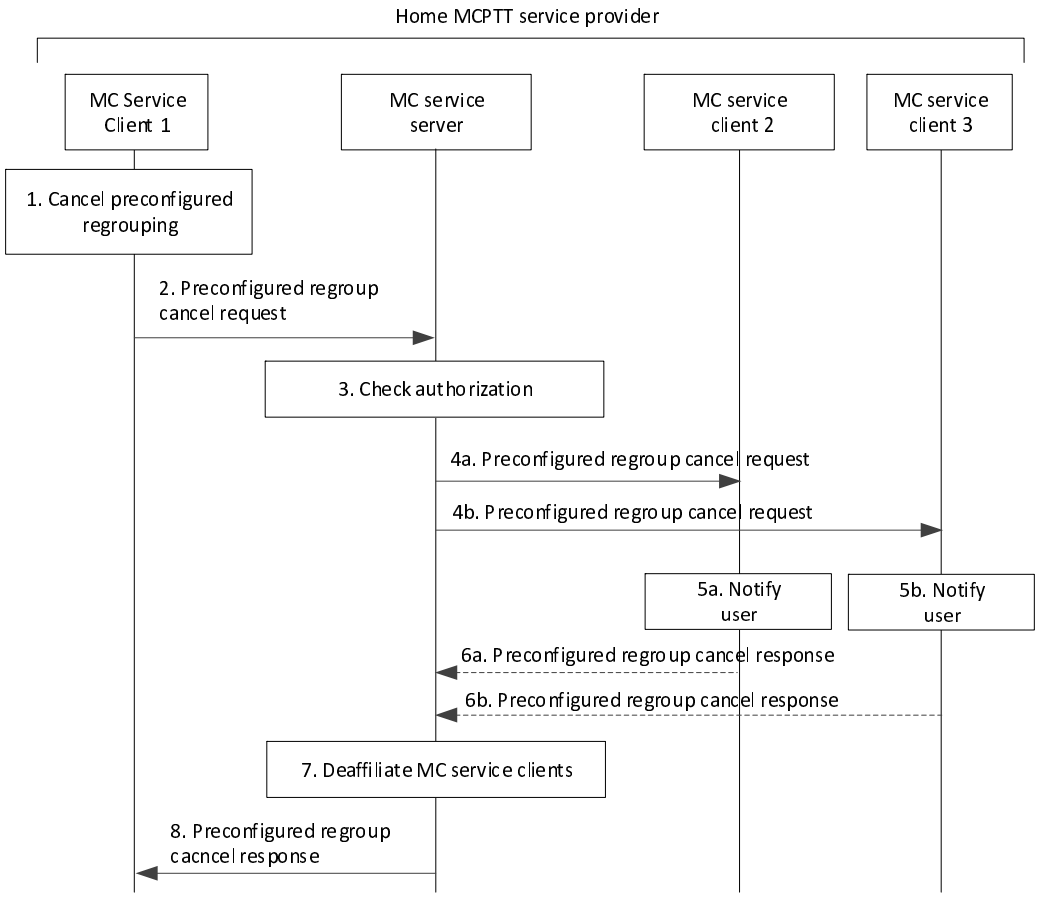

Figure 10.15.3.2.3-1: Cancel preconfigured regroup procedure in a single MC system

1. The authorized user of MC service client 1 initiates the cancellation of the regrouping that uses a preconfigured MC service group.
2. MC service client 1 sends the preconfigured regroup cancel request to the MC service server, specifying the MC service group ID of the regroup group.
3. The MC service server checks that MC service client 1 is authorized to cancel a regrouping that used a regroup procedure with preconfigured groups.
4. The MC service server sends the preconfigured regroup cancel request to MC service clients 2 and 3 (steps 4a and 4b respectively).
5. MC service clients 2 and 3 notify their users of the cancellation of the regrouping in steps 5a and 5b respectively.

6. MC service clients 2 and 3 may send the preconfigured regroup cancel response to the MC service server to acknowledge the cancellation of the regrouping function. These acknowledgements are not sent in response to a multicast transmission of the preconfigured regroup cancel request.

7. The MC service server deaffiliates MC service clients 2 and 3 from the MC service regroup group.

8. The MC service server sends a preconfigured regroup cancel response to MC service client 1.

10.15.3.3 Preconfigured regroup procedures in multiple MC systems

The following subclauses define group and user regroup procedures using preconfigured groups in multiple MC systems.

10.15.3.3.1 Preconfigured Group Regroup formation in multiple MC systems

Figure 10.15.3.3.1-1 illustrates the procedure to initiate a group regroup procedure using a preconfigured MC service group, where at least one of the groups to be regrouped is configured in a partner MC system. The primary MC system where the preconfigured group regrouping is initiated does not need to be aware of the list of group members belonging to groups whose group home system is the partner MC system. If the group management server in the primary MC system of the MC service regroup group shares the necessary security related parameters together with the group configuration of the preconfigured MC service group with the group management server in the partner MC system and the group management server in the partner MC system distributes this configuration including those security parameters to its served MC service users according to the procedures in subclause 10.2.7, the primary MC system does not need to be aware of the list of group members of the MC service regroup group that are receiving service in the partner MC system.

The procedure takes place prior to the establishment of a group call to the MC service regroup group.

In this procedure, any gateway MC servers in the primary or partner MC systems are not shown.

Pre-conditions:

- MC service client 1 is authorized to initiated a preconfigured regroup procedure, and is receiving MC service in the primary MC system of MC service client 1.

- MC service client 2 is an affiliated member of MC service group 1 where MC service group 1 is defined in the partner MC system and MC service client 2 is receiving service in the partner MC system of MC service client 1.

- The MC service group identity and group configuration for the preconfigured MC service group have been preconfigured in MC service client 2, and MC service client 2 has received the relevant security related information to allow communication in the MC service regroup group.

- In order to be aware whether the group is regrouped, the MC service server is subscribed to the group configuration in the GMS.

- The GMS has subscribed to group dynamic data from the MC service server within the same MC system using the procedures defined in subclause 10.1.5.6

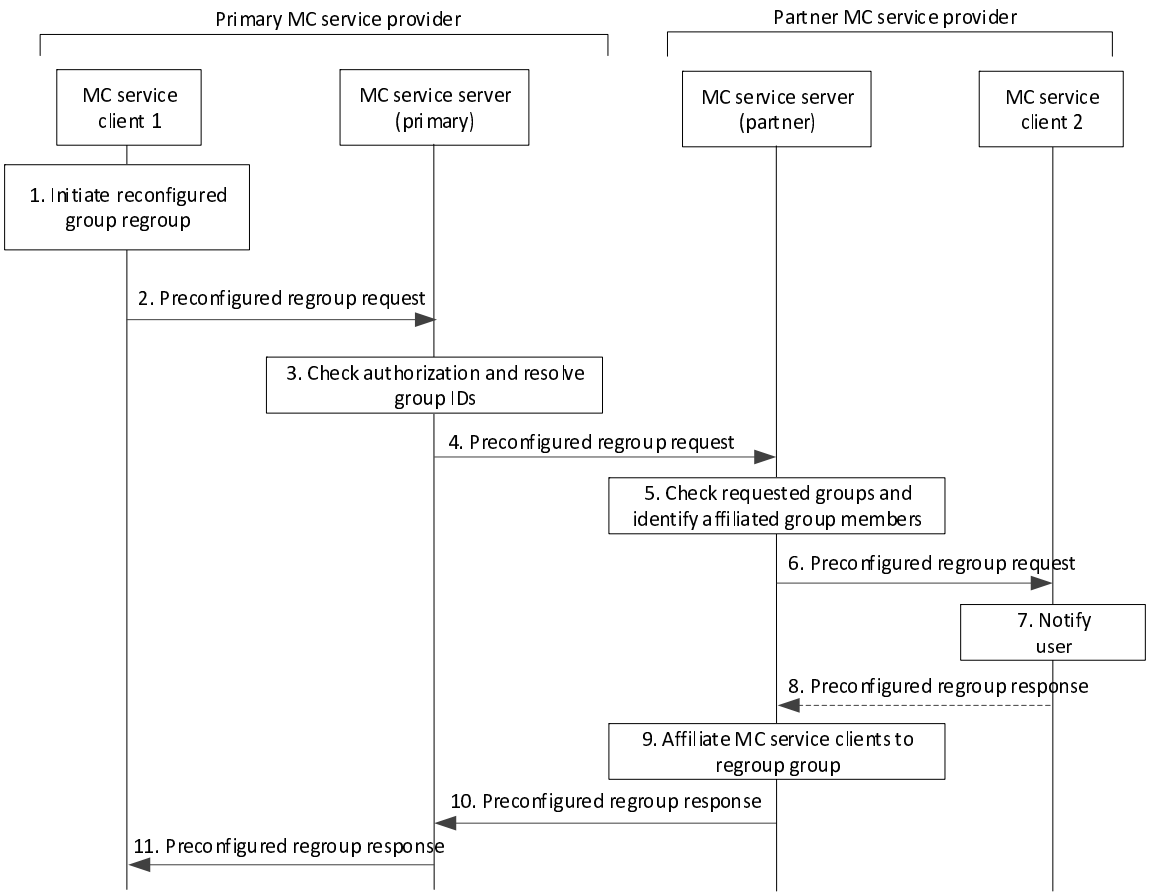

Figure 10.15.3.3.1-1: Group regroup procedure using preconfigured group in multiple MC systems

1. The authorized user of MC service client 1 initiates the group regroup procedure, specifying the list of MC service groups to be regrouped including MC service group 1, the MC service group ID of the regroup group and the MC service group ID of the group from which configuration information for the regroup group is to be taken.

2. MC service client 1 sends the preconfigured regroup request to the MC service server.

3. The MC service server checks that MC service client 1 is authorized to initiate a preconfigured group regroup procedure, and resolves the group identities of the MC service groups requested in step 1. The MC service server also checks which group members are affiliated to the requested MC service groups that are homed in the primary MC system. The MC service server identifies any partner systems which are the group home systems for MC service groups identified in the list of groups to be regrouped. The MC service server may retrieve the configuration for the regroup group from the GMS if that configuration information is not already known to the MC service server. The MC service server also checks that none of the MC service groups that are homed in the primary MC system and that are requested for regrouping are already regrouped by any mechanism.

NOTE 1: This procedure does not require that that the authorized user of MC service client 1 is a group member of the MC service groups listed in the regroup request, or that the authorized user of MC service client 1 is an affiliated group member of any of the listed MC service groups.

4. The MC service server sends the preconfigured regroup requests to the MC service server in the partner MC system.

5. The partner MC service server checks the status of any MC service groups hosted by that partner MC service server, and identifies affiliated group members of any of the identified MC service groups (both MC service groups that are hosted in the primary MC system and MC service groups that are hosted in the partner MC system) that are receiving MC service service in the partner MC system, which include MC service client 2.

6. The partner MC service server sends the preconfigured regroup request to MC service client 2.

NOTE 2: Only group members that are affiliated to the MC service groups that are to be regrouped are sent a preconfigured regroup request.

7. MC service client 2 notifies the user of the regrouping.
8. MC service client 2 may send the preconfigured regroup response to the partner MC service server to acknowledge the regrouping action. This acknowledgement is not sent in response to a multicast transmission of the preconfigured regroup request.
9. The partner MC service server affiliates the regrouped MC service client 2 to the regroup group.
10. The partner MC service server sends a preconfigured regroup response to the primary MC service server.
11. The primary MC service server sends the preconfigured regroup response to MC service client 1.

After the group regrouping procedure, the regrouping remains in effect until explicitly cancelled by the procedure in 10.15.3.3.3.

MC service client participation in the ongoing regroup persists until the MC service client is no longer affiliated to any of the regrouped groups (group 1 or 2 in this procedure).

MC service client affiliation to the regroup group may cease when the UE's MC service ceases, e.g. when the UE is powered down, or by performing a log-off operation.

NOTE 3: Data persistence in the MC service client following a user log-off or power down is out of scope of the present document.

10.15.3.3.2 Preconfigured User Regroup formation in multiple MC systems

Figure 10.15.3.3.2-1 illustrates the procedure to initiate a user regroup procedure using a preconfigured MC service group, where at least one of the MC service users to be regrouped is homed in a partner MC system. It is assumed that the group management server in the primary MC system of the MC service regroup group shares the necessary security related parameters together with the group configuration of the preconfigured MC service group with the group management server in the partner MC system and the group management server in the partner MC system distributes this configuration including those security parameters to its served MC service users according to the procedures in subclause 10.2.7.

The procedure takes place prior to the establishment of a group call to the MC service regroup group.

In this procedure, any gateway MC servers in the primary or partner MC systems are not shown.

Pre-conditions:

- MC service client 1 is homed in the primary MC system and is receiving service in the primary MC system.
- MC service client 2 is homed in the partner MC system and is receiving service in the partner MC service system of MC client 1.
- The MC service group identity and group configuration for the preconfigured MC service group have been preconfigured in MC service client 2, and MC service client 2 has received the relevant security related information to allow communication in the MC service regroup group.
- MC service client 1 is authorized to initiate a preconfigured user regroup procedure.
- MC service client 1 is aware of a suitable preconfigured group whose configuration has been preconfigured in the MC service UEs of the MC service users who will be regrouped.

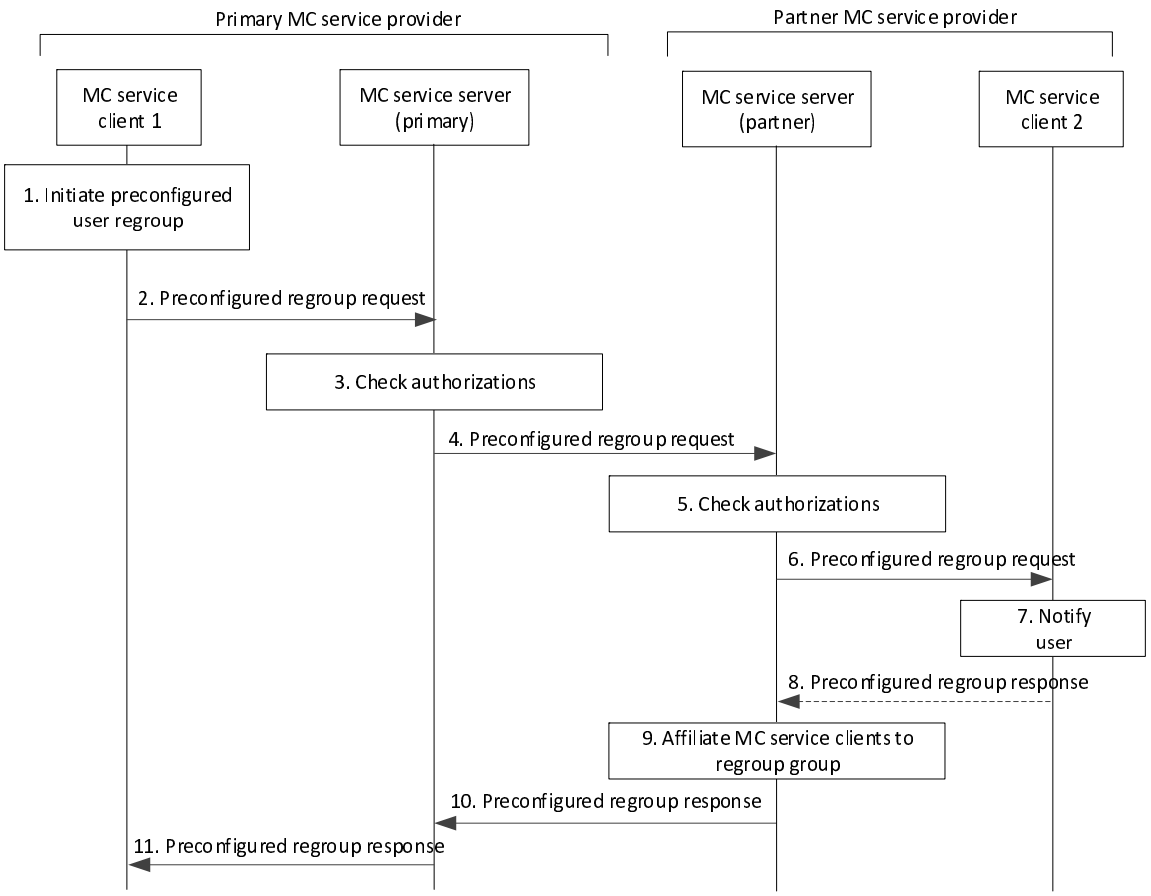

Figure 10.15.3.3.2-1: User regroup procedure using preconfigured group in multiple MC systems

1. The authorized user of MC service client 1 initiates the user regroup procedure, specifying the list of MC service users to be regrouped including MC service client 2, the MC service group ID of the regroup group, and the MC service group ID of the group from which configuration information for the regroup group is to be taken.
2. MC service client 1 sends the preconfigured regroup request to the primary MC service server. The request indicates the list of users to be included in the regroup operation.
3. The primary MC service server checks that MC service client 1 is authorized to initiate a preconfigured user regroup procedure.

NOTE 1: MC service clients can be involved in multiple user and group regroups simultaneously.

4. The primary MC service server sends the preconfigured regroup requests to the MC service server in the partner MC system.
5. The partner MC service server checks that the primary MC service server is authorized to include MC service users homed in the partner system.
6. The partner MC service server sends the preconfigured regroup request to MC service client 2.
7. MC service client 2 notifies the user of the regrouping.
8. MC service client 2 may send the preconfigured regroup response to the partner MC service server to acknowledge the regrouping action. This acknowledgement is not sent in response to a multicast transmission of the preconfigured regroup request.
9. The partner MC service server affiliates the regrouped MC service client 2 to the regroup group.
10. The partner MC service server sends a preconfigured regroup response to the primary MC service server.
11. The primary MC service server sends the preconfigured regroup response to MC service client 1.

NOTE 2: After the user regrouping procedure, the regrouping remains in effect until explicitly cancelled by the procedure in 10.15.3.3.3.

10.15.3.3.3 Preconfigured regroup cancellation in multiple MC systems

Figure 10.15.3.3.3-1 illustrates the procedure to cancel a group or user regroup that uses a preconfigured MC service group where multiple MC systems were involved in the regrouping.

Pre-conditions:

- MC service client 2 has been regrouped into the MC service regroup group, and is receiving service in the partner MC system of the regroup group.
- MC service client 1 is authorized to cancel a regrouping that uses a preconfigured MC service group, and is receiving service in the primary MC system of the regroup group.
- The GMS has subscribed to group dynamic data from the MC service server within the same MC system using the procedures defined in subclause 10.1.5.6.

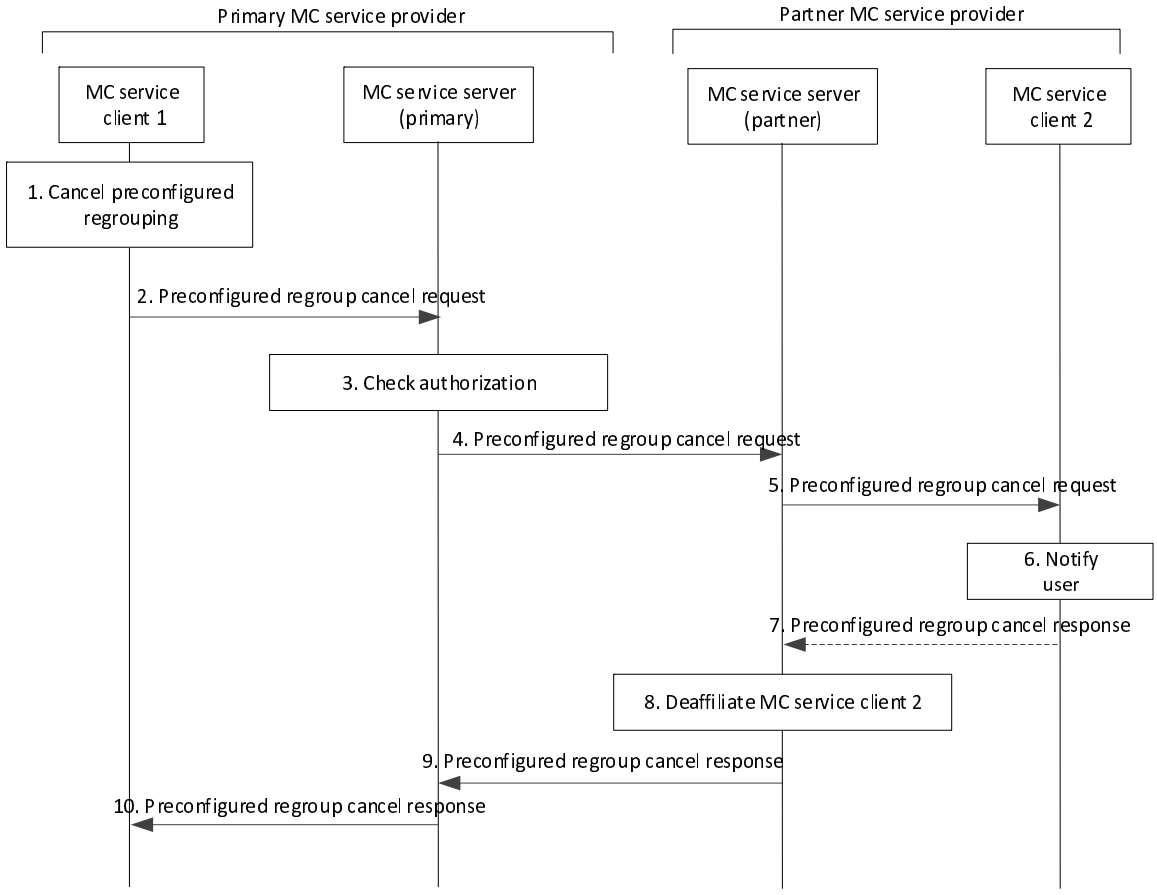

Figure 10.15.3.3.3-1: Cancel preconfigured regroup procedure in multiple MC systems

1. The authorized user of MC service client 1 initiates the cancellation of the regrouping that uses a preconfigured MC service group.
2. MC service client 1 sends the preconfigured regroup cancel request to the MC service server, specifying the MC service group ID of the regroup group.
3. The MC service server checks that MC service client 1 is authorized to cancel a regrouping that uses a preconfigured group regroup procedure.
4. The primary MC service server sends the regroup cancel request to the partner MC service server.
5. The partner MC service server sends the preconfigured regroup cancel requests to MC service client 2.

6. MC service client 2 notifies the user of the cancellation of the group regrouping.
7. MC service client 2 may send the preconfigured regroup cancel response to the partner MC service server to acknowledge the cancellation of the regrouping function. This acknowledgement is not sent in response to a multicast transmission of the preconfigured regroup cancel request.
8. The partner MC service server deaffiliates MC service client 2 from the MC service regroup group.
9. The partner MC service server sends the preconfigured regroup cancel response to the primary MC service server.
10. The primary MC service server sends a preconfigured regroup cancel response to MC service client 1.

10.15.3.3.4 Preconfigured group regroup rejection in multiple MC systems

Figure 10.15.3.3.4-1 illustrates the case where the procedure to initiate a group regroup with multiple MC systems using a preconfigured MC service group described in subclauses 10.15.3.3.1 commences, but where the request for the regroup is rejected by the partner MC service server. The rejection can occur, for example because one of the groups hosted by the partner MC service server is already regrouped by other group regrouping procedures.

In this procedure, any gateway MC servers in the primary or partner MC systems are not shown.

Pre-conditions:

- MC service client 1 is authorized to initiated a preconfigured regroup procedure, and is receiving MC service in the primary MC system of MC service client 1.
- In order to be aware whether the group is regrouped, the MC service server within the same MC system is subscribed to the group configuration in the GMS.

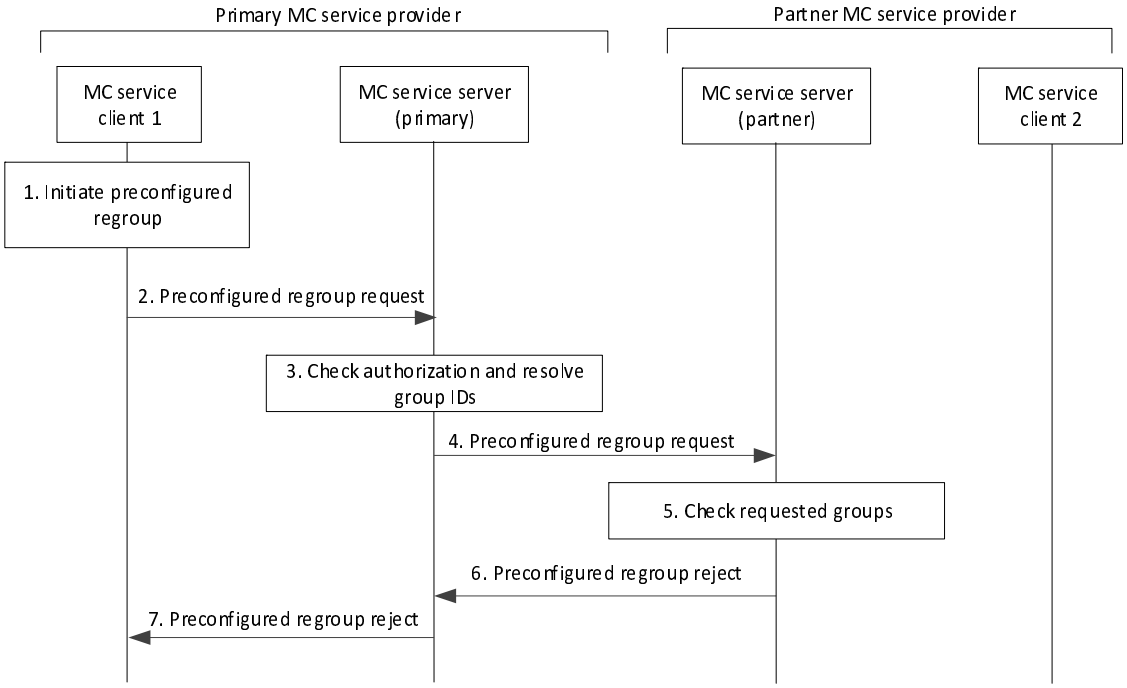

Figure 10.15.3.3.4-1: Regroup rejection using preconfigured group in multiple MC systems

1. The authorized user of MC service client 1 initiates the group regroup procedure, specifying the list of MC service groups to be regrouped including MC service group 1, the MC service group ID of the regroup group and the MC service group ID of the group from which configuration information for the regroup group is to be taken.
2. MC service client 1 sends the preconfigured regroup request to the MC service server.

3. The MC service server checks that MC service client 1 is authorized to initiate a preconfigured group regroup procedure, and resolves the group identities of the MC service groups requested in step 1. The MC service server also checks which group members are affiliated to the requested MC service groups that are homed in the primary MC system. The MC service server identifies any partner systems which are the group home systems for MC service groups identified in the list of groups to be regrouped. The MC service server may retrieve the configuration for the regroup group from the GMS if that configuration information is not already known to the MC service server. The MC service server also checks that none of the MC service groups that are homed in the primary MC system and that are requested for regrouping are already regrouped by any mechanism.

NOTE 1: This procedure does not require that that the authorized user of MC service client 1 is a group member of the MC service groups listed in the regroup request, or that the authorized user of MC service client 1 is an affiliated group member of any of the listed MC service groups.

4. The MC service server sends the preconfigured regroup requests to the MC service server in the partner MC system.

5. The partner MC service server checks the status of any MC service groups hosted by that partner MC service server, and determines that one or more requested MC service groups has already been regrouped by another group regrouping procedure.

6. The partner MC service server sends a preconfigured regroup reject to the primary MC service server, indicating the reason for rejection.

7. The primary MC service server sends a preconfigured regroup reject to MC service client 1, indicating the reason for rejection.

10.15.3.4 Other preconfigured regroup procedures

10.15.3.4.1 Adding newly affiliated user to preconfigured group regroup

Figure 10.15.3.4.1-1 illustrates the procedure to add a newly affiliated user to an in-progress preconfigured MC service group regroup operation.

Pre-conditions:

- The MC service client is a member of a MC service group that is part of an in-progress preconfigured group regroup operation.

- The MC service group identity and group configuration for the preconfigured MC service group has been preconfigured in the MC service client, and the MC service client has received the relevant security related information to allow it to communicate in the MC service regroup group.

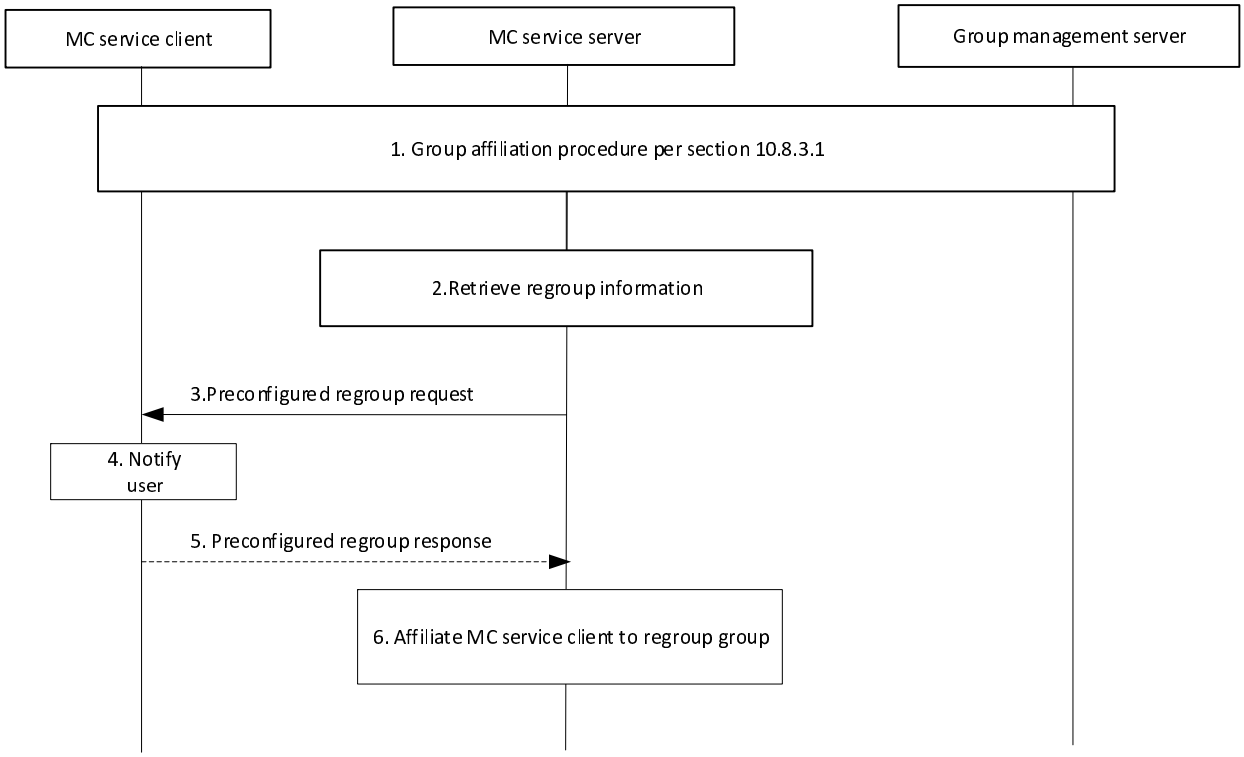

Figure 10.15.3.4.1-1: Procedure to add a newly affiliated user to a preconfigured group regroup

1. The MC service client affiliates to an MC service group that is currently part of an in-progress preconfigured group regroup. The affiliation follows the procedure in section 10.8.3.1 of this specification.
2. The MC service server retrieves the MC service group ID of the regroup group and the MC service group ID of the group from which configuration information for the regroup group is to be taken.
3. The MC service server sends the preconfigured regroup request to the MC service client.
4. The MC service client notifies the user of the regrouping.
5. The MC service client may send the preconfigured regroup response to the MC service server to acknowledge the regrouping action. These acknowledgements are not sent in response to a multicast transmission of the preconfigured regroup request.
6. The MC service server affiliates the regrouped MC service client to the regroup group.

NOTE 1: Whether this procedure can be generalized to apply to both preconfigured and GMS-based group regrouping is out of scope of the present document.

NOTE 2: Affiliations of the MC service client to the regroup group in the MC service server and coordination to the MC System is out of scope of the present document.

10.15.3.4.2 Updating the MC service ID list in a preconfigured regroup group based on user regroup

Figure 10.15.3.4.2-1 illustrates the procedure to add or remove an MC service user based on the MC service user criteria known at the MC service server.

NOTE 1: This procedure applies to MC service users that have been added and are to be added to the preconfigured regroup group based on MC service user criteria known at the MC service server. If only the criteria are to be applied, then only the criteria are included in the request and the group and user lists are not included

Preconditions:

- A preconfigured regroup group has been established.
- The MC service server has selected MC service user 2 to participate in the preconfigured regroup group based on MC service user criteria known at the MC service server.

NOTE 2: Other participants of the preconfigured regroup group are not shown in figure 10.15.3.4.x-1 for simplicity.

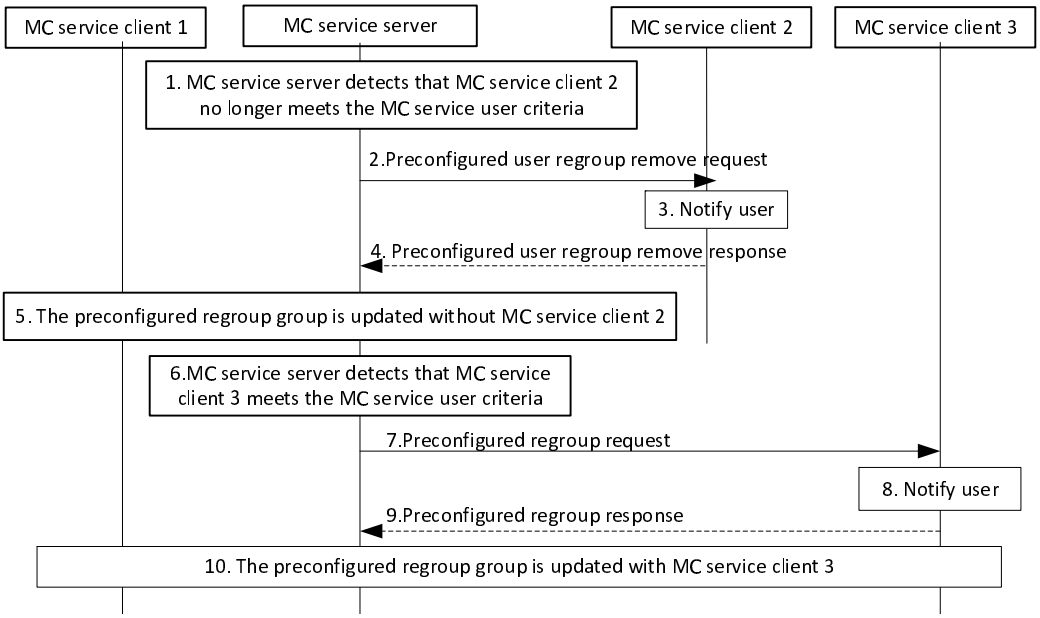

Figure 10.15.3.4.2-1: Procedure to update the MC service ID list

1. The MC service server detects that MC service client 2, which has been earlier included in the preconfigured regroup group, no longer meets the MC service user criteria known at the MC service server.
2. The MC service sends MC service client 2 a preconfigured user regroup remove request.
3. The MC service client 2 notifies the MC service user of the preconfigured user regroup removal.
4. The MC service client 2 may send the MC service server a preconfigured user regroup remove response to acknowledge the preconfigured user regroup removal.
5. The MC service server updates the preconfigured regroup group (including the MC service user ID list) and potential group communication.
6. The MC service server detects that the MC service client 3 meets the MC service user criteria.
7. The MC service server sends the MC service client 3 a preconfigured regroup request.
8. The MC service client 3 notifies the MC service user of the preconfigured regroup request.
9. The MC service client 3 may send the MC service server a preconfigured regroup response.
10. The MC service server updates the preconfigured regroup group (including the MC service user ID list), and potential group communication.

10.16 Generic procedures for migration

10.16.1 General

Migration provides a means for an MC service user to obtain MC service directly from a partner MC system. This subclause describes generic procedures for migration which are variations of specific procedures detailed in 3GPP TS 23.379 [16], 3GPP TS 23.281 [12] and 3GPP TS 23.282 [13]. These procedures should be read in conjunction with specific procedures in those specifications.

10.16.2 Migration during an ongoing group communication

10.16.2.1 General

This provides the capability for an MC service user to migrate to another MC system during an ongoing group communication and to continue the group communication in the other MC system.

NOTE: The migration during an ongoing group communication for MCData is not supported in present document.

10.16.2.2 Procedure

The procedure is based on the following existing procedures:

- MC service group de-affiliation procedure as described in clause 10.8.4.2, or
- De-affiliation from MC service group(s) defined in partner MC service system as described in clause 10.8.4.3.
- MC service user receiving MC service from a partner MC system as described in clause 10.1.4.3.2.
- MC service group affiliation procedure as described in clause 10.8.3.1, or
- Affiliation to MC service group(s) defined in partner MC system as described in clause 10.8.3.2 or clause 10.8.3.2a.
- Late entry MCPTT group call as described in 3GPP TS 23.379 [16] clause 10.6.2.3.1.1.4 (pre-arranged group call) and 3GPP TS 23.379 [16] clause 10.6.2.3.1.2.5 (chat group call).
- Late entry MCVideo group call as described in 3GPP TS 23.281 [12] clause 7.1.2.3.1.1.4 (pre-arranged) and 3GPP TS 23.281 [12] clause 7.1.2.3.1.2.6 (chat group call).

Pre-conditions:

1. The MC service client is a receiving party in one or more ongoing group calls in the primary MC system.
2. The MC service UE detects the need to change the MC system.

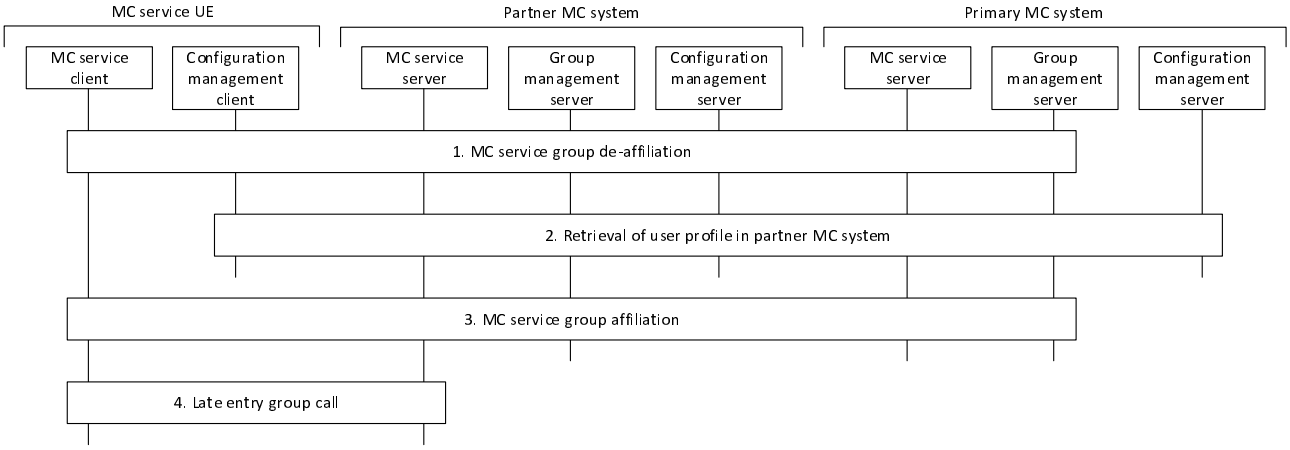

Figure 10.16.2.2-1: Migration to partner MC system during an ongoing group call

1. The MC service client requests de-affiliation from MC service groups. The MC service groups are either defined in the primary MC system (see clause 10.8.4.2) or the partner MC system (see clause 10.8.4.3).

2. After migration to the partner MC system, the configuration management client triggers retrieval of the MC service user profile used within the partner MC system (see clause 10.1.4.3.2).

NOTE: User authentication and service authorisation procedures are not shown.

3. The MC service client requests affiliation to MC service groups. The MCPTT groups are either defined in the primary MC system (see clause 10.8.3.1) or the partner MC system (see clause 10.8.3.2 or clause 10.8.3.2a).

4. If any of the received group calls are ongoing in the partner MC system, the partner MC system shall initiate a late-entry procedure towards the MC service client. If any of the received group calls are taken place in the primary MC system but not yet in the partner MC system, the affiliation by the migrated MC service UE triggers the late-entry procedure which then includes the MC service UE and the partner MC system into the group call.

The MC service client may indicate the successful migration of group communications to the MC service user.

10.16.2.3 Void

10.16.2.3.1 Void

10.16.3 Private call using functional alias towards a partner MC system

10.16.3.1 General

This provides the possibility for an MC service user to initiate a private MC service call using a functional alias, defined in the partner MC system, as target address towards an MC service user in a partner MC system.

10.16.3.2 Information flows

10.16.3.2.1 MC service functional alias resolution request

Table 10.16.3.2.1-1 describes the information flow MC service functional alias resolution request from the MC service server to the MC service functional alias controlling server and from the MC service functional alias controlling server to another MC service functional alias controlling server.

Table 10.16.3.2.1-1: MC service functional alias resolution request information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the calling party
Functional alias	O	The functional alias of the calling party
Functional alias	M	The functional alias of the called party

10.16.3.2.2 MC service functional alias resolution response

Table 10.16.3.2.2-1 describes the information flow MC service functional alias resolution response from the MC service functional alias controlling server to another MC service functional alias controlling server, the MC service functional alias controlling server to the MC service server and the MC service server to the MC service client.

Table 10.16.3.2.2-1: MC service functional alias resolution response information elements

Information Element	Status	Description
MC service ID	M	The MC service ID of the calling party
MC service ID	M	The corresponding MC service ID of the called functional alias. Return "NONE" if no one activates the targeted Functional Alias.

10.16.3.3 Procedure

Figure 10.16.3.3-1 represents a generic MC service private call setup procedure to allow using the functional alias as called party address, i.e., the MC service ID address is resolved by the partner MC system through the primary MC service server and primary MC service functional alias controlling server.

Additional new pre-condition:

1. A secured connection has been established between the MC service functional alias controlling servers in different MC systems.

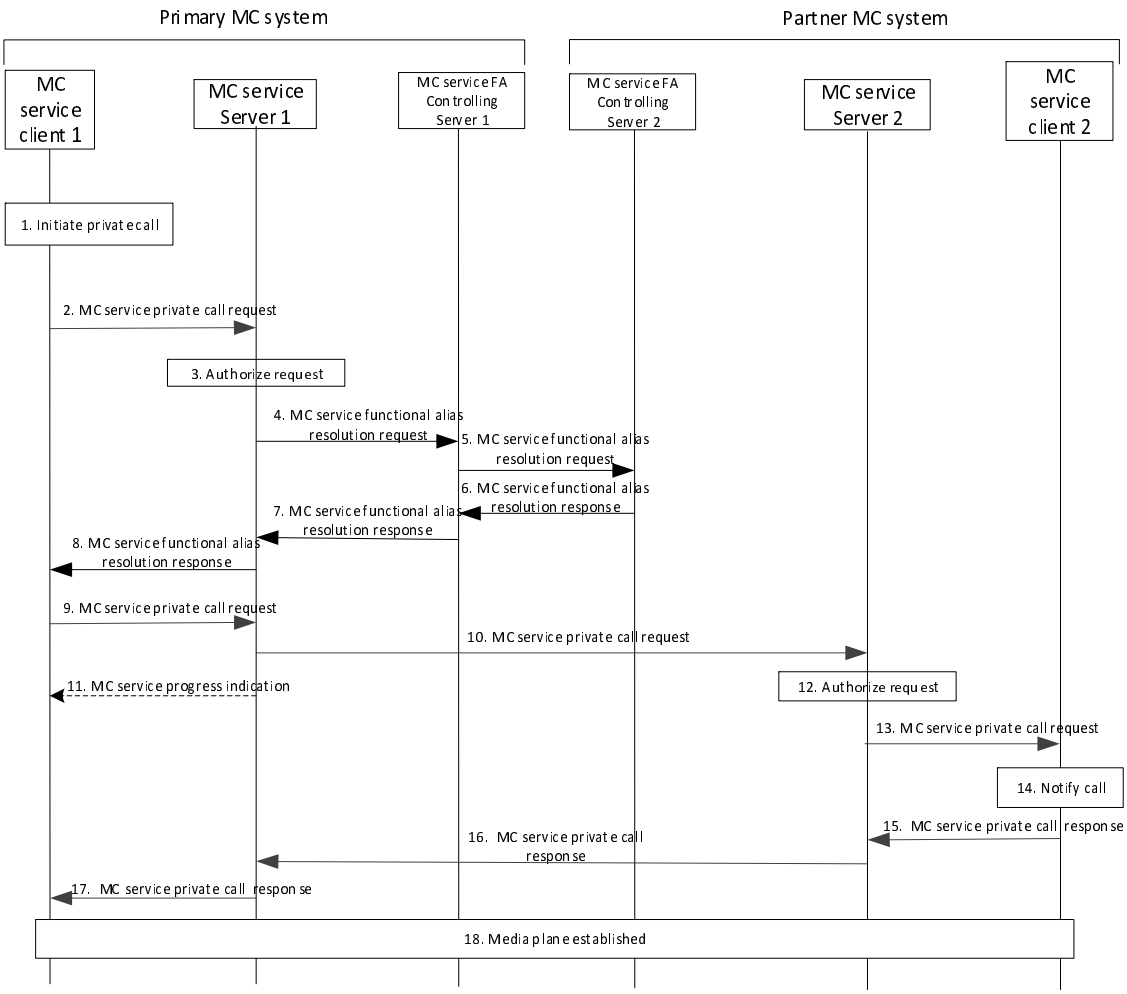

Figure 10.16.3.3-1: Private call setup in automatic commencement mode, users in multiple MC systems

1-2. Same as in 3GPP TS 23.379 [16] clause 10.7.2.2.3.1, 3GPP TS 23.281 [12] clause 7.2.2.3.1 or corresponding procedures in 3GPP TS 23.282 [13], but MC service private call request contains a functional alias of invited user.

3. If the MC service private call request contains a functional alias instead of an MC service ID as called party, the MC service server checks whether MC service client 1 can use the functional alias to setup a private call. If authorized, the MC service server 1 resolves the functional alias to the corresponding MC service ID for which the functional alias is active by using subsequent steps 4-7.

4. The MC service server 1 sends an MC service functional alias resolution request message to the MC service functional alias controlling server 1 to resolve the functional alias of the called party.

5. The MC service functional alias controlling server 1 determines that the functional alias belongs to the partner MC system and forwards the MC service functional alias resolution request message to MC service functional alias controlling server 2.

6. The MC service functional alias controlling server 2 resolves the functional alias and determines the corresponding MC service ID to terminate the call and returns it to the MC service functional alias controlling server 1 in the MC service functional alias resolution response message.

NOTE: Depending on implementation the MC service server can apply additional call restrictions and decide whether the call is allowed to proceed with the resolved MC service ID(s) (e.g., whether the MC service ID is within the allowed area of the functional alias). If the MC service server detects that the functional alias used as the target of the private call request is simultaneously active for multiple MC service users, then the MC service server can proceed by selecting an appropriate MC service ID based on some selection criteria. The selection of an appropriate MC service ID is left to implementation. This selection criteria can include rejection of the call, if no suitable MC service ID is selected.

7. The MC service functional alias controlling server 1 returns the corresponding MC service ID to MC service server 1 in the MC service functional alias resolution response message. The MC service server 1 checks if MC service user at MC service client 1 is authorized to initiate the private call to the MC service user at MC service client 2. If not authorized stop the procedure, otherwise continue with step 8.

8. The MC service server 1 responds with a MC service functional alias resolution response message that contains the resolved MC service ID back to MC service client 1.

9. The MC service client 1 sends a new MC service private call request towards the resolved MC service ID according 3GPP TS 23.379 [16] clause 10.7.2.2.3.1, 3GPP TS 23.281 [12] clause 7.2.2.3.1 or corresponding procedures in 3GPP TS 23.282 [13].

10-14. Same as in 3GPP TS 23.379 [16] clause 10.7.2.2.3.1, 3GPP TS 23.281 [12] clause 7.2.2.3.1 or 3GPP TS 23.282 [13] clause 7.14.2.2.

15. The receiving MC service client 2 accepts the private call automatically, and an acknowledgement is sent to the MC service server 2.

16. The MC service server 2 forwards the MC service private call response message to MC service server 1.

17-18. Same as in 3GPP TS 23.379 [16] clause 10.7.2.2.3.1, 3GPP TS 23.281 [12] clause 7.2.2.3.1 or corresponding procedures in 3GPP TS 23.282 [13].

10.16.4 Migration during an onging private communication

10.16.4.1 General

This subclause provides a generic guidance on the behaviour an MC service client follows to perform migration during an ongoing private communication, e.g., MCPTT private call. Once the MC service client detects the need to migrate during an ongoing private communication, it may initiate preparations and UE configuration which facilitate migration as mentioned in clause 10.1.1.2. The described procedure is applicable to the scenarios whether an MC service client is migrating into its primary MC system or a partner MC system.

10.16.4.2 Procedure

Figure 10.16.4.2-1 represents a generic procedure to be followed when migration is needed to be done during an ongoing private communication, such as MCPTT private call, or MCVideo private call.

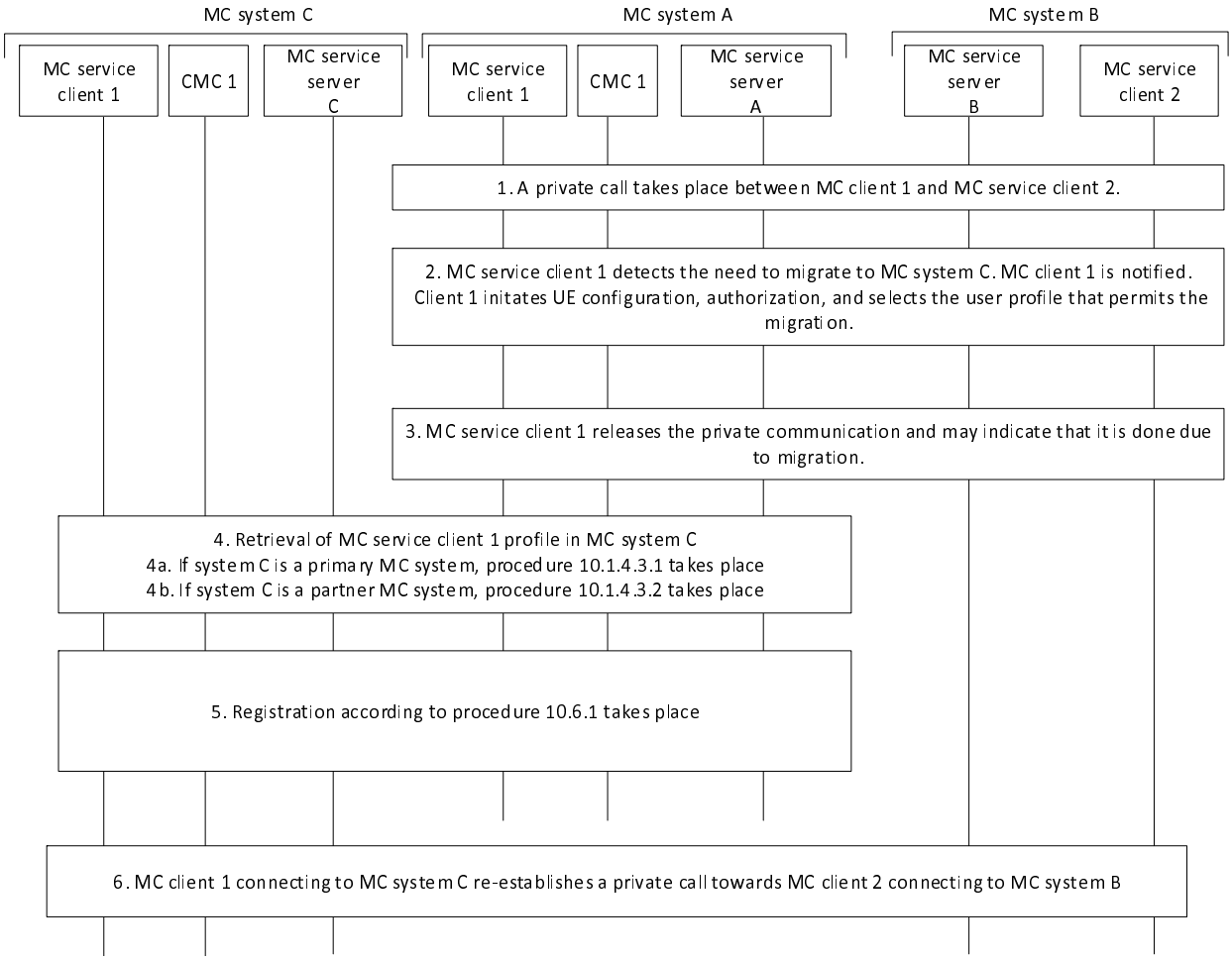

Figure 10.16.4.2-1: Migration during ongoing private communication.

1. A private call takes place between MC service client 1 and MC service client 2, where the former is connected to MC system A and the latter to MC system B.

2. The MC service client 1 detects the need to migration into MC system C and MC service server 1 is notified to be prepared for possible service interruption. Furthermore, upon detection, MC service client 1 performs initial steps to be considered prior migration, e.g., UE configuration, authorization, and selection of user profile that permits migration, as described in clause 10.1.1.2

3. MC service client 1 releases the private communication towards the MC service client 2 as described in clause 10.7.2.2.3.1 of 3GPP TS 23.379 [16] for MCPTT private call, or in clause 7.2.2.3.3.1 of 3GPP TS 23.281 [12] for MCVideo private call. A call release reason IE "release due to migration" may be included so that MC service client 2 is informed.

4. Migration takes place and MC system C retrieves MC service client 1 profile:

   4a. if MC system C is the primary MC system, retrieval of MC service client 1 profile takes place according to clause 10.1.4.3.1.

   4b. if MC system C is a partner MC system, retrieval of MC service client 1 profile takes place according to clause 10.1.4.3.2.

5. Registration according to procedure in clause 10.6.1 takes place.

6. MC service client 1 initiates a new private communication toward MC service client 2 as described in clause 10.7.2.2.1 of 3GPP TS 23.379 [16] for MCPTT private call, or in clause 7.2.2.3.1 of 3GPP TS 23.281 [12] for MCVideo private call.

10.16.5 Generic private call procedure towards a migrated MC service user

10.16.5.1 General

This subclause describes a generic private communication procedure towards a migrated MC service user at a partner MC system. This generic private communication can be an MCPTT private call, an MCVideo private call, or a one-to-one MCData communication. For the generic private call, this procedure is used in conjunction with the corresponding MCPTT, MCVideo and MCData procedures described in 3GPP TS 23.379 [16], 3GPP TS 23.281 [12], or 3GPP TS 23.282 [13], respectively.

Once an MC service user is migrated, he or she will be assigned a new MC service ID by the migrated MC system and this MC service ID will be used for all his/her communications. When another MC service user communicates with the migrated MC service user using the newly assigned MC service ID, the private call request described in clause 10.7.2.1.1 in 3GPP TS 23.379 [16], in clause 7.2.2.2.1 in 3GPP TS.23.281 [12], or the corresponding procedures in 3GPP TS 23.282 [13] applies.

For callers that are not aware of the migrated MC service user`s new MC service ID, the migrated MC service user is also reachable by his/her MC service ID assigned by the primary MC system via redirection done by the primary MC system`s MC service server described in this procedure.

10.16.5.2 Private call redirection

Table 10.16.5.2-1 describes the information flow of a private call redirection, which is sent from the MC service server to an MC service client initiating a private call towards a migrated MC service user.

Table 10.16.5.2-1: Private call redirection

Information element	Status	Description
MC service ID	M	The MC service ID of the MC service user initiating a private call, i.e., calling party. The MC service ID can either be MCPTT ID, MCVideo ID, or MCData ID.
MC service ID	M	The MC service ID of the target MC service user (i.e., called party), which the MC service user has obtained from its primary MC system before migration. The MC service ID can either be MCPTT ID, MCVideo ID, or MCData ID.
MC service ID	M	The MC service ID of the target MC service user, which the MC service user has obtained from its migrated MC system after Migration. The MC service ID can either be MCPTT ID, MCVideo ID, or MCData ID.
KMS URI (NOTE)	O	The KMS URI associated with the MC service ID of the migrated MC service user.
Redirection reason	O	The MC service server informs the calling party that the target MC service user has migrated.
NOTE: If the KMS URI is not configured in the MC service user profile and is not included in the private call redirection messange, then the MC service client shall obtain KMS URI using the KMS lookup procedure defined in 3GPP TS 33.180 [19].		

10.16.5.3 Procedure

Figure 10.16.5.4-1 presents a generic private communication procedure from MC service user 1 towards a migrated MC service user 2 where the MC system A is the primary MC system of MC service user 2 before migration, and the MC system B is the MC system that the MC service user 2 has migrated

Pre-conditions:

- MC system A and MC system B are interconnected.
- MC system A is the primary MC system of MC service user 2 before migration. MC system B is the MC system that MC service user 2 has migrated.

- The MC service server A is aware that MC service user 2 has migrated and is informed of its MC service ID provided by MC system B, as described in clause 10.6.3.3.

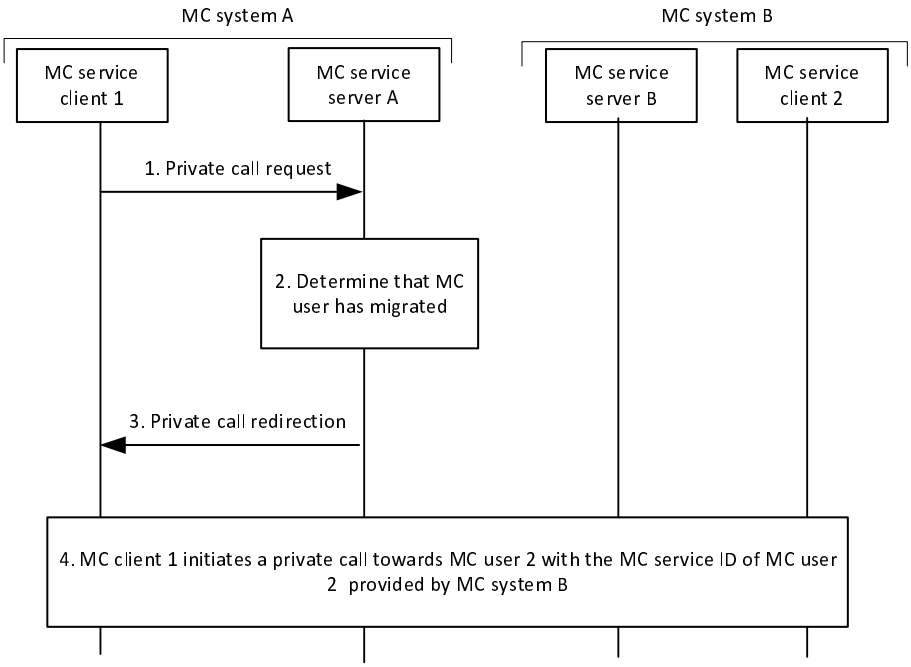

Figure 10.16.5.3-1: MC private call towards a migrated MC service user.

1. The MC service client 1 initiates a private call request towards MC service user 2 (MC service client 2) who has migrated to MC system B. The private call request includes among others the MC service ID of MC service user 2, which is provided by its primary MC system, as the target, i.e., called party. The private call request is described in clause 10.7.2.1.1 in 3GPP TS 23.379 [16], in clause 7.2.2.2.1 in 3GPP TS 23.281 [12], or the corresponding procedures in 3GPP TS 23.282 [13].

   If the private call request contains a functional alias instead of an MC service ID as the target party, the MC service server A checks whether the MC service user 1 at the MC service client 1 is allowed to use functional alias during private call setup.

2. MC service server A checks that MC service user 2 has migrated to MC system B with a new MC service ID assigned by MC system B.

   If the private call request contains a functional alias, and if the MC service user 1 at the MC service client 1 is authorized, the MC service server A resolves the functional alias to a corresponding MC service ID of the MC service user which has activated the functional alias. If the MC service server A determines that the corresponding MC service user of the resolved MC service ID is migrated, i.e., MC service user 2 at MC service client 2 is migrated, it checks whether the resolved MC service ID of the MC service user 2 is allowed to receive a private call from the MC service ID of the MC service user 1 using functional alias based on entries in the user profile of the MC service user 2 assigned by the primary system.

3. The MC service server A sends a private call redirection towards the MC service client 1, to inform MC service user 1 that the target MC service user, i.e., MC service user 2 has migrated and its new MC service ID of MC service user 2 assigned by the migrated MC system. The MC service client 1 releases the private call request at step 1.

4. The MC service client 1 initiates a private call towards MC service user 2, including the MC service ID of MC service user 2 obtained from MC system. The initiated private call can either be an MCPTT private call, an MCVideo private call, or a corresponding one-to-one MCData communication, and shall perform the procedures as described in 3GPP TS 23.379 [16], 3GPP TS 23.281 [12], or 3GPP TS 23.282 [13], respectively.

NOTE: If end-to-end encryption is required, the migrated MC service user 2 is assumed to have the necessary security information needed to establish a protected call, as defined in 3GPP TS 33.180 [25].

11 MC gateway UE

11.1 General

An MC gateway UE enables MC service access for a MC service user residing on non-3GPP devices which may or may not have the ability to host MC service clients. In order to be able to participate in a MC service, the MC gateway UE provides the following necessary functions to enable the MC service access for such MC clients:

- **3GPP transport resources**: Sharing of MC gateway UE 3GPP transport resources among the associated MC service clients.
- **MC client identification**: Independent MC service client identification, MC service client authorisation and MC service profile association.
- **MC client communication integrity**: Ensure that signalling, media content and traffic attributes, e.g. priority and QoS, of communications between the MC system and MC service client remains unaltered.
- **Transparent MC traffic forwarding**: The MC gateway UE forwards MC traffic without altering the content to the non-3GPP device whether it hosts or does not host an MC client. For the case the MC client is hosted at the non-3GPP device, the MC gateway UE forwards:
  - the signalling between the MC client in the non-3GPP device and the MC service server/ CSC server
  - the signalling between the user agent in the non-3GPP device and the SIP core
  - the signalling between the HTTP client in the non-3GPP device and the HTTP proxy
  - the media between the MC service server and the MC client in the non-3GPP device

NOTE 1: The traffic exchange between the non-3GPP device and the MC gateway UE is implementation specific.

NOTE 2: Information related to MC gateway UE routing capabilities is found in Annex E.

NOTE 3: Information about MC gateway UE selection are summarized in Annex D.

11.2 Functional Model

11.2.0 General

The MC gateway UE offers access to the MC server for several MC clients as shown in Figure 11.2.0-1. The MC clients can be either located in the MC gateway UE or in the non-3GPP devices connected to the MC gateway UE via non-3GPP access. The configuration data defined in Annex A is needed in the MC client and the UE that is hosting the MC clients, i.e., either non-3GPP device or MC gateway UE, to access the MC service.

For non-3GPP devices which can host an MC client, the MC gateway UE enables connectivity to the MC server. For non-3GPP devices which cannot host the MC client, the MC gateway UE hosts the instantiation of the MC client on behalf of the non-3GPP device.

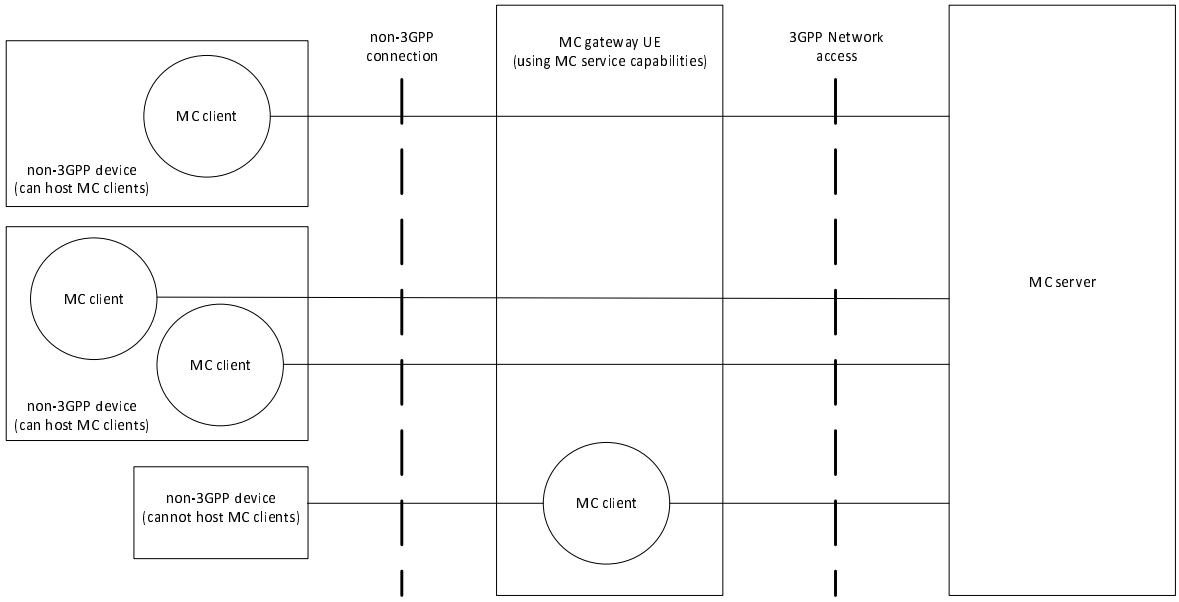

Figure 11.2.0-1: Functional architecture

The MC gateway UE obtains MC service access via 3GPP network using the procedures as defined in 3GPP TS 33.180 [25].

The non-3GPP connection between the non-3GPP device and the MC gateway UE is out of scope of 3GPP.

For non-3GPP devices which cannot host MC clients, the MC gateway UE instantiates an MC client, acting on behalf of the non-3GPP device, to provide the requested services (e.g. emergency call, group calls, short data messages services, etc.). The communication interworking and the definition of associated procedures between the MC client (initiated at the MC gateway UE) and the non-3GPP devices is out of scope of this document.

For non-3GPP devices that host MC clients, MC service access is through the MC gateway UE. The MC gateway UE forwards (unmodified) signalling and media from the individual MC clients to the MC server and vice versa.

If the MC service user on the non-3GPP device utilizes multiple MC services simultaneously, the MC service access may also be provided via one or multiple MC gateway UEs as shown in figure 11.2.0-2. In this case, each MC service is restricted to one MC gateway UE (e.g. MCPTT via MC gateway UE1, MCData via MC gateway UE2).

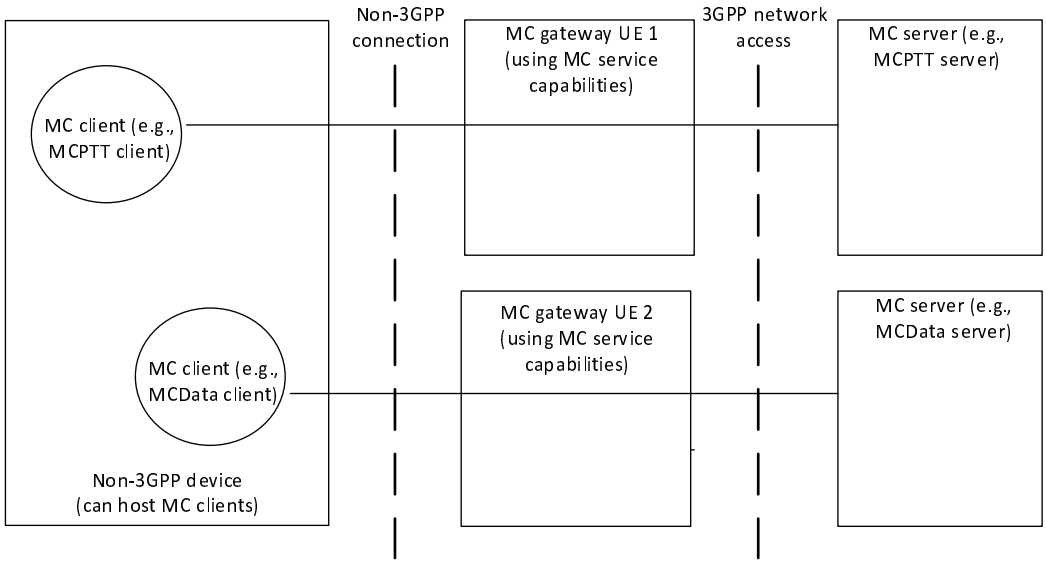

Figure 11.2.0-2: Simultaneous multiple MC gateway UE use by a single non-3GPP device

NOTE 2: Although not shown in the above figure, the same principle of simultaneous use of multiple MC gateway UEs is applied for non-3GPP devices which cannot host an MC client.

11.2.1 Functional model

The authentication and authorisation of the MC clients hosted on the MC gateway UE follows the procedures described in 3GPP TS 33.180 [25]. Upon successful authentication and authorisation the MC clients can access a MC server via an MC gateway UE.

The MC gateway UE supports the authentication and authorisation of the MC client residing at the non-3GPP device by forwarding the unmodified application layer signalling between the MC client and the corresponding MC server. The authentication and authorisation of the MC client in the non-3GPP device follows the procedures described in 3GPP TS 33.180 [25].

NOTE: The authentication and authorisation between the MC gateway UE and the non-3GPP device is out of scope of 3GPP.

Figure 11.2.1-1 represents the functional model for the application plane for utilizing MC gateway UE to enable MC services to non-3GPP devices that can host an MC client.

Figure 11.2.1-2 represents the functional model for the signalling plane for utilizing MC gateway UE to enable MC services to non-3GPP devices that can host an MC client.

Figure 11.2.1-3 represents the functional model for the application plane for non-3GPP devices that cannot host an MC client.

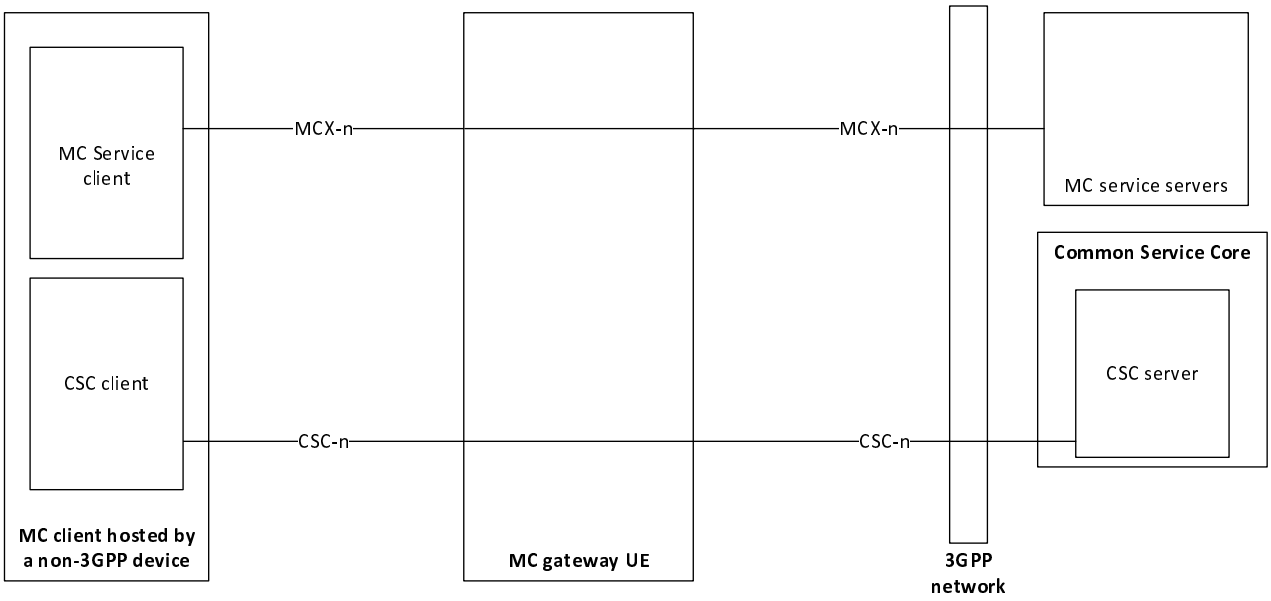

Figure 11.2.1-1: Functional model of MC gateway UE application plane with MC client hosted in the non- 3GPP device

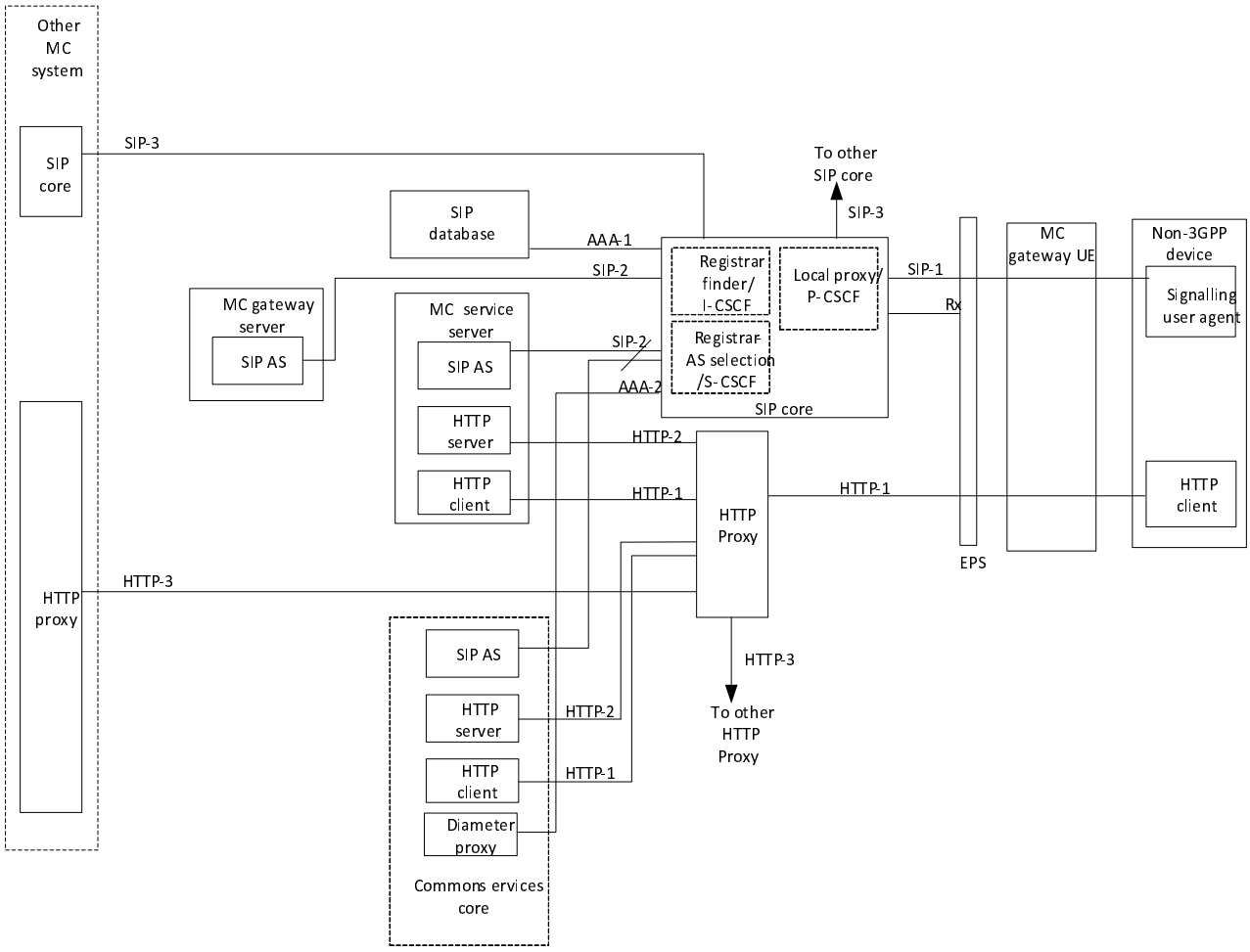

Figure 11.2.1-2: Functional model of MC gateway UE signalling plane with MC client hosted in the non- 3GPP device

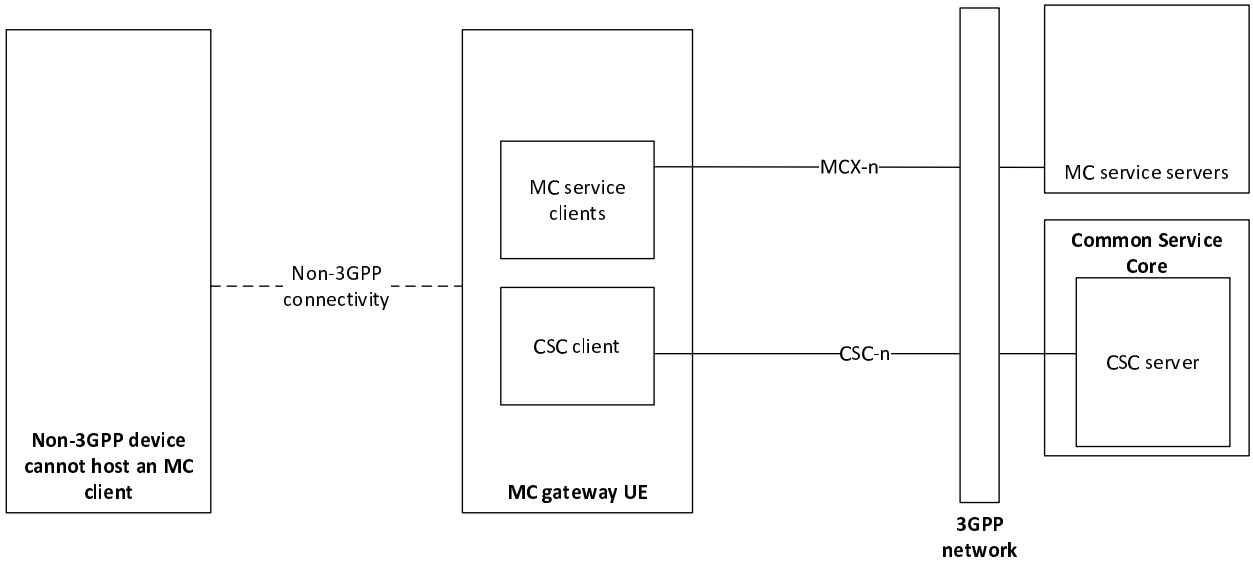

Figure 11.2.1-3: Functional model of MC gateway UE application plane with MC client hosted in the MC gateway UE

The functional model for the signalling control plane as described in figure 7.3.1-2 is applicable to figure 11.2.1-3.

11.2.2 Reference points

11.2.2.1 General

The reference points for the use of the MC gateway UE are described in the following subclauses.

11.2.2.2 Void

11.2.2.3 Void

11.2.2.4 Reference points MCX-n, CSC-n, SIP-1 and HTTP-1

The reference points MCX-n and CSC-n belonging to the application plane, and the reference points SIP-1 and HTTP-1 belonging to the signalling control plane, are relayed by the MC gateway UE between MC client on the non-3GPP device and the corresponding MC service server.

MCX-n, CSC-n, SIP-1 and HTTP-1 reference points are specified in the present specification. The MCX-n reference points are specified in 3GPP TS 23.379 [16], 3GPP TS 23.281 [12] and 3GPP TS 23.282 [13].

NOTE: The MCPTT-8, MCPTT-9, MCVideo-8, MCVideo-9, MCData-FD-5 are not included within MCX-n.

11.2.3 Void

11.3 Using identities behind the MC gateway UE

11.3.1 General

The MC gateway UE enables access to the MC system for MC clients either hosted on the MC gateway UE or hosted on non-3GPP devices. MC clients hosted in a non-3GPP device utilize MC service identities that are transparently passed through the MC gateway UE. This is further illustrated in subclause 11.3.2.

MC clients hosted in MC gateway UE also utilize unique MC service identities and share one common IMS subscription that is unique for MC gateway UE. This is further illustrated in subclause 11.3.3.

11.3.2 When using separate IMS subscriptions

NOTE: The content of this clause is out of scope of the present document.

11.3.3 When sharing MC gateway UE's IMS subscription

The MC clients, instantiated at the MC gateway UE on behalf of the non-3GPP devices which cannot host an MC client, rely on the IMS subscription provided by the MC gateway UE. In this case, the MC clients instantiated at the MC gateway UE share the credentials from the IMS subscription of the MC gateway UE, as shown in Figure 11.3.3-1.

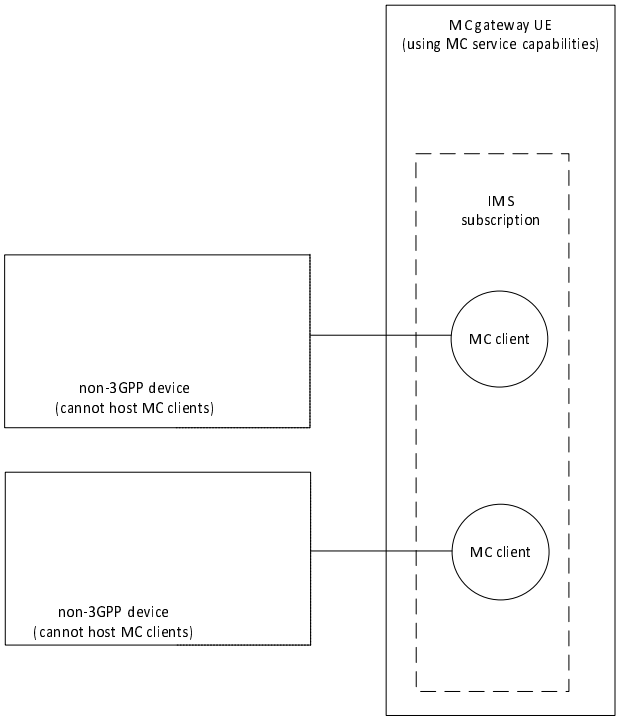

Figure 11.3.3-1: Sharing MC gateway UE's IMC for non-3GPP devices which cannot host a client

11.4 Void

11.5 Procedures and information flows

11.5.1 Void

11.5.2 Void

11.5.3 Void

11.5.4 Void

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];
- MCData user profile configuration data is specified in 3GPP TS 23.282 [13]; and
- Location user profile configuration data is specified in clause A.8.

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) (see NOTE 8)			
[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-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
[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-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
[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
[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
Subclause 10.6.2.9 of 3GPP TS 23.379 [16]	Group is a preconfigured regroup group	Y	Y	Y
[R-5.2.1-002] of 3GPP TS 22.280 [3]	Group is a broadcast group	Y	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].
NOTE 8: The list of group members comprises all group members in primary and in partner MC systems of the MC service group.

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]	List of authorised users who can request the list of members of an MC service group	Y	Y	Y
	> MCPTT IDs			Y
	> MCVideo IDs			Y
	> MCData IDs			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
Subclause 5.2.9 of 3GPP TS 23.280 [16	List of partner MC systems from which interconnection is permitted for the group			
Subclause 5.2.9 of 3GPP TS 23.280 [16	> Identity of partner MCPTT system		Y	Y
Subclause 5.2.9 of 3GPP TS 23.280 [16	> Identity of partner MCVideo system		Y	Y
Subclause 5.2.9 of 3GPP TS 23.280 [16	> Identity of partner MCData system		Y	Y
[R-6.4.4-003] of 3GPP TS 22.280 [16]	List of functional aliases which prevents de-affiliating			
	> Functional alias	N	Y	Y
[R-6.4.4-004] of 3GPP TS 22.280 [16]	List of functional aliases which prevents de-affiliating, if only one user has bound the functional alias to the group			
	> Functional alias	N	Y	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 (also known as KMSUri for security domain managed by KMS)
	> Indication of whether the UE shall use Ipv4 or Ipv6 for on-network MCPTT
	> MCPTT Server
	>> Server URI
	> Indication of whether the UE shall use Ipv4 or Ipv6 for on-network MCData
	> MCData Server
	>> Server URI
	> Indication of whether the UE shall use Ipv4 or Ipv6 for on-network MCVideo
	> MCVideo Server
	>> Server URI
	> Location management server
	>> Server URI
Subclause 10.1.1	Operational information
	> MC service UE label (see NOTE)
NOTE: The MC service label is optional.	

A.7 Void

A.8 Location user profile configuration data

The location user profile configuration data is stored in the location user database. The location management server obtains the location user profile configuration data via the configuration management server (CSC-24).

Table A.8-1 contains the location user profile configuration required to support the use of on-network location service. Data in table A.8-1 can be configured offline using the CSC-11 reference point.

Table A.8-1: location user profile data (on and off network)

Reference	Parameter description	Location UE	Location Server	Configuration management server	Location user database
[R-5.11-007] of 3GPP TS 22.280 [3] Clause 10.9.3.3	Authorization to set a trigger at a LMC				
	> List of MC service IDs for which a trigger is authorized to be set	Y	Y	Y	Y
	>> MCPTT ID (see NOTE 1)	Y	Y	Y	Y
	>> MCVideo ID (see NOTE 1)	Y	Y	Y	Y
	>> MCData ID (see NOTE 1)	Y	Y	Y	Y
[R-5.11-008] of 3GPP TS 22.280 [3]	Authorization to cancel a trigger at a LMC				
	> List of MC service IDs for which a trigger is authorized to be cancelled	Y	Y	Y	Y
	>> MCPTT ID (see NOTE 1)	Y	Y	Y	Y
	>> MCVideo ID (see NOTE 1)	Y	Y	Y	Y
	>> MCData ID (see NOTE 1)	Y	Y	Y	Y
Clause 10.9.3.5 Clause 10.9.3.7	Authorization to subscribe to location information for an MC user				
	> List of MC service IDs for which subscription and subscription cancellation is authorized	Y	Y	Y	Y
	>> MCPTT ID (see NOTE 1)	Y	Y	Y	Y
	>> MCVideo ID (see NOTE 1)	Y	Y	Y	Y
	>> MCData ID (see NOTE 1)	Y	Y	Y	Y
Clause 10.9.3.6.2 Clause 10.9.3.7	Authorization to obtain location information for an MC user				
	> List of MC service IDs for which obtaining location information is authorized	Y	Y	Y	Y
	>> MCPTT ID (see NOTE 1)	Y	Y	Y	Y
	>> MCVideo ID (see NOTE 1)	Y	Y	Y	Y
	>> MCData ID (see NOTE 1)	Y	Y	Y	Y
Clause 10.9.3.10.6 Clause 10.9.3.11	Authorization to modify the location user profile of an MC user				
	> Modification to the location user profile is permanent/temporary	Y	N	Y	Y
	>> Duration of time for temporary modification	Y	N	Y	Y
	> List of MC service IDs for which modifying the location reporting configuration is authorized	Y	N	Y	Y
	>> MCPTT ID (see NOTE 1)	Y	N	Y	Y
	>> MCVideo ID (see NOTE 1)	Y	N	Y	Y
	>> MCData ID (see NOTE 1)	Y	N	Y	Y

NOTE 1: There can be zero or more.
NOTE 2: The default authorization applies to all MC users not listed as specifically authorized or not authorized. The intent of this parameter is to avoid having to list all MC users as specifically authorized or not authorized and allowing the administrator to only indicate specific authorization statuses.

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.

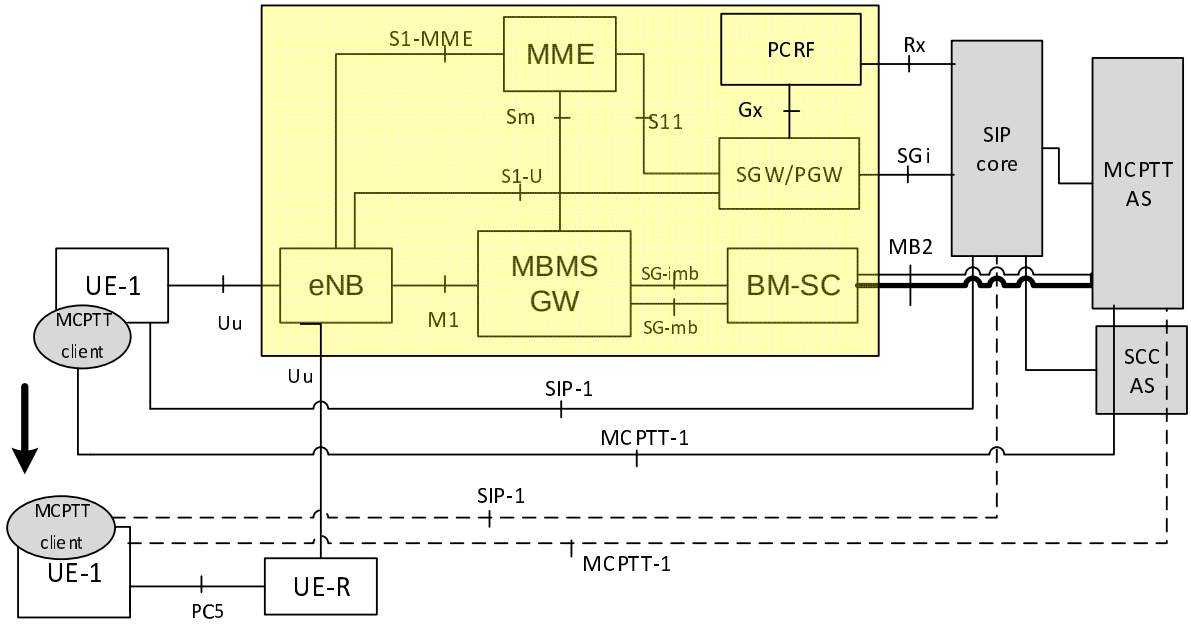

Figure B.1-1: Service continuity from on-network to UE-to-network relay

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.

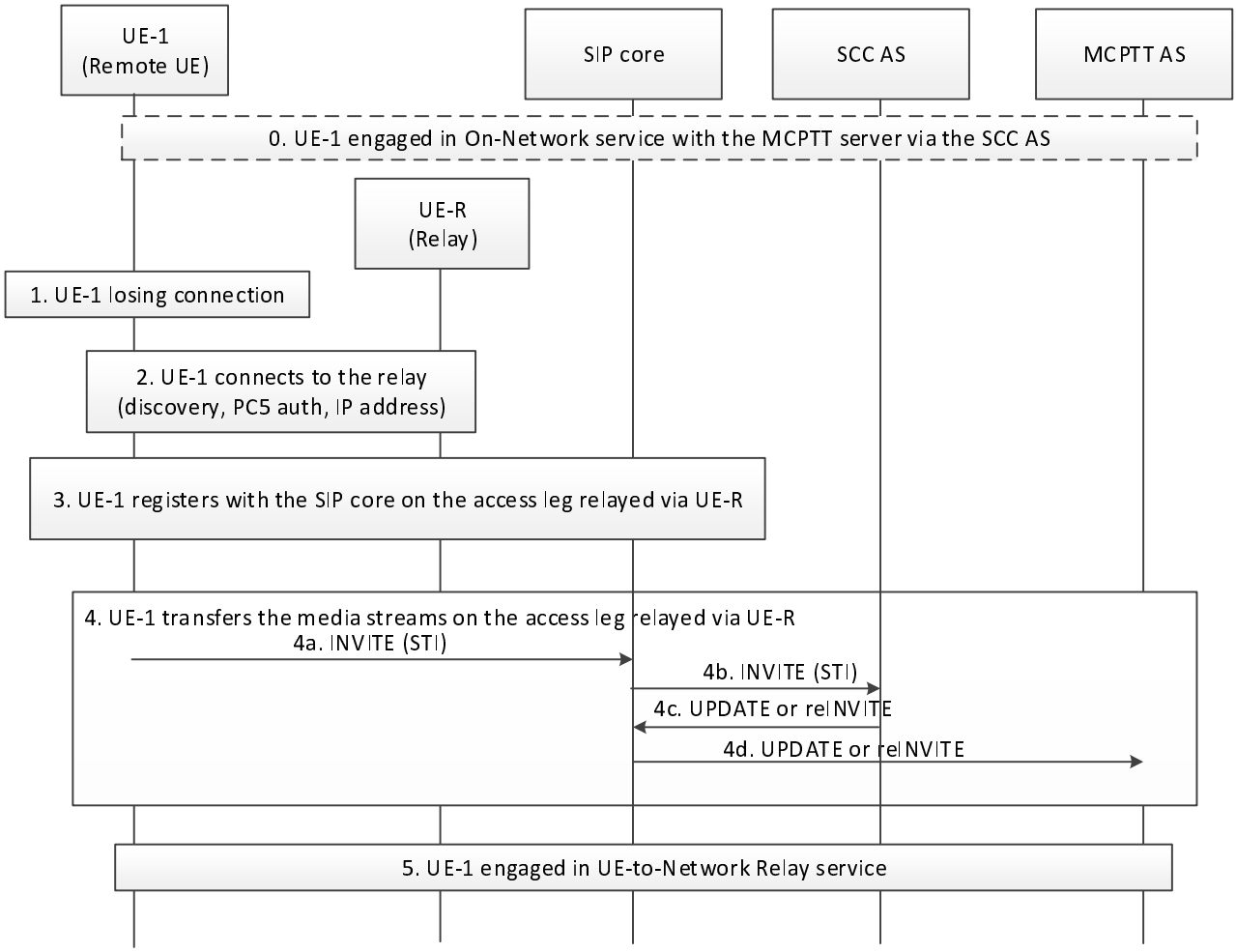

Figure B.1-2 Service continuity when UE switches from on-network MCPTT service to UE-to-network relay MCPTT service

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): Application Priority

C.1 Use of application priorities

Different communications between two or more MC service users need to be distinguished in their urgency in order to appropriately or less preferably allocate 3GPP system transport resources. Also simultaneous incoming communications to a MC service user requires an indication of the urgency in order to preferentially join the communication in accordance with the urgency.

To make this distinction of urgencies, the MC system necessarily supports different types of priorities and corresponding levels within each priority category representing the relative importance of a request at the application level. The use of application priority allows the MC system to decide whether a communication establishment or modification request can be accepted or needs to be rejected (e.g. in case of transport resource limitations), or it allows the MC service client to rank simultaneous incoming communication for presentation to an MC service user. Hence the application priority can also be used to decide which existing transport resources (e.g. bearers) to pre-empt during resource limitations. Such pre-emption capability information defines whether a communication can obtain transport resources that were already assigned to another communication with a lower priority level. The pre-emption vulnerability information defines whether a communication can lose the resources assigned to it in order to admit a communication with higher priority level.

The following types of application priorities are provided by the MC system:

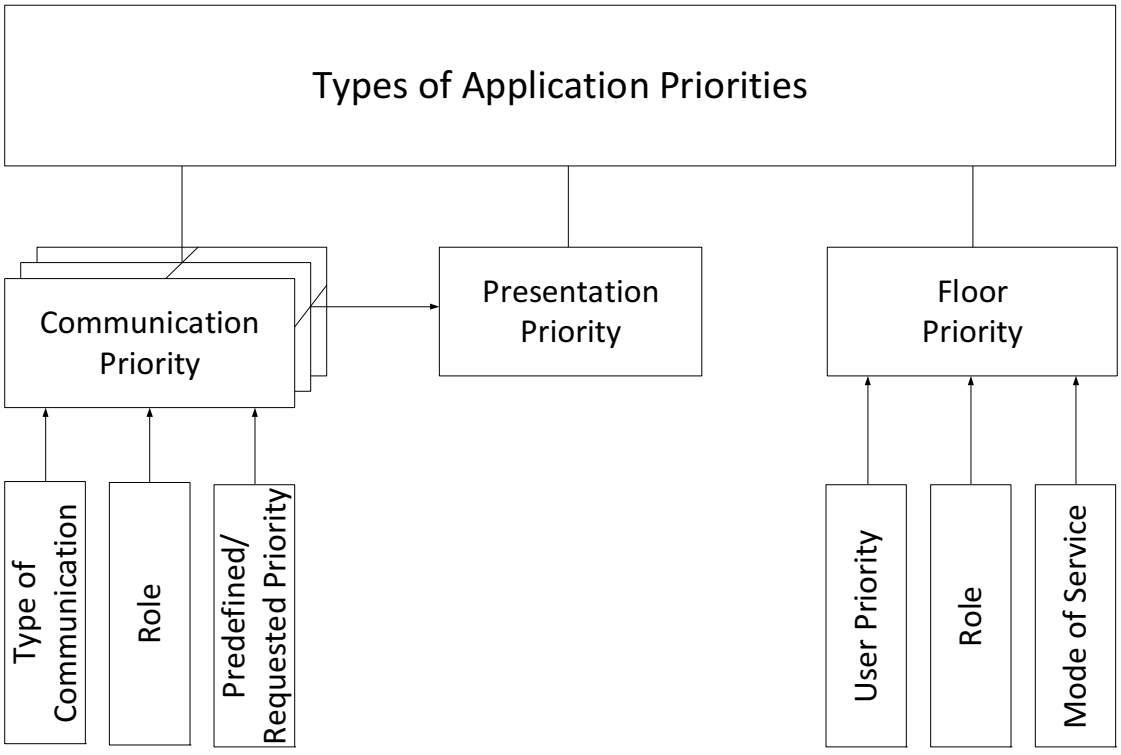

Figure C.1.-1: Types of application priorities in the MC system

Communication priority involves a combination of the type of call/communication, the role of the requesting MC service user, and the predefined/requested priority of the initiating MC service user and/or group.

Presentation priority involves the determination of which communications, from within multiple simultaneous possible, are the highest priority to present to the MC service user either audibly or visibly. An example would be a private call received at the same time as an emergency call on a monitored group. This category can be configured uniquely for each MC service user.

Floor priority involves the determination of who can transmit within a communication at a particular time. This is essentially the priority of the MC service user according to its profile, and possibly modified by its role and/or mode of service (e.g. using emergency or imminent peril call). This category is used, for example, to determine the ordering of the floor control queue within an established communication.

Annex D (informative): Considerations for MC gateway UE selection

D.1 General

Operating conditions can influence the selection and the use of the MC gateway UE.

Multiple conditions can be considered by the non-3GPP device either to connect to another MC gateway UE (e.g. with better operating conditions for the requested service), or to re-connect to the same MC gateway UE (e.g. reattempt connection after a certain time).

D.2 Potential operating conditions

Possible operating conditions information could belong to one of the following categories:

MC gateway UE capacity limits

The MC gateway UE might not be able to allow non-3GPP devices to connect when the limit of connected MC clients has been reached.

3GPP access congestion

The MC gateway UE can make use of to the special Categories/Access Identity, the preferential access applies based on its assigned Access Control Class/Access Identity during periods of congestion. The MC gateway UE subscription allows to obtain priority treatment for the required communication.

Nevertheless, the serving access network can indicate to the UEs (including MC gateway UE) that Access Class Barring applies and this can be passed by the MC gateway UE to the non-3GPP device.

PLMN reselection

PLMN reselection depends on operator policy, roaming agreements, and on national/regional regulatory requirements.

Network status information

If the network status information of an EPS/5GS capability available at MC gateway UE, it can be further propagated to the corresponding non-3GPP devices for further processing (e.g., if the requested QoS for service can be provided for MC client or not).

Annex E (informative): MC gateway UE routing capabilities

E.1 General

The use of the MC gateway UE requires the support of an IP network behind the MC gateway UE, that a range of IP addresses are reachable over a single MC gateway UE. That enables the forwarding of signalling information and media plane between non-3GPP devices and MC server by the MC gateway UE.

E.2 MC client IP address association

The use of a unique IP address by the MC clients shall be ensured for the period of association of the MC clients via the MC gateway UE with the IMS/SIP core and the MC server. Each MC gateway UE requires a unique IP address range for their MC client association which is known by the MC service environment and a correlation between the MC client's IP address and the MC gateway UE's IP address exists.

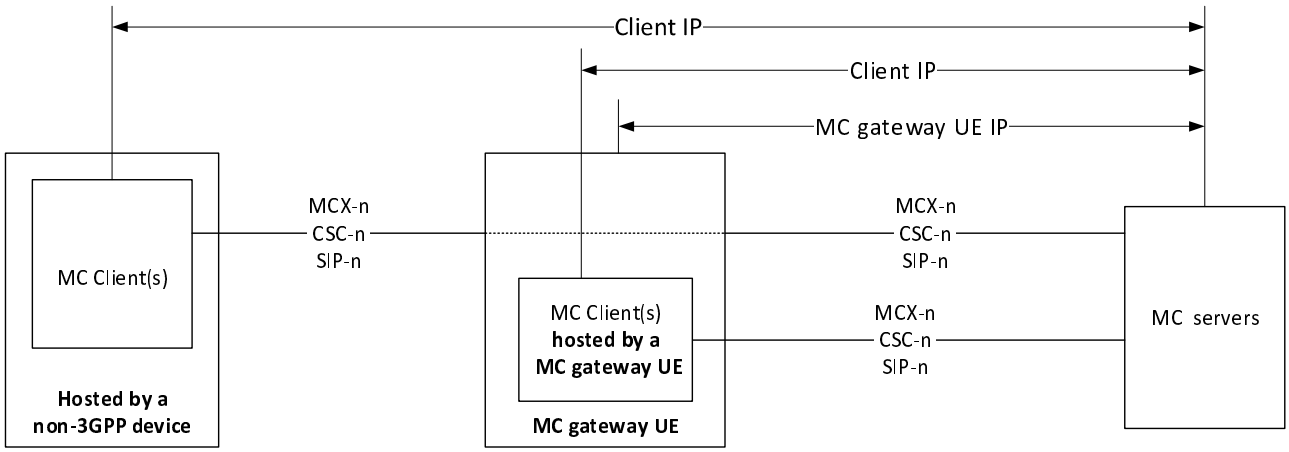

Figure E.2-1: MC client IP address relationship

Framed routing in accordance with IETF RFC 2865 [32], IETF RFC 3162 [33], 3GPP TS 23.501 [34] shall be used to enable the support of an IP network behind the MC gateway UE, such that a range of IP addresses is reachable over a single 3GPP transport session. It allows the routing of packets to IP addresses that do not belong to the PDN/PDU session of the MC gateway UE.

NOTE: The MC gateway UE can provide necessary IP address allocation to MC clients, e.g., as a DHCP relay agent in accordance with IETF RFC 1541 [35] and IETF RFC 8415 [36], or as a requesting router in accordance with IETF RFC 8415 [36] and 3GPP TS 23.401 [17] when using IPv6 prefix delegation.

E.3 IP address association using the MC gateway UE

If the MC client relies on IP address provided by the MC gateway UE, the MC gateway UE shall store the correlation between the non-3GPP device and the IP address (MC gateway UE IP and the local IP) used by the MC client . The procedures initiated by the MC client, i.e., SIP registration, user authentication and service authorisation use the MC gateway UE's IP address.

The MC gateway UE assigns the local IPs from address pool which it maintains to the individual MC clients. Managing the local IP addresses, re-using the local IP address, and how the traffic is routed between the MC clients and the network is left for implementation.

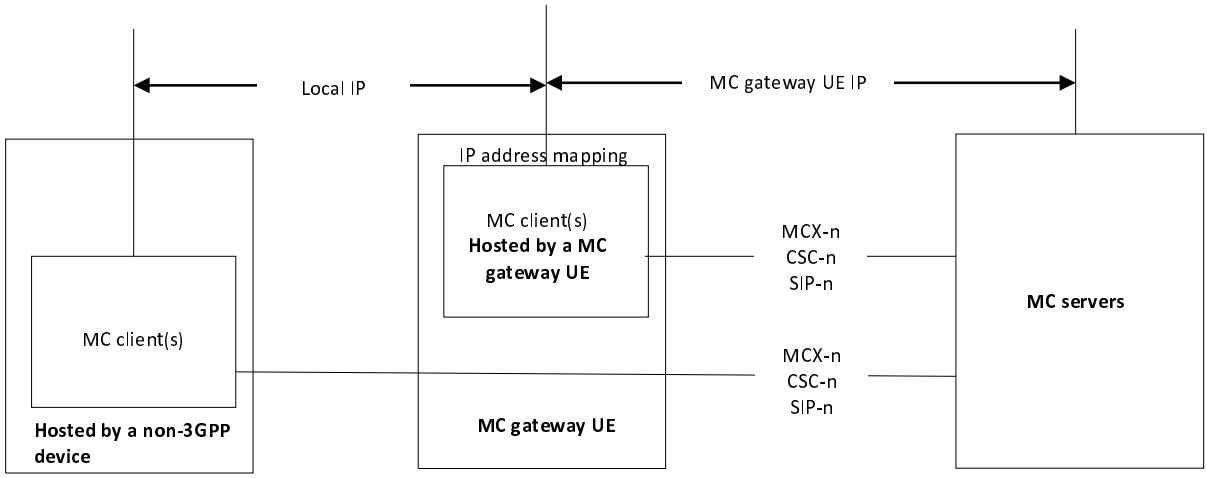

Figure E.3-1: Non-3GPP device uses MC gateway UE's IP address

Annex F (informative): Change history

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
2017-06	SA#76	SP-170396	0026	4	B	Introduction of MC server initiated group de-affiliation procedure	15.0.0
2017-06	SA#76	SP-170396	0052	1	B	Enhancement on group regrouping with an MC system	15.0.0
2017-06	SA#76	SP-170396	0053	3	B	MC server initiated group de-affiliation from group(s) in partner system	15.0.0
2017-06	SA#76	SP-170396	0059	2	B	Resource Management in CFA	15.0.0
2017-06	SA#76	SP-170397	0025	2	B	MBMS bearer event notification	15.0.0
2017-06	SA#76	SP-170397	0043	4	B	FEC for mission critical services	15.0.0
2017-06	SA#76	SP-170397	0058	1	B	Header compression for MC services over MBMS	15.0.0
2017-09	SA#77	SP-170679	0070	1	A	MC group configuration data correction	15.1.0
2017-09	SA#77	SP-170684	0073	2	B	Application plane functional model for interconnection	15.1.0
2017-09	SA#77	SP-170684	0074	1	B	Group configuration for interconnection	15.1.0
2017-09	SA#77	SP-170684	0075	2	B	User profile retrieval for migration	15.1.0
2017-09	SA#77	SP-170683	0076	2	B	Service type for group regroup	15.1.0
2017-09	SA#77	SP-170684	0077	2	C	Rules for temporary groups	15.1.0
2018-01	SA#78	SP-170895	0066	9	B	Retrieval of migration credentials for access to SIP core / IMS of a partner MC system	15.2.0
2018-01	SA#78	SP-170897	0070	2	A	MC group configuration data correction	15.2.0
2018-01	SA#78	SP-170893	0071	4	B	Priority between MC service servers	15.2.0
2018-01	SA#78	SP-170894	0072	3	C	Multi-server MBMS bearer coordination	15.2.0
2018-01	SA#78	SP-170895	0079	1	B	Architecture requirements for migration	15.2.0
2018-01	SA#78	SP-170895	0080	4	B	Signalling plane functional model for interconnection	15.2.0
2018-01	SA#78	SP-170895	0081	1	B	Architectural requirements for interconnection	15.2.0
2018-01	SA#78	SP-170895	0082	4	B	Addition of interconnection affiliation	15.2.0
2018-01	SA#78	SP-170897	0086	3	F	CR on clarification for MC service group ID	15.2.0
2018-01	SA#78	SP-170894	0088	1	F	CR on MBMS usage for group configuration	15.2.0
2018-01	SA#78	SP-170893	0091	1	B	Request for resources from MC service server	15.2.0
2018-01	SA#78	SP-170893	0092	2	B	Functional model update	15.2.0
2018-01	SA#78	SP-170893	0093	1	F	Location Server integration to PLMN	15.2.0
2018-01	SA#78	SP-170896	0094	1	B	Introduction of multi-talker control	15.2.0
2018-01	SA#78	SP-170896	0095	4	B	Introduction of Functional alias(es)	15.2.0
2018-01	SA#78	SP-170887	0096		D	CR to replace uneditable figures	15.2.0
2018-01	SA#78	SP-170897	0097	1	F	Renaming of "emergency condition"	15.2.0
2018-01	SA#78	SP-170895	0099	1	B	Network selection for EPC-level roaming to support migration	15.2.0
2018-01	SA#78	SP-170896	0105	2	C	Take over procedure for Functional alias(es)	15.2.0
2018-01	SA#78	SP-170896	0106	2	B	Functional alias controlling role of MC service server	15.2.0
2018-01	SA#78	SP-170893	0107	1	F	GMS selection during group regroup	15.2.0
2018-01	SA#78	SP-170893	0108	1	F	Correction of "Group creation confirmation response"	15.2.0
2018-01	SA#78	SP-170895	0110	1	B	Information flows for interconnection group configuration	15.2.0
2018-01	SA#78	SP-170895	0111	1	B	Interconnection call procedures	15.2.0
2018-01	SA#78	SP-170895	0112	2	B	Interconnection configuration enforcement	15.2.0
2018-01	SA#78	SP-170895	0113	1	B	Interconnection media replication	15.2.0
2018-01	SA#78	SP-170895	0114	1	B	Serving server and system definition	15.2.0
2018-01	SA#78	SP-170897	0115	2	F	Renaming of "MCService emergency state cancel"	15.2.0
2018-01	SA#78	SP-170893	0117	2	F	Addition to group configuration data	15.2.0
2018-01	SA#78	SP-170894	0118		F	Removal of Editor's note in the procedures for MBMS usage	15.2.0
2018-01	SA#78	SP-170887	0120	1	A	Add group deletion functionality	15.2.0
2018-01	SA#78	SP-170893	0122	2	B	Provision of group dynamic data	15.2.0
2018-01	SA#78	SP-170895	0123		B	Defintions of interconnection, migration and MC gateway server	15.2.0
2018-04	SA#79	SP-180154	0125	4	B	Signalling plane registration for MC UE migration	15.3.0
2018-04	SA#79	SP-180153	0127	2	C	Multi-server MBMS bearer coordination	15.3.0
2018-04	SA#79	SP-180145	0129	1	A	Correction of security specification references	15.3.0
2018-04	SA#79	SP-180154	0130		F	Correction of interconnection configuration enforcement figure	15.3.0
2018-04	SA#79	SP-180154	0131	1	B	Interconnection subscription to group configuration	15.3.0
2018-04	SA#79	SP-180154	0131	6	B	User authorization for interconnection and migration	15.3.0
2018-04	SA#79	SP-180154	0133	2	B	Group configuration for interconnection	15.3.0
2018-04	SA#79	SP-180145	0135	1	A	Aligning 10.9.3.1 procedure with diagram	15.3.0
2018-04	SA#79	SP-180149	0137	1	A	Update of references to stage 1 specifications	15.3.0
2018-04	SA#79	SP-180154	0138	2	B	Description of MC system identity	15.3.0
2018-04	SA#79	SP-180154	0139	2	B	Functional model update for interconnection	15.3.0

2018-04	SA#79	SP-180154	0140	1	B	Removal of editor's notes related to interconnection	15.3.0
2018-04	SA#79	SP-180154	0141	1	B	Service configuration for migration	15.3.0
2018-04	SA#79	SP-180154	0142	1	B	Update to connectivity for interconnection	15.3.0
2018-06	SA#80	SP-180371	0143	4	F	Correction of MC service system	15.4.0
2018-06	SA#80	SP-180364	0145	2	A	Clarification on MBMS bearer announcement	15.4.0
2018-06	SA#80	SP-180368	0146		F	Functional model corrections	15.4.0
2018-06	SA#80	SP-180368	0149	1	F	Handling of group configuration and group state over MBMS	15.4.0
2018-09	SA#81	SP-180676	0151	2	C	Multicast application level control signal clarification	16.0.0
2018-12	SA#82	SP-181171	0153	2	A	Editorial correction of figure in TS 23.280	16.1.0
2018-12	SA#82	SP-181172	0162	1	A	Removal of notes for FEC and ROHC	16.1.0
2018-12	SA#82	SP-181177	0165	4	C	Proposal for affiliation status information in group management server	16.1.0
2018-12	SA#82	SP-181177	0167		C	Spelling of ProSe	16.1.0
2018-12	SA#82	SP-181177	0169	2	F	Align UE configuration with TS 33.180	16.1.0
2018-12	SA#82	SP-181177	0171	1	B	Regroup group configuration	16.1.0
2018-12	SA#82	SP-181174	0172		A	Correcting title of a functional alias management subclause	16.1.0
2019-03	SA#83	SP-190073	0173	3	C	Improvement of the group creation request	16.2.0
2019-03	SA#83	SP-190073	0174	2	B	Broadcast group regroup	16.2.0
2019-03	SA#83	SP-190073	0178	1	B	Group status notification over MBMS	16.2.0
2019-03	SA#83	SP-190075	0179	1	F	Migration connectivity information	16.2.0
2019-03	SA#83	SP-190071	0180	-	A	Correction of emergency location triggering criteria	16.2.0
2019-03	SA#83	SP-190073	0181	4	B	MBMS listening status report	16.2.0
2019-06	SA#84	SP-190482	0184	1	A	Clarifications on functional alias controlling role	16.3.0
2019-06	SA#84	SP-190488	0185	3	B	Functional alias information query	16.3.0
2019-06	SA#84	SP-190484	0186	1	F	Add location management sever URI to initial MC service UE configuration	16.3.0
2019-06	SA#84	SP-190488	0187	4	F	Functional alias alternative addressing for MCX services	16.3.0
2019-06	SA#84	SP-190488	0188	1	B	Implicit functional alias management	16.3.0
2019-06	SA#84	SP-190484	0190		F	Corrections to affiliation procedures	16.3.0
2019-06	SA#84	SP-190484	0191	3	F	Affiliation clarifications	16.3.0
2019-06	SA#84	SP-190484	0192	1	C	Preconfigured regroup information in dynamic data	16.3.0
2019-06	SA#84	SP-190484	0194	2	F	Remove the duplicated Key Management Server URI definiton	16.3.0
2019-06	SA#84	SP-190484	0196	3	B	Change to Location Subscription for notification immediate	16.3.0
2019-06	SA#84	SP-190488	0201	2	B	Functional alias subscription and notification	16.3.0
2019-06	SA#84	SP-190488	0203	3	B	Location information reporting based on functional alias	16.3.0
2019-06	SA#84	SP-190488	0204	2	F	Functional alias clarifications	16.3.0
2019-06	SA#84	SP-190484	0205	2	F	Abbreviations	16.3.0
2019-06	SA#84	SP-190484	0206	2	F	Clarifications for group regroup rules	16.3.0
2019-09	SA#85	SP-190731	0182	4	C	Configuration of the user notification in temporary group formation	16.4.0
2019-09	SA#85	SP-190731	0210	5	F	Corrections to the emergency alert procedures	16.4.0
2019-09	SA#85	SP-190731	0211	3	F	Corrections to clauses in 10.9 Location Management (on-network)	16.4.0
2019-09	SA#85	SP-190730	0220	2	F	Functional model update for interconnection and migration	16.4.0
2019-09	SA#85	SP-190735	0207	3	B	Providing activated functional alias information to the group controlling server	17.0.0
2019-09	SA#85	SP-190735	0208	2	B	Providing the list of functional aliases used by affiliated group members	17.0.0
2019-09	SA#85	SP-190735	0209	1	B	Prevent from de-affiliation when using a specific functional alias(es)	17.0.0
2019-12	SA#86	SP-191113	0221	4	F	Introducing descriptive text describing the urgency handling in the MC service system	17.1.0
2019-12	SA#86	SP-191114	0222	2	B	Addition of preconfigured regroup procedures	17.1.0
2019-12	SA#86	SP-191113	0223	1	F	Corrections on functional alias to group binding	17.1.0
2019-12	SA#86	SP-191113	0224		C	Resolving EN on functional alias to group binding impacts	17.1.0
2019-12	SA#86	SP-191114	0226	1	F	Alignment on MCX emergency alert procedures	17.1.0
2019-12	SA#86	SP-191109	0228	1	A	Alignment on MCX emergency alert procedures	17.1.0
2020-03	SA#87-E	SP-200119	0233	1	F	Add temporary group teardown within an MC system	17.2.0
2020-03	SA#87-E	SP-200118	0236	1	B	Purpose of requested priority	17.2.0
2020-07	SA#88-E	SP-200342	0243	1	B	Additional details to the Location information report	17.3.0
2020-07	SA#88-E	SP-200342	0244	1	B	Additional details to the Location information notification	17.3.0
2020-07	SA#88-E	SP-200342	0245	1	B	Additional details to the Location report response	17.3.0
2020-07	SA#88-E	SP-200342	0246	1	B	Additional details to the Location reporting procedures	17.3.0

2020-07	SA#88-E	SP-200342	0248	1	F	Replacing the usage of MCPTT with MC Service	17.3.0
2020-07	SA#88-E	SP-200342	0249	3	F	Corrections to the location information flows	17.3.0
2020-07	SA#88-E	SP-200342	0250	1	F	Location information in the emergency alert request	17.3.0
2020-07	SA#88-E	SP-200342	0251	1	B	Configuration location history reporting	17.3.0
2020-07	SA#88-E	SP-200342	0252	1	B	Cancel location history transmission	17.3.0
2020-07	SA#88-E	SP-200342	0253	1	B	Location history reporting	17.3.0
2020-07	SA#88-E	SP-200342	0254	1	B	Status location history reporting	17.3.0
2020-07	SA#88-E	SP-200342	0255	1	B	Clarification on setting the MBMS broadcast areas when activating MBMS bearer	17.3.0
2020-07	SA#88-E	SP-200340	0257	1	B	Communication security context when using functional alias	17.3.0
2020-07	SA#88-E	SP-200342	0260	1	B	Dynamic data associated with a group at GMS	17.3.0
2020-09	SA#89-E	SP-200844	0258	5	B	Clarification on user subscription, group policy and functional alias policy	17.4.0
2020-09	SA#89-E	SP-200844	0261	1	F	Removal of Editors Note related to functional alias resolution by LMS	17.4.0
2020-09	SA#89-E	SP-200844	0267		F	Private calls in emergency state	17.4.0
2020-09	SA#89-E	SP-200844	0269	1	B	Individual emergency alert cancel	17.4.0
2020-09	SA#89-E	SP-200844	0270	1	D	Clarification of MCX Administrator	17.4.0
2020-09	SA#89-E	SP-200843	0273		B	Functional alias configuration	17.4.0
2020-12	SA#90-E	SP-200995	0275	1	C	MC service emergency alert clarifications	17.5.0
2020-12	SA#90-E	SP-200995	0278	1	B	Request for network resources at session establishment from the MC service server	17.5.0
2021-04	SA#91-E	SP-210180	0282	-	F	EN removal regarding MC system ID	17.6.0
2021-04	SA#91-E	SP-210180	0283	1	B	Introduction of MC service UE label for location reporting	17.6.0
2021-04	SA#91-E	SP-210180	0284	1	F	Functional alias takeover request related correction	17.6.0
2021-06	SA#92-E	SP-210567	0262	3	C	Clarification to location information cancel subscription	17.7.0
2021-06	SA#92-E	SP-210567	0289		F	Addition of MBMS suspension report information flow	17.7.0
2021-06	SA#92-E	SP-210567	0290	1	F	General corrections to MBMS procedures	17.7.0
2021-06	SA#92-E	SP-210567	0291		F	Corrections to location management procedures	17.7.0
2021-09	SA#93-E	SP-210960	0292	2	A	Clarification of MC service server retry for dedicated bearer request	17.8.0
2021-09	SA#93-E	SP-210963	0293	2	F	Clarifications for Location management PLUS NEW enhancements for MC service UE label	17.8.0
2021-09	SA#93-E	SP-210963	0293	2	F	Corrections to Location Information table in 10.9.2.3	17.8.0
2021-12	SA#94-E	SP-211524	0296		F	Clarification for Location reporting configuration	17.9.0
2021-12	SA#94-E	SP-211524	0297		F	Clarification for location reporting within MBSFN	17.9.0
2021-12	SA#94-E	SP-211524	0304	1	F	Clarification to MC group configuration procedures for interconnect	17.9.0
2021-12	SA#94-E	SP-211529	0298	1	B	Addition of definitions of terms and introduction related to MC gateway UE function	18.0.0
2021-12	SA#94-E	SP-211529	0299	2	B	Introduction of subclauses to capture MC gateway UE function details	18.0.0
2021-12	SA#94-E	SP-211529	0300		B	MCGWUE 3GPP access network related location information management	18.0.0
2021-12	SA#94-E	SP-211529	0301	1	B	MCGWUE_MBMS support for MC clients residing on non-3GPP devices	18.0.0
2021-12	SA#94-E	SP-211529	0302	1	B	Connection authorisation mechanisms	18.0.0
2021-12	SA#94-E	SP-211529	0303		B	Functional architecture	18.0.0
2022-03	SA#95-E	SP-220109	0305		F	Correction to On-demand usage of location information procedure	18.1.0
2022-03	SA#95-E	SP-220106	0306		D	Editorial corrections in section 11 on MC Gateway UE	18.1.0
2022-03	SA#95-E	SP-220106	0307	1	B	Functional model reference points	18.1.0
2022-03	SA#95-E	SP-220106	0308	1	B	Functional model media plane aspects	18.1.0
2022-03	SA#95-E	SP-220106	0309	1	B	Using identities behind the MC gateway UE	18.1.0
2022-03	SA#95-E	SP-220106	0310		B	MC gateway UE routing capabilties	18.1.0
2022-06	SA#96	SP-220478	0311	1	B	MC gateway UE – MC client disconnection procedure	18.2.0
2022-06	SA#96	SP-220478	0312	1	F	Clean-up of clause 11 specifying MC gateway UE support	18.2.0
2022-06	SA#96	SP-220478	0313	1	B	Clarification regarding the protocol used on new reference points	18.2.0
2022-06	SA#96	SP-220478	0314	1	B	Clarify the association between certain entities	18.2.0
2022-06	SA#96	SP-220477	0315	1	B	Migration during an ongoing group communication	18.2.0
2022-06	SA#96	SP-220477	0317	1	B	Private call using functional alias towards a partner MC system	18.2.0
2022-06	SA#96	SP-220478	0318		B	Clarification of MC gateway UE selection	18.2.0
2022-06	SA#96	SP-220476	0319		F	Corrections to the use of MC service system	18.2.0

2022-06	SA#96	SP-220478	0320		B	Added MC GW UnMapGroupToBearer request and response support	18.2.0
2022-06	SA#96	SP-220477	0322		B	Sharing location information across MC systems (functional model)	18.2.0
2022-06	SA#96	SP-220477	0323	1	B	Sharing location information across MC systems (on-demand)	18.2.0
2022-06	SA#96	SP-220477	0324		B	Sharing location information across MC systems (triggered)	18.2.0
2022-06	SA#96	SP-220477	0325		B	Sharing location information across MC systems (subscription)	18.2.0
2022-06	SA#96	SP-220477	0326		B	Sharing location information across MC systems (configuration)	18.2.0
2022-06	SA#96	SP-220477	0327	1	B	Functional alias support for migrated users	18.2.0
2022-06	SA#96	SP-220478	0328		B	MC GW UnMapGroupToBearer request and response procedure	18.2.0
2022-06	SA#96	SP-220477	0330	2	B	Migration procedure during and ongoing private communication	18.2.0
2022-06	SA#96	SP-220477	0331	1	B	Allow no roaming migration	18.2.0
2022-06	SA#96	SP-220478	0332	1	B	IP Assignment support by MC Gateway UE	18.2.0
2022-09	SA#97	SP-220924	0329	2	B	Allow the user to restrict the dissemination of the location information	18.3.0
2022-09	SA#97	SP-220926	0334	1	B	Functional alias as target address towards a partner MCData system	18.3.0
2022-09	SA#97	SP-220924	0335	1	F	Functional Alias URI requirement	18.3.0
2022-09	SA#97	SP-220927	0336	1	F	MC client IP address relationship	18.3.0
2022-09	SA#97	SP-220926	0339	1	F	Addition of functional alias that corresponds to the location information requesting MC service user	18.3.0
2022-09	SA#97	SP-220924	0340	1	B	LMS access to all the MCX user profiles (functional model)	18.3.0
2022-09	SA#97	SP-220927	0341	2	C	MC gateway UE association with one MC service	18.3.0
2022-09	SA#97	SP-220924	0342	1	C	Removing unicast bearer status from MBMS bearer information	18.3.0
2022-09	SA#97	SP-220926	0346	1	F	Terminology clean-up on the architectural requirements for migration	18.3.0
2022-09	SA#97	SP-220926	0347	1	D	Editorial corrections in clause 10.16.2.3	18.3.0
2022-09	SA#97	SP-220924	0348	1	F	Corrections to reference point CSC-16	18.3.0
2022-09	SA#97	SP-220924	0349	1	F	SIP interface corrections for reference points CSC-7, CSC-19, CSC-20	18.3.0
2022-12	SA#98-e	SP-221243	0351	1	F	Clarification of use of QCI-69 bearer for HTTP-1 reference point	18.4.0
2022-12	SA#98-e	SP-221247	0352	1	C	Updating migration overview	18.4.0
2022-12	SA#98-e	SP-221247	0353	5	B	Private call towards a migrated MC service user	18.4.0
2022-12	SA#98-e	SP-221243	0354	2	F	Description for the terms used in the location management procedures	18.4.0
2022-12	SA#98-e	SP-221247	0355	4	B	Partner MC service server stores necessary information for communication redirection	18.4.0
2023-03	SA#99	SP-230289	0356	3	B	Introduction of the ad hoc group emergency alert	18.5.0
2023-03	SA#99	SP-230287	0358	5	C	Add Criteria to the Preconfigured Group Regroup Request	18.5.0
2023-03	SA#99	SP-230288	0363	3	B	Migration service de-authorization procedure initiated by MC service server	18.5.0
2023-03	SA#99	SP-230287	0366	2	B	Preconfigured regrouping support for MCPTT	18.5.0
2023-03	SA#99	SP-230288	0367	3	F	Clarification on storing of MC service IDs mapping in Primary system during migration service authorization	18.5.0
2023-06	SA#100	SP-230710	0360	5	F	Corrections related to MC gateway UE and identities	18.6.0
2023-06	SA#100	SP-230703	0364	3	B	Updating the MC service user ID list within preconfigured user regroup	18.6.0
2023-06	SA#100	SP-230710	0365	3	F	Terminology alignment within MC GW UE	18.6.0
2023-06	SA#100	SP-230703	0369	1	B	User Location Authorization and Profile	18.6.0
2023-06	SA#100	SP-230703	0376		D	Correct the repeated space errors in TS 23.280	18.6.0
2023-06	SA#100	SP-230703	0377		D	Correct the spelling errors of words in TS 23.280.	18.6.0
2023-06	SA#100	SP-230708	0378	1	B	Updates procedures for allowing subsequent MCVideo and MCData communications after an adhoc group emergency alert	18.6.0
2023-06	SA#100	SP-230708	0379	1	B	Adhoc group emergency alert participants list notification	18.6.0
2023-06	SA#100	SP-230708	0380	1	B	Clarification on emergency states in conjunction with adhoc group alert procedures	18.6.0
2023-06	SA#100	SP-230708	0382	2	F	Behaviour corrections on ad hoc group emergency alert removal	18.6.0
2023-06	SA#100	SP-230708	0383	1	F	Clarification on subsequent group call on ad hoc group for emergency alert	18.6.0

2023-06	SA#100	SP-230707	0384	2	F	MC service authorization notification alignment	18.6.0
2023-06	SA#100	SP-230708	0389	4	B	Ad hoc group emergency alert between multiple MC systems	18.6.0
2023-06	SA#100	SP-230703	0392		D	Correct the errors in the use of singular and plural forms in TS 23.280	18.6.0
2023-06	SA#100	SP-230703	0393		D	Remove the duplicate and extra words in the expression of TS 23.280.	18.6.0
2023-06	SA#100	SP-230703	0394	2	B	Group de-affiliation for specific UE	18.6.0
2023-06	SA#100	SP-230710	0395	1	B	MC gateway UE routing capabilities	18.6.0
2023-06	SA#100	SP-230703	0396	1	D	Syncing Criteria changes with 23.379	18.6.0
2023-06	SA#100	SP-230703	0397	1	D	Reference corrections in 10.6.3.3.2	18.6.0
2023-06	SA#100	SP-230708	0398	3	B	Addressing EN related to implicit affiliation to ad hoc group alert participants	18.6.0
2023-06	SA#100	SP-230707	0399	1	B	Updating private call using FA	18.6.0
2023-06	SA#100	SP-230703	0400	1	F	Corrections to Ad hoc group emergency alert request information flow	18.6.0
2023-06	SA#100	SP-230703	0401	1	F	Corrections to preconfigured regroup request information flow	18.6.0
2023-06	SA#100	SP-230703	0402	1	D	Moving emergency alert information flow under emergency alert section	18.6.0
2023-06	SA#100	SP-230710	0403		F	Corrections of the GW-local and GW-core interface	18.6.0
2023-09	SA#101	SP-231001	0361	6	F	Resolving the target KMS URI for a migrated MC service user	18.7.0
2023-09	SA#101	SP-230998	0408	2	F	Correction for group de-affiliation for specific UE	18.7.0
2023-09	SA#101	SP-230998	0411	1	F	Adding group definitions (Common Core)	18.7.0
2023-09	SA#101	SP-231005	0414	1	F	PDN connection establishment for MC service clients behind MC GW UE	18.7.0
2023-09	SA#101	SP-231005	0415	2	F	GW reference point protocol	18.7.0
2023-09	SA#101	SP-231005	0416		F	Correcting figure 11.4.3-1	18.7.0
2023-09	SA#101	SP-230998	0421		F	Remove the EN in 10.15.1	18.7.0
2023-09	SA#101	SP-230998	0422	2	F	Resolve the affiliation related EN in clause 5.2.5	18.7.0
2023-09	SA#101	SP-230998	0427		F	Corrections to the informative wordings	18.7.0
2023-09						Re-implementation of CR 0422 Rev. 2	18.7.1
2023-12	SA#102	SP-231559	0445	1	F	Definition of MC server	18.8.0
2023-12	SA#102	SP-231553	0456		F	Correction to information flow description in 10.9.2.16	18.8.0
2023-12	SA#102	SP-231558	0457	1	F	Reporting success or failure of an ad hoc group emergency alert request	18.8.0
2023-12	SA#102	SP-231558	0459	1	F	Reporting success or failure of an ad hoc group emergency alert cancel request	18.8.0
2023-12	SA#102	SP-231558	0461	2	F	Improving reliability of MC ad hoc group emergency alert	18.8.0
2023-12	SA#102	SP-231559	0491	1	F	Corrections of the use of MC client term in MCGWUE	18.8.0
2023-12	SA#102	SP-231559	0495	1	F	Connection/disconnection authorisation procedures	18.8.0
2024-03	SA#103	SP-240305	0516	1	F	Corrections to the IP model figures	18.9.0
2024-03	SA#103	SP-240304	0533	1	F	Reporting success or failure of an ad hoc group emergency alert initiation request (multiple MC systems)	18.9.0
2024-03	SA#103	SP-240304	0535	1	F	Reporting success or failure of an ad hoc group emergency alert cancel request (multiple MC systems)	18.9.0
2024-03	SA#103	SP-240297	0542	1	A	Removal of procedure 10.1.6.2 on signalling plane registration between MC systems	18.9.0
2024-06	SA#104	SP-240758	0550	1	F	MC gateway UE updates for security alignment	18.10.0
2024-06	SA#104	SP-240758	0557	1	F	Clarification on MC gateway UE definition	18.10.0
2024-06	SA#104	SP-240758	0559	1	F	Configuration for MC client on non-3GPP device	18.10.0
2024-12	SA#106	SP-241707	0603	1	F	Removing external applications access to MC services	18.11.0
2024-12	SA#106	SP-241707	0625	2	F	Void MBMS bearer event notification procedure	18.11.0
2024-12	SA#106	SP-241707	0627	1	F	Removing EN on Entering MC service emergency alert area	18.11.0
2025-03	SA#107	SP-250199	0634	1	F	Resolve the EN in clause 7.5.2.23	18.12.0
2025-03	SA#107	SP-250199	0636	1	F	Resolve the EN in clause 7.5.2.24	18.12.0
2025-03	SA#107	SP-250199	0638	1	F	Resolve the EN in clause 7.5.3.4	18.12.0
2025-03	SA#107	SP-250199	0640	1	F	Resolve the EN in clause 7.5.3.7	18.12.0
2025-03	SA#107	SP-250199	0642	1	F	Resolve the EN in clause 10.16.2.1	18.12.0
2025-03	SA#107	SP-250199	0644	1	F	Resolve the EN in clause 10.8.3.2a.2	18.12.0
2025-03	SA#107	SP-250199	0648	1	F	Correction in MC service configuration on primary MC system	18.12.0
2025-03	SA#107	SP-250199	0651		F	Resolving an editor's note in clause describing MC service group affiliation and MC service group de-affiliation	18.12.0

2025-09	SA#109	SP-251056	0677	1	F	Resolving Editor's Notes in the Rel-18 version of TS 23.280	18.13.0
2025-09	SA#109	SP-251056	0683	1	F	Resolve the EN in clause 10.7.3.6.2	18.13.0

History

Document history		
V18.9.0	April 2024	Publication
V18.10.0	July 2024	Publication
V18.11.0	January 2025	Publication
V18.12.0	April 2025	Publication
V18.13.0	September 2025	Publication