ETSI TS 122 280 V15.3.0 (2018-07)

LTE;
Mission Critical Services Common Requirements
(3GPP TS 22.280 version 15.3.0 Release 15)

Reference
RTS/TSGS-0122280vf30

Keywords
LTE

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

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

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

Modal verbs terminology

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

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

Contents

Intellectual Property Rights 2
Foreword 2
Modal verbs terminology 2
Foreword 8
1 Scope 9
2 References 9
3 Definitions and abbreviations 9
3.1 Definitions 9
3.2 Abbreviations 11
4 Overview 11
4.1 Rationale for MCCoRe 11
4.2 MCCoRe creation process 11
5 MCX Service requirements common for on the network and off the network 12
5.1 General Group Communications requirements 12
5.1.1 General aspects 12
5.1.2 Group/status information 12
5.1.3 Group configuration 12
5.1.4 Identification 13
5.1.5 Membership/affiliation 13
5.1.6 Group Communication administration 13
5.1.7 Prioritization 13
5.1.8 Charging requirements for MCX Service 13
5.1.9 MCX Service Emergency Alert triggered by Location 14
5.2 Broadcast Group 14
5.2.1 General Broadcast Group Communication 14
5.2.2 Group-Broadcast Group (e.g., announcement group) 14
5.2.3 User-Broadcast Group (e.g., System Communication) 14
5.3 Late communication entry 14
5.4 Receiving from multiple MCX Service communications 15
5.4.1 Overview 15
5.4.2 Requirements 15
5.5 Private Communication 16
5.5.1 Private Communication general requirements 16
5.5.2 Charging requirements for MCX Service 16
5.6 MCX Service priority requirements 16
5.6.1 Overview 16
5.6.2 Communication types based on priorities 17
5.6.2.1 MCX Service Emergency and Imminent Peril general requirements 17
5.6.2.1.1 Overview 17
5.6.2.1.2 Requirements 17
5.6.2.2 MCX Service Emergency Group Communication 17
5.6.2.2.1 MCX Service Emergency Group Communication requirements 17
5.6.2.2.2 MCX Service Emergency Group Communication cancellation requirements 18
5.6.2.3 MCX Service Imminent Peril Group Communication 18
5.6.2.3.1 MCX Service Imminent Peril Group Communication requirements 18
5.6.2.3.2 MCX Service Imminent Peril Group Communication cancellation requirements 19
5.6.2.4 MCX Service Emergency Alert 19
5.6.2.4.1 MCX Service Emergency Alert requirements 19
5.6.2.4.2 MCX Service Emergency Alert cancellation requirements 20
5.7 MCX Service User ID 20
5.8 MCX UE management 20
5.9 MCX Service User Profile 20
5.9a Functional alias 21

5.10 Support for multiple devices 22
5.11 Location 22
5.12 Security 23
5.13 Media quality 24
5.14 Relay requirements 24
5.15 Gateway requirements 24
5.16 Control and management by Mission Critical Organizations 24
5.16.1 Overview 24
5.16.2 General requirements 24
5.16.3 Operational visibility for Mission Critical Organizations 25
5.17 General administrative – groups and users 25
5.18 Open interfaces for MCX services 25
5.18.1 Overview 25
5.18.2 Requirements 25
5.19 Media forwarding 25
5.19.1 Service description 25
5.19.2 Requirements 26
5.20 Receipt notification 26
5.20.1 Service description 26
5.20.2 Requirements 26
5.21 Additional services for MCX Service communications 26
5.21.1 Remotely initiated MCX Service communication 26
5.21.1.1 Overview 26
5.21.1.2 Requirements 26
5.21.2 Remotely terminated MCX Service communication 26
5.21.2.1 Requirements 26

6 MCX Service requirements specific to on-network use 27
6.1 General administrative – groups and users 27
6.2 MCX Service communications 27
6.2.1 Notification and acknowledgement for MCX Service Group Communications 27
6.2.2 Queuing 27
6.3 General requirements 28
6.4 General MCX Service Group Communications 28
6.4.1 General aspects 28
6.4.2 Group status/information 28
6.4.3 Identification 28
6.4.4 Membership/affiliation 29
6.4.5 Membership/affiliation list 29
6.4.6 Authorized user remotely changes another MCX User's affiliated and/or Selected MCX Service Group(s) 29
6.4.6.1 Mandatory change 29
6.4.6.2 Negotiated change 29
6.4.7 Prioritization 30
6.4.8 Relay requirements 30
6.4.9 Administrative 30
6.5 Broadcast Group 30
6.5.1 General Broadcast Group Communication 30
6.5.2 Group-Broadcast Group (e.g., announcement group) 31
6.5.3 User-Broadcast Group (e.g., System Communication) 31
6.6 Dynamic group management (i.e., dynamic regrouping) 31
6.6.1 General dynamic regrouping 31
6.6.2 Group regrouping 31
6.6.2.1 Service description 31
6.6.2.2 Requirements 31
6.6.3 Temporary Group-Broadcast Group 32
6.6.4 User regrouping 32
6.6.4.1 Service description 32
6.6.4.2 Requirements 32
6.7 Private Communication 33
6.7.1 Overview 33
6.7.2 General requirements 33

6.7.3 Administrative 33
6.7.4 Prioritization 34
6.7.5 Private Communication (without Floor control) commencement requirements 34
6.7.6 Private Communication (without Floor control) termination 34
6.8 MCX Service priority requirements 34
6.8.1 General 34
6.8.2 3GPP system access controls 35
6.8.3 3GPP system admission controls 35
6.8.4 3GPP system scheduling controls 36
6.8.5 UE access controls 36
6.8.6 Mobility and load management 36
6.8.6.1 Mission Critical mobility management according to priority 36
6.8.6.2 Load management 36
6.8.7 Application layer priorities 36
6.8.7.1 Overview 36
6.8.7.2 Requirements 36
6.8.8 Communication types based on priorities 37
6.8.8.1 MCX Service Emergency Group Communication requirements 37
6.8.8.2 MCX Service Emergency Private Communication requirements 37
6.8.8.3 Imminent Peril Group Communication requirements 37
6.8.8.4 MCX Service Emergency Alert 38
6.8.8.4.1 Requirements 38
6.8.8.4.2 MCX Service Emergency Alert cancellation requirements 38
6.9 IDs and aliases 38
6.10 MCX Service User Profile management 38
6.11 Support for multiple devices 39
6.12 Location 39
6.13 Security 39
6.13.1 Overview 39
6.13.2 Cryptographic protocols 39
6.13.3 Authentication 39
6.13.4 Access control 40
6.13.5 Regulatory issues 40
6.13.6 Storage control 40
6.14 Interactions for MCX Service Group Communications and MCX Service Private Communications 40
6.15 Additional services for MCX Service communications 40
6.15.1 Discreet listening capabilities 40
6.15.2 Ambient listening 41
6.15.2.1 Overview of ambient listening 41
6.15.2.2 Ambient listening requirements 41
6.15.2.2.1 General ambient listening requirements 41
6.15.2.2.2 Remotely initiated ambient listening requirements 41
6.15.2.2.3 Locally initiated ambient listening requirements 41
6.15.3 Remotely initiated MCX Service Communication 41
6.15.3.1 Overview 41
6.15.3.2 Requirements 42
6.15.4 Recording and audit requirements 42
6.16 Interaction with telephony services 43
6.17 Interworking 43
6.17.1 Non-3GPP access 43
6.17.2 Interworking between MCX Service systems 43
6.18 MCX Service coverage extension using ProSe UE-to-Network Relays 43
6.19 Additional MCX Service requirements 44
6.19.1 Communication rejection and queuing 44
6.19.1.1 Requirements 44

7 MCX Service requirements specific to off-network use 44
7.1 Off-network communications overview 44
7.2 General off-network MCX Service requirements 46
7.3 Admission control 47
7.3.1 General aspects 47
7.3.2 Communication initiation 47

7.4 Communication termination 47
7.5 Broadcast Group 47
7.6 MCX Service priority requirements 47
7.7 Communication types based on priorities 48
7.7.1 MCX Service Emergency Group Communication requirements 48
7.7.2 MCX Service Emergency Group Communication cancellation requirements 48
7.7.3 Imminent Peril Communication 48
7.7.3.1 Imminent Peril Group Communication requirements 48
7.7.3.2 Imminent Peril Group Communication cancellation requirements 49
7.8 Location 49
7.9 Security 49
7.10 Off-network MCX Service operations 49
7.11 Off-network UE functionality 49
7.12 Streaming for ProSe UE-to-UE Relay and UE-to-Network Relay 50
7.12.1 UE-to-Network Relay for all data types 50
7.12.2 UE-to-UE Relay streaming 50
7.12.3 Off-Network streaming 50
7.13 Switching to off-network MCX Service 50
7.14 Off-network recording and audit requirements 51
7.15 Off-network UE-to-UE Relay 51
7.15.1 Private Communications 51
7.15.2 Group Communications 51

8 Inter-MCX Service interworking 51
8.1 Inter-MCX Service interworking overview 51
8.2 Concurrent operation of different MCX Services 51
8.2.1 Overview 51
8.2.2 Requirements 52
8.3 Use of unsharable resources within a UE 52
8.4 Single group with multiple MCX Services 53
8.4.1 Overview 53
8.4.2 Requirements 53
8.4.3 Compatibility of UE 53
8.4.3.1 Advertising service capabilities required 53
8.4.3.2 Conversion between capabilities 53
8.4.4 Individual permissions for service access 53
8.4.5 Common alias and user identities or mappable 54
8.4.6 Single location message 54
8.5 Priority between services 54
8.5.1 Overview 54
8.5.2 Requirements 54

9 Air ground air Communication 54
9.1 Service Description 54
9.2 Requirements 55

10 MCX Service in IOPS mode 55

Annex A (normative): MCCoRe Requirements for MCPTT 56

Annex B (normative): MCCoRe Requirements for MCVideo 66

Annex C (normative): MCCoRe Requirements for MCData 76

Annex D (informative): Characteristics and traffic assumptions for air ground air communications 86

D.1 Environment 86
D.2 Altitudes 86
D.3 Maximum speed and mobility 86
D.4 Traffic assumptions 86

Annex E (informative): Variables 87

Annex F (informative): Change history 88

History 90

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

The present document provides the service requirements that are common across two or more mission critical services, that is MCPTT, MCData and MCVideo. The mission critical services make use of capabilities included in Group Communications System Enablers and Proximity Services, with additional requirements specific to the MCPTT Service as specified in 3GPP TS 22.179 [1], MCVideo Service as specified in 3GPP TS 22.281 [2], and MCData Service as specified in 3GPP TS 22.282 [3]. The mission critical services can be used for public safety applications and also for general commercial applications (e.g., utility companies and railway operators). The requirements in this specification do not apply to GSM or UMTS.

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 TS 22.179: "Mission Critical Push to Talk (MCPTT); Stage 1".

[2] 3GPP TS 22.281: "Mission Critical Video services".

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

[4] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[5] 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS)".

[6] 3GPP TS 22.468: "Group Communication System Enablers for LTE (GCSE_LTE) ".

[7] 3GPP TS 22.011: "Service accessibility".

[8] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Stations (MS) in idle mode".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [4] 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 [4].

Affiliated MCX Service Group Member: An MCX Service Group Member who has indicated an interest in participating in communications of the group, has been accepted by the MCX Service, and is prepared to receive and/or transmit Group Communications from/to the particular MCX Group.

Air ground air Communication: A communication (point-to-point or group) between at least one MCX User located on the ground and one or more MCX Users in helicopter(s) or aircraft while not on the ground, but in flight (in the air).

Broadcast Group Communication: A group communication where the initiating MCX User expects no response from the other MCX Users, so that when the user’s transmission is complete, so is the communication.

Group Communication: A one-to-many or many-to-many communication using an MCX Service.

In-progress Emergency: An emergency condition that has been accepted by the MCX Service, but has not yet been cancelled.

Late Entry: An Affiliated MCX Service Group Member joins in an in progress MCX Service Group Communication.

Location: The current physical location of the MCX UE.

MCX Service Administrator: An individual authorized to control MCX parameters for an organization including, for example, user and group definitions, user/group aliases, user priorities, group membership/priorities/hierarchies, security and privacy controls.

MCX Service Emergency Alert: A notification from the MCX UE to the MCX Service that the MCX User has an emergency condition.

MCX Service Emergency State: A heightened condition of alarm for an MCX User indicating a need for immediate assistance due to a personal life-threatening situation.

MCX Service Emergency Group Communication: An urgent MCX Service group communication initiated by a MCX user when there is the potential of immediate death or serious injury.

MCX Service Group: A defined set of MCX Users with associated communication dispositions (e.g. media restrictions, default priority and commencement directions).

MCX Service Group Communication: A group communication for a particular MCX Service.

MCX Service Group Member: An MCX User authorized, upon successful affiliation, to participate in Group Communications of a particular MCX Group.

MCX Service Imminent Peril Group Communication: An urgent MCX Service Group Communication initiated by an MCX user when there is a potential of death or serious injury, but is less critical than an MCX Service Emergency Group Communication.

MCX Service User Profile: The set of information associated to an MCX User that allows that user to employ the MCX Service in a given role and/or from a given MCX UE.

MCX UE: A UE that can be used to participate in MCX Services.

MCX User: A user of MCX Service, who can use an MCX UE to participate in MCX Services.

Mission Critical: Quality or characteristic of a communication activity, application, service or device, that requires low setup and transfer latency, high availability and reliability, ability to handle large numbers of users and devices, strong security and priority and pre-emption handling.

Mission Critical Applications: Generic communication applications with mission critical characteristics, traditionally encompassing push-to-talk voice (MCPTT), real-time video (MCVideo) and real-time data (MCData).

NOTE 1: The short name, **MCX,** is used instead, with X standing for PTT, Video or Data

Mission Critical Organization: An end-user organization that includes MCX Users and/or MCX UEs, and can include MCX Service Administrators, and can be organized hierarchically with administrative control delegated within the organization or to an outside entity.

Mission Critical Service: Communication service reflecting enabling capabilities Mission Critical Applications and provided to end users from Mission Critical Organizations and mission critical applications for other businesses and organizations (e.g., utilities, railways).

NOTE 2: The short name, MCX Service, can be used instead.

Participant: An MCX User who is currently receiving and/or transmitting in a Group Communication or a Private Communication.

Participant type: Functional category of the Participant (e.g., first responder, second responder, dispatch, dispatch supervisor), typically defined by the MCX Service Administrators.

Private Communication: A one-to-one communication between a pair of users using an MCX Service.

Selected MCX Service Group: An MCX Service Group that a particular Affiliated MCX Service Group Member uses for transmission.

Transmitting MCX Service Group Member: An Affiliated MCX Service Group Member who is currently transmitting in a Group Communication to a Selected MCX Service Group.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [4] 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 [4].

MCCoRe	Mission Critical Services Common Requirements
MCData	Mission Critical Data
MCPTT	Mission Critical Push To Talk
MCVideo	Mission Critical Video
MCX	Mission Critical X, with X = PTT or X= Video or X= Data
MCX Service	Mission Critical Service

4 Overview

4.1 Rationale for MCCoRe

Further development of mission critical services beyond Mission Critical Push To Talk (MCPTT), such as Mission Critical Video (MCVideo) and Mission Critical Data (MCData), created an opportunity to re-use base functionality documented in the Stage 1 requirements for MCPTT. For example, the ability to communicate mission critical information to groups of users is a common need regardless of service type. Wherever originating MCPTT requirements were found to be in common with other mission critical services, those requirements were moved to this Technical Specification (3GPP TS 22.280). Each requirement that was moved has been voided in 3GPP TS 22.179, and an informative annex has been created at the end of that specification documenting the location of the originating 3GPP TS 22.179 requirement in the present document.

4.2 MCCoRe creation process

The creation of 3GPP TS 22.280 followed a thorough analysis by mission critical application stakeholders of all the requirements in 3GPP TS 22.179, TR 22.879, and TR 22.880. Each set of requirements was evaluated, requirement-by-requirement, to determine if any one requirement was applicable to another service (MCPTT, MCVideo, or MCData). If anyone requirement was shared between two or more services, it was designated as a Mission Critical Services Common Requirements (MCCoRe) requirement and placed into this technical specification. At the end of this specification, there are sets of normative annexes that enumerate each requirement in the present document that is applicable to the given scope for the annex. For instance, one annex covers MCPTT, and there is a comprehensive table that lists every requirement that follows in clauses 5-9 that are applicable to MCPTT.

In the present document the term, MCX Service, is used to mean any mission critical service and when applied in requirements it means any mission critical service that is identified in the normative annexes as applying to the requirement in question. When the term, MCX Service, is used multiple times in a single requirement it means the same MCX Service except in the case of the inter service interworking in clause 8. Therefore, other than requirements in the inter services interworking clause, all requirements in the present document are single service requirements.

In principle, a mission critical group could use multiple services. At any time during a mission critical group communication, a group of mission critical users can, subject to permissions and availability of services and capable UEs, start or stop using any one or more instantiation(s) of any of the MCX services. In the text of the specification for each individual service, the group is considered to use the services of that individual type, and consequently is called MCPTT Group, MCVideo Group, MCData Group, or generically, MCX Service Group. Referring to a group as an individual service group is for writing simple requirements purposes, and does not mean that the group cannot actively use other services. See sub-clause 8.4 for more information.

The grouping and consolidation of common requirements shared by multiple mission critical applications is not to be construed as a statement or requirement of architectural design, impacting entities and interfaces. It is for downstream working groups to determine whether they can:

a) create generic MCX Service functionality that can be re-used by all Mission Critical Applications virtually unmodified;

b) extend and/or customize common MCX Services, if they determine that a Mission Critical Application has special needs, or

c) define separate support for Mission Critical Applications if they determine that they are so specialized that they cannot take advantage of a common MCX Service.

5 MCX Service requirements common for on the network and off the network

5.1 General Group Communications requirements

5.1.1 General aspects

[R-5.1.1-001] The MCX Service shall allow an MCX User utilizing one or more MCX UE(s), concurrently, to sign-in and receive service on each of the MCX UE(s).

[R-5.1.1-002] The MCX Service shall provide a mechanism by which an MCX UE makes a MCX Service group transmission to any MCX Service Group(s) for which the current MCX User is authorized.

NOTE: For off-network use, only group members with MCX UEs within communication range receive the transmission.

[R-5.1.1-003] The MCX Service shall be able to notify the Affiliated MCX Service Group Members when the group communication is set up (e.g., this can be provided as an audible tone on the MCX UE).

[R-5.1.1-004] The MCX Service shall provide a mechanism to disable notifications (e.g., audible tone) on an MCX UE when receiving normal MCX Service Group Communications (not MCX Service Emergency or Imminent Peril Communications).

[R-5.1.1-005] At any moment in time in an MCX Service Group communication, only one Participant type shall be used per Participant.

[R-5.1.1-006] The MCX Service shall provide a mechanism for a dispatcher or authorized user to configure which content source shall be able to transmit the content to an MCX Service Group (e.g. video cameras near an incident).

5.1.2 Group/status information

[R-5.1.2-001] The MCX Service shall provide a mechanism by which an MCX Service UE determines in which of the MCX Service Groups for which it is authorized there is an on-going MCX Service Group Communication.

[R-5.1.2-002] The MCX Service shall provide a mechanism by which an authorized MCX User determines in which MCX Service Groups there is an on-going MCX Service Group Communication.

5.1.3 Group configuration

[R-5.1.3-001] The MCX Service shall allow the MCX Service Administrator to restrict who can be a member of specific MCX Service Groups, so that those MCX Service Groups shall be inaccessible to other users, including dispatchers or supervisors.

[R-5.1.3-002] The MCX Service shall enable a properly provisioned and authorized MCX UE operating on the network to receive its application layer level parameters (e.g., MCX Service Group ID, group keys) necessary for initiating and participating in Selected MCX Service Group and Private Communications at a future time, while off the network.

NOTE: This is a "run-time" requirement applicable to an already configured MCX UE, when MCX Service Groups and/or MCX Users, in addition to what was already configured, need to participate in future off-network communications.

5.1.4 Identification

[R-5.1.4-001] The MCX Service shall support identifiers using character sets for international languages specified via configuration.

5.1.5 Membership/affiliation

[R-5.1.5-001] The MCX Service shall provide a mechanism by which an MCX User determines the currently defined MCX Service Groups for which the MCX User is authorized.

[R-5.1.5-002] The MCX Service shall provide a mechanism by which an MCX UE determines the currently defined MCX Service Groups for which it is authorized.

[R-5.1.5-003] The MCX Service shall support an MCX User's ability to affiliate to one or more MCX Service Groups.

[R-5.1.5-004] The MCX Service shall provide a mechanism for an MCX Service Administrator to limit the total number (Nc2) of MCX Service Groups that an MCX User can be affiliated to simultaneously.

[R-5.1.5-005] An MCX User may simultaneously be an MCX Service Group Member of one or more MCX Service Groups.

[R-5.1.5-006] The MCX Service shall provide a mechanism for an MCX Service Group Member to select zero or one Selected MCX Service Group.

[R-5.1.5-007] The MCX Service shall require that MCX Users affiliate with MCX Service Groups prior to participation in the communications of those groups.

[R-5.1.5-008] An MCX User shall be able to affiliate with a multiplicity of MCX Service Groups, subject to restrictions configured by the MCX Service Administrator.

5.1.6 Group Communication administration

[R-5.1.6-001] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure the maximum duration for MCX Service Group Communications for MCX Users within their authority.

5.1.7 Prioritization

[R-5.1.7-001] The MCX Service shall provide a mechanism to organize MCX Service Groups into a hierarchy(ies).

[R-5.1.7-002] The MCX Service shall provide a mechanism to prioritize MCX Service Group Communications based on the priorities associated with elements of the communication (e.g., service type, requesting identity, and target identity).

5.1.8 Charging requirements for MCX Service

[R-5.1.8-001] The MCX Service shall support charging for MCX Service Group Communications.

[R-5.1.8-002] Void

[R-5.1.8-003] The MCX Service shall support time-of-day sensitive charging based on actual resource utilization, provided QoS and provided priority.

[R-5.1.8-004] The MCX Service shall generate charging data that identifies the device(s) involved in a communication.

[R-5.1.8-005] The MCX Service shall support confidentiality of the charging between the service provider and the network operator.

[R-5.1.8-006] The MCX Service shall support confidentiality of the identity of the Mission Critical Organization.

[R-5.1.8-007] The MCX Service shall support reconciliation of the charging records between the service provider and the network operator.

[R-5.1.8-008] The MCX Service shall support offline charging.

[R-5.1.8-009] The MCX Service shall support online charging.

[R-5.1.8-010] The MCX Service shall be able to generate charging data for on-network mode.

[R-5.1.8-011] The MCX Service shall be able to generate charging data for off-network mode.

5.1.9 MCX Service Emergency Alert triggered by Location

[R-5.1.9-001] The MCX Service shall provide a mechanism for an MCX Service Emergency Alert to be triggered when an MCX UE moves into a predefined area.

[R-5.1.9-002] The MCX Service shall provide a mechanism for an MCX Service Emergency Alert to be cancelled when the MCX UE moves out of a predefined area or to remain active until cancelled by the MCX User.

5.2 Broadcast Group

5.2.1 General Broadcast Group Communication

[R-5.2.1-001] The MCX Service shall support Broadcast Group Communications within that MCX Service from authorized MCX Service Group Members as determined by the MCX Service Administrator.

[R-5.2.1-002] The MCX Service shall only allow the initiating MCX Service Group Member to transmit on a Broadcast Group Communication, unless overridden (e.g., by a supervisor).

5.2.2 Group-Broadcast Group (e.g., announcement group)

[R-5.2.2-001] The MCX Service shall provide for the creation of Group-Broadcast Groups within that MCX Service with up to Bc1 levels of group hierarchy.

[R-5.2.2-002] The MCX Service shall be configurable to create a Group-Broadcast Group from one or more Group-Broadcast Groups within that MCX Service with any other non-Broadcast Group from the same MCX Service.

[R-5.2.2-003] The MCX Service shall enable an MCX Service Administrator to create a Group-Broadcast Group.

[R-5.2.2-004] A Broadcast Group Communication transmitted on a Group-Broadcast Group shall have priority over Group Communications on its subordinate groups from the same MCX Service.

5.2.3 User-Broadcast Group (e.g., System Communication)

[R-5.2.3-001] The MCX Service shall provide for the creation of User-Broadcast Groups within that MCX Service with up to Bc2 levels of user hierarchy.

[R-5.2.3-002] A Broadcast Group Communication transmitted on a User-Broadcast Group shall have priority over Group Communications from the same MCX Service involving users within the user hierarchy.

5.3 Late communication entry

[R-5.3-001] The MCX Service shall provide a mechanism by which an Affiliated MCX Service Group Member can join an on-going MCX Service Group Communication.

[R-5.3-002] The MCX Service shall provide the identities of the transmitting MCX Service Group Member, and of the MCX Service Group and, if available, the aliases of the transmitting MCX Service Group Member and the identity of the Mission Critical Organization to the MCX UEs that enter the communication late.

[R-5.3-003] The MCX Service shall provide the transmitting MCX Service Group Member's Location information to MCX UEs that are late entering a communication in progress, subject to permissions.

[R-5.3-004] If an MCX Service Group Communication proceeds without all Affiliated MCX Service Group Members (e.g., due to one or more members being temporarily out of coverage during the communication setup or in one or more higher priority communications), the MCX Service shall attempt to add those affiliated members as the communication proceeds and they become available.

[R-5.3-005] If during an on-going MCX Service Group Communication, additional MCX Service Group Members affiliate with the MCX Service Group, the MCX Service shall add those members to the Group Communication.

5.4 Receiving from multiple MCX Service communications

5.4.1 Overview

MCX Users receive communications traffic of their affiliated MCX Service Groups. This multiple receiving, called monitoring by some organizations, provides MCX Users current information about police, fire or critical medical events that are occurring within their jurisdictions. This is useful for dispatchers or those that might not be the primary support for that event at that moment. The information gained by monitoring might be useful for the dispatcher to determine any actions to take or be useful later if the MCX User is deployed to provide additional support for that event. The MCX User might be assigned to support the activities of more than one MCX Service Group on the same shift. This means that the MCX User receives multiple MCX Service Groups.

An MCX User with limited resources (e.g., a handheld UE) might find that using concurrent received MCX Service communications from multiple active MCX Service Groups becomes confusing. During periods of time when the MCX User is receiving communications from multiple MCX Service Groups, which MCX Service Group's communication is presented to the MCX User is determined by the MCX User's choice, the priority associated with the sender of the Selected MCX Service Group, other considerations or combinations of these. The MCX UE is aware of all the active groups to which the MCX User has affiliated and which is the selected group (if any). The identities of the other active receiving groups can be made available for display on the MCX UE. When the receive activity from the Selected MCX Service Group stops, the MCX UE might present the communications from another group per the MCX User's choice or by other means.

If none of the multiple groups to which the MCX User has affiliated or selected is active, the MCX UE would continue to monitor for activity by any of the multiple affiliated or Selected MCX Service Groups. Monitoring for activity of multiple MCX Service Groups is also known as scanning and the list of the multiple groups is also known as a scan list.

5.4.2 Requirements

[R-5.4.2-001] The MCX Service shall allow an MCX UE to be receiving or transmitting in one MCX Service Group while simultaneously receiving additional MCX Service Groups.

[R-5.4.2-002] The MCX Service shall provide a mechanism to configure the number (Nc4) of MCX Service Group Communications to be simultaneously received by an MCX UE, authorized by an MCX Service Administrator and/or authorized user.

[R-5.4.2-003] The MCX Service shall provide a mechanism to configure the number (Nc5) of MCX Service Group Communications to be simultaneously received by an MCX User, authorized by an MCX Service Administrator and/or authorized user.

[R-5.4.2-004] The MCX Service shall provide a mechanism for an MCX Service Administrator and/or authorized user to prioritize the order in which communications on multiple MCX Service Groupss within an MCX Service User Profile are presented by the MCX user's MCX UE.

[R-5.4.2-005] The MCX Service shall provide multiple MCX Service User IDs to an MCX UE when multiple MCX Service Groups that have a sender are received by the MCX UE.

[R-5.4.2-006] The MCX Service shall allow an authorized MCX UE to receive on-network MCX Service Group and off-network MCX Service Group Communications simultaneously.

[R-5.4.2-007] The MCX Service shall ensure that if there is an MCX Service Emergency Group Communication on one of the MCX Service Groups that an MCX User is affiliated to, but that user is already in a lower priority MCX Service Group Communication or Private Communication, that the MCX User automatically hears/displays the MCX Service Emergency Group Communication.

[R-5.4.2-008] The MCX Service shall support reception and recording of multiple concurrent Private Communications by an authorized user (e.g., dispatch operator).

[R-5.4.2-009] The MCX Service shall provide a mechanism by which an MCX UE can receive and record multiple concurrent Private Communications from MCX users for which the current MCX User is authorized.

5.5 Private Communication

5.5.1 Private Communication general requirements

[R-5.5.1-001] The MCX Service shall provide a mechanism for a dispatcher or authorized user to configure which content source shall be able to send the content to an MCX User (e.g. video cameras near an incident).

5.5.2 Charging requirements for MCX Service

[R-5.5.2-001] The MCX Service shall support charging for Private Communications.

5.6 MCX Service priority requirements

5.6.1 Overview

MCX Service Emergency Group Communications and MCX Service Imminent Peril Group Communications are MCX Service Group Communications that provide the MCX User elevated priority towards obtaining resources of the MCX Service system. The MCX Service Emergency Private Communication similarly provides elevated priority to resources of the MCX Service system. The MCX Service Emergency Alert provides a notification of an MCX Service Emergency situation from an MCX UE, regardless if the MCX User is signed in with the MCX Service or not.

The MCX Service Emergency Alert is initiated from an MCX UE to inform the MCX Service of the MCX User's immediate need of assistance due to the MCX User's personal, life-threatening situation. If the MCX User is not properly authenticated, he/she is treated as a temporary MCX User with limited permissions. The MCX User initiates this notification by actuating an MCX User interface on the MCX UE. The notification to the MCX Service includes the MCX User's ID, potentially an MCX Service Group ID, the user's Mission Critical Organization name and the most current location available for the user's MCX UE.

The MCX Service User Profile/group configuration determines which MCX Service Group ID is used, if any. If the MCX Service User Profile indicates that a dedicated (i.e., not used for everyday traffic) MCX Service Emergency Group is to be used, then the MCX Service Emergency communication traffic moves to a different group. MCX Users that support MCX Service Emergency situations monitor the dedicated MCX Service Emergency Group(s) for communications activity. If the MCX Service User Profile indicates that the Selected MCX Service Group is to be used, then its MCX Service Group ID is used, unless no group is selected for transmissions.

After the MCX User has initiated an MCX Service Emergency Alert, MCX Service Emergency Private Communication or MCX Service Emergency Group Communication, the MCX User is considered to be in the MCX Service Emergency State. The user remains in the MCX Service Emergency State until the MCX User cancels the MCX Service Emergency State.

An MCX Service Group Communication started by an MCX User while in the MCX Service Emergency State or previously started but followed by an MCX Service Emergency Alert becomes an MCX Service Emergency Group Communication. The MCX Service Group ID used for the MCX Service Emergency Group Communication is the same MCX Service Group ID included in the MCX Service Emergency Alert. An MCX User or dispatcher might initiate an MCX Service Emergency Group Communication without an MCX Service Emergency Alert. The start of an MCX Service Emergency Group Communication starts an In-progress Emergency condition for the MCX Service Group. Any subsequent MCX Service Group Communications made by any MCX Service Group Member of an MCX Service Group, which has an In-progress Emergency, is treated as an MCX Service Emergency Group Communication. MCX Service Emergency Group Priority is removed when the In-progress Emergency for the group is cancelled.

An MCX Service Private Communication started by an MCX User while in the MCX Service Emergency State becomes an MCX Service Emergency Private Communication.

MCX Service Imminent Peril Group Communications are differentiated from MCX Service Emergency Group Communications based on for whom the assistance is required. The MCX Service Emergency Group Communication is initiated by an MCX User for assistance for the MCX Service Emergency condition involving that user. An MCX Service Imminent Peril Group Communication is initiated by an MCX User for assistance to other MCX Users or persons of the general public observed to be in trouble and may soon need assistance.

There is no MCX Service Imminent Peril Alert and no MCX Service Imminent Peril State for MCX Users. The granting of an MCX Service Imminent Peril Group Communication starts an In-progress Imminent Peril condition for the MCX Service Group. Any subsequent MCX Service Group Communication made by any MCX Service Group

Member of an MCX Service Group that has an In-progress Imminent Peril condition is treated as an MCX Service Imminent Peril Group Communication. MCX Service Imminent Peril Group Priority is removed when the In-progress Imminent Peril for the group is cancelled.

5.6.2 Communication types based on priorities

5.6.2.1 MCX Service Emergency and Imminent Peril general requirements

5.6.2.1.1 Overview

Emergency Group Communication and Imminent Peril Group Communication are MCX Service Group Communications that provide the MCX User elevated priority towards obtaining resources of the MCX Service system. The MCX Service Emergency Alert provides a notification of an MCX Service Emergency situation from an MCX UE, regardless if the user is signed in with the MCX Service or not. The MCX Service Emergency Alert is initiated from an MCX UE to inform the MCX Service of the user's immediate need of assistance due to the user's personal, life-threatening situation.

When multiple MCX Services are active in an MCX UE, the interaction of these features between the services needs to be considered. When an MCX User initiates an Emergency Group Communication, he/she may only want a subset of the active MCX Services to have emergency priority. Likewise, for Imminent Peril the North American user requirement is that only the active MCX Service receives Imminent Peril priority when the Imminent Peril condition is initiated. For example, if the MCX User is transmitting a video when he/she initiates Imminent Peril, then only the MCVideo service will be granted elevated priority.

5.6.2.1.2 Requirements

[R-5.6.2.1.2-001] When an MCX User initiates an MCX Service Emergency Group Communication, a subset of MCX Service applications (e.g. MCPTT, MCVideo) relevant to the MCX User and configured for the MCX Service Group, shall be used for MCX Service Emergency Group Communications.

[R-5.6.2.1.2-002] The MCX Service shall support an MCX Service Emergency Alert, which on initiation by an MCX User shall put that MCX User into the MCX Service Emergency State and cause that MCX UE to send an MCX Service Emergency Alert containing the following information: Location, MCX Service User ID, the user's Mission Critical Organization name, the list of notification IDs (e.g. groups, other users), and the list of application service MCX Service Group IDs to be used for MCX Service Emergency Group Communication (i.e., user's selected group or dedicated MCX Service Emergency Group).

[R-5.6.2.1.2-003] The MCX Service in the UE shall request Imminent Peril priority for the currently active MCX Service Application (e.g. MCPTT, MCVideo) when the MCX User requests an MCX Service Imminent Peril Group Communication.

[R-5.6.2.1.2-004] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure which MCX Service Applications (e.g. MCPTT, MCVideo) are used for MCX Service Emergency Group Communications by an MCX User when that user is in an MCX Service Emergency State.

[R-5.6.2.1.2-005] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure which MCX Service Applications (e.g. MCPTT, MCVideo) can be used for Imminent Peril Group Communication.

5.6.2.2 MCX Service Emergency Group Communication

5.6.2.2.1 MCX Service Emergency Group Communication requirements

[R-5.6.2.2.1-001] The MCX Service shall support MCX Service Emergency Group Communications from an authorized MCX Group Member on the currently Selected MCX Group or on an MCX Group designated for MCX Service Emergency Group Communications.

[R-5.6.2.2.1-002] When an MCX User initiates an MCX Service Emergency Group Communication this may trigger an MCX Service Emergency Alert for that MCX User.

[R-5.6.2.2.1-003] When an MCX User initiates an MCX Service Emergency Group Communication this shall put that MCX User into an MCX Service Emergency State.

[R-5.6.2.2.1-004] The MCX Service shall ensure that MCX Service Emergency Group Communications have the highest priority over all other MCX Service Group transmissions from the same MCX Service, except MCX Service

System Communications, MCX Service Emergency Private Communications, and other MCX Service Emergency Group Communications.

[R-5.6.2.2.1-005] The MCX Service shall be capable of changing a group communication in progress to an MCX Service Emergency Group Communication.

[R-5.6.2.2.1-006] MCX Service Emergency Group Communications, including their content and signalling, shall have pre-emptive priority over all other types of MCX Service communications from the same MCX Service, except MCX Service System Communications, MCX Emergency Private Communications, and other MCX Service Emergency Group Communications.

[R-5.6.2.2.1-007] The MCX Service shall provide the MCX Service User ID of the initiator of an MCX Service Emergency Group Communication and an indication that it is an MCX Service Emergency Group Communication to Affiliated MCX Service Group Members.

[R-5.6.2.2.1-008] The MCX Service shall add the MCX Service Emergency priority to the group when an In-progress Emergency on that group is initiated.

[R-5.6.2.2.1-009] The MCX Service shall remove the MCX Service Emergency Priority associated with the group when an In-progress Emergency on that group is cancelled.

Editor's Note: The interaction of MCX Service Emergency Communication and Imminent Peril Communication is FFS.

[R-5.6.2.2.1-010] The Affiliated MCX Service Group Members shall be notified when their group communication transitions to an In-progress Emergency.

[R-5.6.2.2.1-011] The MCX Service shall maintain knowledge of the Affiliated MCX Service Group Member(s) that initiated the MCX Service Emergency Group Communication(s) until the In-progress Emergency is cancelled.

[R-5.6.2.2.1-012] The MCX Service shall maintain an In-progress Emergency condition for a group from the time the initial MCX Service Emergency Group Communication was requested until the In-progress Emergency condition is cancelled.

[R-5.6.2.2.1-013] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure which MCX Service Group (i.e., user's selected group or dedicated MCX Service Emergency Group) is used for the MCX Service Emergency Group Communication by an MCX User.

[R-5.6.2.2.1-014] While In-progress Emergency status is maintained for an MCX Service Group Communication, the MCX Service shall provide the MCX Service User ID of the initiator of the In-progress Emergency status and an indication that it is an MCX Service Emergency Group Communication to existing and Late communication entry Affiliated MCX Service Group Members.

5.6.2.2.2 MCX Service Emergency Group Communication cancellation requirements

[R-5.6.2.2.2-001] The MCX Service shall support cancellation of an In-progress Emergency by an authorized MCX User for an MCX Service Group.

[R-5.6.2.2.2-002] The MCX Service shall support cancellation of an In-progress Emergency for an MCX Service Group when criteria established by the MCX Service Administrator are met (e.g., timeout).

[R-5.6.2.2.2-003] The MCX Service shall support cancellation of an In-progress Emergency for an MCX Service Group and MCX Service Emergency State for an MCX User by the MCX Service Emergency Group Communication initiator.

[R-5.6.2.2.2-004] The MCX Service shall notify Affiliated MCX Service Group Members of the cancellation of the In-progress Emergency and the identity of the cancelling MCX User.

[R-5.6.2.2.2-005] The MCX Service shall provide a mechanism for an MCX Service Administrator to authorize an MCX User to cancel in-progress Emergencies.

5.6.2.3 MCX Service Imminent Peril Group Communication

5.6.2.3.1 MCX Service Imminent Peril Group Communication requirements

[R-5.6.2.3.1-001] The MCX Service shall support Imminent Peril group communications from authorized Affiliated MCX Service Group Members.

[R-5.6.2.3.1-002] The MCX Service (e.g. MCPTT, MCVideo) shall ensure that MCX Service Imminent Peril group communications have priority over all other MCX Service Group transmissions from the same MCX Service, except MCX Service System Communications, MCX Service Emergency Group Communications, MCX Service Emergency Private Communications, and other MCX Service Imminent Peril group communications.

[R-5.6.2.3.1-003] The MCX Service shall be capable of changing an MCX Service Group communication in progress to an Imminent Peril group communication.

[R-5.6.2.3.1-004] MCX Service Imminent Peril group communications, including their content and signalling, shall have pre-emptive priority over all other types of MCX Service communications from the same MCX Service, except MCX Service Emergency Group Communications, MCX Service Emergency Private Communications, MCX Service System Communications, and other MCX Service Imminent Peril group communications.

[R-5.6.2.3.1-005] The Affiliated MCX Service Group Members shall be notified when an MCX Service Group communications transitions to In-progress Imminent Peril status.

[R-5.6.2.3.1-006] While Imminent Peril status is maintained for an MCX Service Group communications, the MCX Service shall provide the MCX Service User ID of the initiator of the Imminent Peril status and an indication that it is an Imminent Peril group communication to existing and Late communication entry Affiliated MCX Service Group Members.

[R-5.6.2.3.1-007] The MCX Service shall add the Imminent Peril priority to the group when an In-progress Imminent Peril on that group is initiated.

[R-5.6.2.3.1-008] The MCX Service shall remove the Imminent Peril priority associated with the MCX Service Group when the In-progress Imminent Peril status of that MCX Service Group is cancelled.

Editor's note: The interaction of MCX Service Emergency Communication and Imminent Peril Communication is FFS.

[R-5.6.2.3.1-009] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure which MCX Service Group (i.e., user's selected group or dedicated imminent peril group) shall be used for the Imminent Peril communications for an MCX User.

5.6.2.3.2 MCX Service Imminent Peril Group Communication cancellation requirements

[R-5.6.2.3.2-001] The MCX Service shall support cancellation of an In-progress Imminent Peril by an authorized MCX User.

[R-5.6.2.3.2-002] The MCX Service shall provide a mechanism for an MCX Service Administrator to authorize MCX Service Users to cancel an In-progress Imminent Peril.

[R-5.6.2.3.2-003] The MCX Service shall support cancellation of an In-progress Imminent Peril by the Imminent Peril group communication initiator.

[R-5.6.2.3.2-004] The MCX Service shall support cancellation of an In-progress Imminent Peril when criteria created by the MCX Service Administrator are met.

5.6.2.4 MCX Service Emergency Alert

5.6.2.4.1 MCX Service Emergency Alert requirements

[R-5.6.2.4.1-001] The MCX Service shall support an MCX Service Emergency Alert capability, which on initiation by an MCX User shall put that MCX User into the MCX Service Emergency State and cause that MCX UE to send an MCX Service Emergency Alert.

[R-5.6.2.4.1-002] The MCX Service shall provide a means for an authorized user to be able to activate the MCX Service Emergency Alert capability.

[R-5.6.2.4.1-003] The MCX Service Emergency Alert shall contain the following information: Location, MCX Service User ID and MCX Service Group ID (i.e., user's selected group or dedicated MCX Service Emergency Group, as per group configuration) and the user's Mission Critical Organization name.

[R-5.6.2.4.1-004] The MCX Service Emergency Alert shall be distributed to affiliated members of the group that was used in the MCX Service Emergency Alert.

[R-5.6.2.4.1-004a] For an MCX Service Emergency Private Communication the MCX Service Emergency Alert shall be distributed to the MCX User that the communication was initiated to.

[R-5.6.2.4.1-005] The MCX Service shall provide a mechanism for an authorized MCX User to configure an MCX Service Emergency Alert to send a notification to MCX Users within a configurable geographic area of the MCX User entering the MCX Service Emergency State, independent of the MCX Service Group Membership.

[R-5.6.2.4.1-006] The MCX UE shall maintain knowledge of the MCX Service Emergency State, until cancelled.

[R-5.6.2.4.1-007] Until the MCX Service Emergency State is cancelled on the MCX UE, all MCX Service Group communications or Private Communications transmissions by the MCX User shall be an MCX Service Emergency Group Communication or Emergency Private Communication.

[R-5.6.2.4.1-008] The MCX UE shall be configurable as to which group (i.e., user's selected group or dedicated MCX Service Emergency Group) or MCX User is used for the MCX Service Emergency communications.

[R-5.6.2.4.1-009] The MCX UE shall immediately affiliate to the group configured for MCX Service Emergency Group Communication, if not already affiliated to the group, after activating an MCX Service Emergency Alert.

[R-5.6.2.4.1-010] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure how an MCX User is notified of an incoming MCX Service Emergency Alert (e.g., visual, audio).

[R-5.6.2.4.1-011] The MCX Service shall provide a mechanism for an MCX User to configure, subject to MCX Service Policy, how they are notified of an incoming MCX Service Emergency Alert (e.g., visual, audio).

[R-5.6.2.4.1-012] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure which MCX Service Group (i.e., user's selected group or dedicated MCX Service Emergency Group) or MCX User (e.g., dispatcher) is used for the MCX Service Emergency Alert by an MCX User.

5.6.2.4.2 MCX Service Emergency Alert cancellation requirements

[R-5.6.2.4.2-001] The MCX UE shall only provide a means for cancelling the MCX Service Emergency State locally by an authorized user of that MCX UE.

[R-5.6.2.4.2-002] The MCX Service shall support MCX Service Emergency Alert cancellation by authorized MCX Users.

[R-5.6.2.4.2-003] The MCX Service shall distribute MCX Service Emergency Alert cancellation to all affiliated members of the group identified in the cancellation.

5.7 MCX Service User ID

[R-5.7-001] The MCX Service shall provide a mechanism for the creation and deletion of aliases for an MCX User and its associated MCX Service User Profiles by authorized parties.

[R-5.7-002] The MCX Service shall provide a mechanism for each MCX Service User ID to be associated with an alphanumeric identifier (with a minimum length of Nc3) (i.e., alias) assigned by an MCX Service Administrator.

[R-5.7-003] All UEs shall provide a configurable capability to display the MCX Service User ID, aliases associated with the MCX Service User ID, with the Selected MCX Service Group, and with the Mission Critical Organization name.

5.8 MCX UE management

[R-5.8-001] An MCX UE shall support one or more MCX Service User Profiles.

[R-5.8-002] The MCX Service shall provide a mechanism for an MCX Service Administrator and/or authorized MCX User to perform MCX UE Provisioning.

5.9 MCX Service User Profile

[R-5.9-001] The MCX Service shall ensure that each MCX User has at least one associated MCX Service User Profile that records the MCX User's: information, including permissions and privileges with respect to the MCX Service.

NOTE: Examples of profile information include: their MCX Service User ID, which MCX Service Groups they are a member of, their Participant type, which authority they belong to, whether they can make/receive Private Communications.

[R-5.9-002] The MCX Service shall provide a means for an MCX Service Administrator to manage the MCX Service User Profile for MCX Users within their authority.

5.9a Functional alias

5.9a.1 Overview

A functional alias is a user selectable alias that is tied to the assignment or task of the user. A MCX User can activate one or multiple functional aliases at the same time. A functional alias can be used for communication and for addressing targets of an MCX communication as an alternative to the MCX User ID. The activation of the functional alias(es) will take place after the user has signed in to the MCX Service using the MCX User ID.

The same functional alias can be assigned for use to multiple users depending on MCX Service Administrator settings. A functional alias can be taken over by an authorized MCX User, depending on MCX Service Administrator settings. These two capabilities are mutually exclusive and can not be configured for the same functional alias.

A functional alias can be used to identify for example the driver(s) of a particular train, identified by train number and the role of the user on that train.

Each functional alias that is active on the MCX Service system is unique for addressing purposes. For example, if there are two drivers of TRAIN29 (e.g. DRIVER1_TRAIN29, DRIVER2_TRAIN29), then each active functional alias should be uniquely addressable.

5.9a.2 Requirements

[R-5.9a-001] If the MCX Service system supports functional aliases, then the MCX Service shall provide a mechanism for the MCX User to activate one or more functional alias(es).

[R-5.9a-002] If the MCX Service system supports functional aliases, the MCX User shall be reachable by its functional alias(es).

[R-5.9a-003] If the MCX Service system supports functional aliases, then the MCX Service shall provide a mechanism for the MCX User to deactivate a functional alias.

[R-5.9a-004] If the MCX Service system supports functional aliases, then the MCX Service shall upon request provide the MCX User a list of functional aliases from which the user can select for activation.

NOTE: The list may contain functional aliases based on a certain context, like location of the MCX User, operational schedule, etc.

[R-5.9a-005] If an MCX Service system supports functional alias, the MCX Service shall provide a mechanism for an MCX Service Administrator to manage functional aliases, and for each functional alias indicate either if it can be simultaneously active for multiple MCX Users up to a per-alias configurable number, or if it is allowed to be taken over by an authorized MCX User, or none of these two options.

[R-5.9a-006] If a MCX User attempts to activate a functional alias that is already active for another MCX User, and not allowed to be simultaneously active for multiple MCX Users or the number of simulateneous MCX Users is reached to the upper limit,, the MCX Service shall inform the MCX User that the functional alias is already in use.

[R-5.9a-007] If a MCX User attempts to activate a functional alias that is already active for at least one other MCX User, and that functional alias is allowed to be simultaneously active for multiple MCX Users and the upper limit of number of simultaneous MCX Users is not reached, the MCX Service shall activate the functional alias for the MCX user and inform all other MCX User(s) with the same functional alias.

[R-5.9a-008] If an authorized MCX User attempts to activate a functional alias that is already used by another MCX User, and that functional alias is allowed to be taken over, and is not indicated for simultaneous activation to multiple MCX Users, the MCX Service shall offer the MCX User to take over the functional alias from the MCX User using the alias.

[R-5.9a-008a] If an authorized MCX User attempts to activate a functional alias that is already active for at least one other MCX User, and the upper limit of number of simultaneous MCX Users is reached, the MCX Service shall reject the MCX User's request.

[R-5.9a-009] If an authorized MCX User takes over the functional alias that is already active for another MCX User, the MCX Service shall activate the functional alias to the MCX User and inform the previous MCX User that the alias has been deactivated.

[R-5.9a-010] If an MCX Service System supports functional alias, the MCX Service shall allow the MCX User to perform an activation of an unlisted functional alias that is defined in the MCX Service system.

[R-5.9a-011] If an MCX Service system supports functional alias, then an authorized MCX User shall be able to interrogate the MCX Service system of the alias(es) active for a certain MCX User.

[R-5.9a-012] If an MCX Service system supports functional alias, the MCX Service shall provide a mechanism for an MCX Service Administrator to authorize a MCX User to take over a functional alias.

[R-5.9a-013] If an MCX Service system supports functional alias, the MCX Service shall provide a mechanism for an MCX Service Administrator to authorize a MCX User to interrogate the MCX Service system of the alias(es) active for a certain MCX User.

5.10 Support for multiple devices

[R-5.10-001] The MCX Service shall allow an MCX User to log in to multiple MCX UEs concurrently.

[R-5.10-002] The MCX Service shall ensure that the MCX User logs into each MCX UE separately.

5.11 Location

[R-5.11-001] The MCX Service shall support obtaining and conveying Location information describing the position of the MCX UE.

[R-5.11-002] The MCX Service should support obtaining and conveying high accuracy Location information describing the position of the MCX UE.

[R-5.11-003] The MCX Service shall provide for the flexibility to convey future formats of Location information.

[R-5.11-004] The MCX Service shall provide a means for MCX Service Administrators to manage the privacy of Location information for MCX Users within their authority.

[R-5.11-005] An authorized MCX User shall be able to control the supplying of Location information by the MCX UE for MCX Service communications.

[R-5.11-006] The conveyed Location information shall be the most recently obtained information about the position of the MCX UE at the time of the Location information conveyance.

[R-5.11-007] The MCX Service shall be capable of configuring and re-configuring one or more Location information update triggers (i.e., identified conditions that, when satisfied, cause the MCX UE to report its current Location information).

[R-5.11-008] The MCX Service shall be able to modify Location information update triggers of an MCX User while the MCX User is on the network.

[R-5.11-009] The MCX Service shall provide a means for an MCX UE to send a Location information update whenever a trigger condition is satisfied (e.g., initial registration, distance travelled, elapsed time, cell change, tracking area change, PLMN change, MCX Service communication initiation).

[R-5.11-010] The MCX Service shall provide a means for an MCX UE to send a Location information update whenever the MCX User initiates an MCX Service Emergency Alert.

[R-5.11-011] The MCX Service shall provide a means for an MCX UE to send a Location information update whenever the MCX User initiates an MCX Service Emergency Group Communication.

[R-5.11-012] The MCX Service shall provide a means for an MCX UE to send a Location information update if the MCX User is in an MCX Service Emergency State and a configured amount of time has passed since the previous location information update.

[R-5.11-013] The MCX Service shall provide a means for an MCX UE to send a Location information update whenever a trigger condition is satisfied while the MCX User is in MCX Service Emergency State (e.g., initial registration, distance travelled, elapsed time, cell change, tracking area change, PLMN change, MCX Service communication initiation).

NOTE 1: The Location information update triggers for an MCX User in an MCX Service Emergency State might be different than the Location information update triggers used when the MCX User is not in an MCX Service Emergency State.

[R-5.11-014] The MCX Service shall provide a means for an MCX Service Administrator to define geographical areas to be used for Location information update triggers for MCX Users within their authority.

[R-5.11-015] The MCX Service shall provide a means for an MCX UE in a predefined area to send a Location information update whenever a trigger condition configured in an MCX User's active MCX Service User Profile is satisfied (e.g., initial registration, distance travelled, elapsed time, cell change, tracking area change, PLMN change, MCX Service communication initiation).

NOTE 2: The Location information update triggers for an MCX User in a predefined area might be different than the Location information update triggers used when the MCX User is not in a predefined area.

5.12 Security

[R-5.12-001] The MCX Service shall provide a means to support the confidentiality and integrity of all user traffic and signalling at the application layer.

[R-5.12-002] The MCX Service shall support MCX User with globally unique identities, independent of the mobile subscriber identity (IMSI) assigned by a 3GPP network operator to UEs.

[R-5.12-003] The MCX Service identities shall be part of the MCX Service application service domain.

[R-5.12-004] The MCX Service identities shall form the basis of the MCX Service application layer security for the MCX Service.

[R-5.12-005] The MCX Service shall provide the MCX User with a mechanism to perform a single authentication for access to all authorized features.

[R-5.12-006] The MCX Service shall provide a means for an authorized MCX UE to access selected MCX Service features prior to MCX User authentication.

[R-5.12-007] The MCX Service shall require authentication of the MCX User before service access to all authorized MCX Service features is granted.

NOTE: The MCX Service features available are based on the authenticated user identity(s).

[R-5.12-008] Subject to regulatory constraints, the MCX Service shall provide a means to support confidentiality, message integrity, and source authentication for some information exchanges (e.g., MCX Service User Profile management, kill commands) that have the potential to disrupt the operation of the target MCX UE.

[R-5.12-009] The MCX Service shall provide a means to support end-to-end security for all media traffic transmitted between MCX UEs.

[R-5.12-010] End-to-end security shall be supported both within and without network coverage and regardless of whether the traffic is transmitted directly or via the network infrastructure.

[R-5.12-011] Subject to regulatory constraints, the MCX Service shall provide a cryptographic key management service(s).

[R-5.12-012] The cryptographic key management service(s) shall support both pre-provisioning and over-the-air provisioning of cryptographic keys.

[R-5.12-013] The cryptographic key management service(s) shall ensure that cryptographic keys are confidentiality protected, integrity protected and authenticated when delivered over-the-air.

[R-5.12-014] The MCX Service shall provide end-to-end confidentiality and integrity protection to the MCX User Profile when transferred to and/or from and while stored on an MCX Server, an MCX UE or both.

5.13 Media quality

[R-5.13-001] The MCX Service shall have the flexibility to be used with different codecs (audio / video).

5.14 Relay requirements

[R-5.14-001] The MCX Service shall be able to use ProSe Relay capabilities defined in TS 22.278 [5] and TS 22.468 [6].

[R-5.14-002] An MCX UE which is unable to gain service from a 3GPP network should attempt to make use of one or more suitable ProSe UE-to-Network Relay(s) in its proximity (see sub-clause 6.18).

[R-5.14-003] In off-network situations ProSe UE-to-UE Relay functionality shall be supported (see sub-clause 7.15) between MCX UEs.

[R-5.14-004] The MCX Service shall provide a means for an MCX UE in a robot to have a ProSe UE-to-Network Relay capability.

5.15 Gateway requirements

[R-5.15-001] The MCX Service system shall be accessible via gateway MCX UEs by MCX Users.

5.16 Control and management by Mission Critical Organizations

5.16.1 Overview

Clause 5.16 contains general requirements for management of the MCX Service by Mission Critical Organizations sharing the same MCX Service system, and more specific requirements pertaining to management controls and operational visibility, and to management of security services.

5.16.2 General requirements

[R-5.16.2-001] The MCX Service shall be able to support multiple Mission Critical Organizations, each with their own MCX Users and MCX Service Groups, on the same MCX Service system.

[R-5.16.2-002] The MCX Service shall provide a means by which Mission Critical Organizations designate and manage (i.e., add, delete, change authorizations, etc.) MCX Service Administrators with authority to manage users, groups, other MCX Service Administrators, security controls, and other mission affecting parameters (e.g., authorizations and priorities) of the MCX Service.

[R-5.16.2-003] The MCX Service shall protect the operational privacy of Mission Critical Organizations by providing effective separation between the administrative and security management (e.g., key) parameters of those organizations except as authorized by the Mission Critical Organizations involved.

[R-5.16.2-004] The MCX Service shall protect the administrative and security management parameters of Mission Critical Organizations from viewing and manipulation by individuals (including those within and outside of the mission critical organization) not explicitly authorized by the Mission Critical Organization.

[R-5.16.2-005] The MCX Service shall provide a means by which Mission Critical Organizations may share subsets of their administrative and security parameters with other Mission Critical Organizations.

NOTE: The purposes of these requirements protect the operational security of organizations while still allowing for interworking of MCX UE and Users under the control of the Mission Critical Organizations.

5.16.3 Operational visibility for Mission Critical Organizations

[R-5.16.3-001] The MCX Service shall provide a means by which an MCX Service Administrator associated with a Mission Critical Organization has visibility into the operational status of the service (e.g., during a natural disaster).

5.17 General administrative – groups and users

[R-5.17-001] The MCX Service shall provide a mechanism for an MCX Service Administrator to create and define the membership of MCX Service Groups.

[R-5.17-002] The MCX Service shall provide a mechanism for an MCX Service Administrator to authorize a user to request an MCX Service Group Communication to one or more MCX Service Groups.

[R-5.17-003] The MCX Service shall provide a mechanism for an MCX Service Administrator to determine MCX Users who have the role of a particular Participant type on an MCX Service Group.

[R-5.17-004] The MCX Service shall provide mechanisms for an MCX Service Administrator to assign and amend the identifying information of an MCX Service Group (e.g., name, alias).

[R-5.17-005] The MCX Service shall provide a mechanism for an MCX Service Administrator to assign and amend the identifying information of MCX Service User Profiles (e.g., name, identifier, alias).

[R-5.17-006] The MCX Service shall provide a mechanism to notify MCX Users when they become a member of an MCX Service Group or their membership of an MCX Service Group is removed. This notification shall include any provisions required by the MCX User to use the MCX Service Group if the MCX User has been added to the MCX Service Group or remove provisions if the MCX User has been removed from the MCX Service Group.

[R-5.17-007] The MCX Service shall provide mechanisms for an MCX Service Administrator to create, amend, delete, and suspend MCX Service User Profiles.

[R-5.17-008] The MCX Service shall enable an MCX Service Administrator to configure which MCX Service Group Members are authorized to select to transmit to an MCX Service Group.

5.18 Open interfaces for MCX services

5.18.1 Overview

It is expected that data applications such as database access or event managers are or will be, enhanced thanks to the use of multimedia communications. As a consequence, there is a need for external applications to securely access and use MCX Services.

5.18.2 Requirements

[R-5.18.2-001] The MCX Service shall be securely accessible via an open interface by an external application.

NOTE: Access includes one or more of the following: ability to obtain information on demand or via notification, ability to set parameters, ability to control aspects of the service, and the ability to transmit/receive media to/from the service (e.g. video).

[R-5.18.2-002] The MCX Service shall restrict external access based on MCX Service permissions and authorizations.

[R-5.18.2-003] The open interface for MCX Services shall support control and indication of communication priority.

[R-5.18.2-004] The MCX Service shall be able to authenticate the MCX User connecting to the MCX Service through the open interface.

5.19 Media forwarding

5.19.1 Service description

When receiving any kind of media, a user may need to forward it to another user or to another group, subject to relevant authorization. That is to say to communicate between groups the user has to be a member of both groups. Video, messages, files, and streaming may be forwarded.

5.19.2 Requirements

[R-5.19.2-001] An MCX Service shall provide a mechanism for an authorized MCX User to forward media received within an MCX Group to another MCX User or another MCX Group.

[R-5.19.2-002] An MCX Service shall provide a mechanism for an authorized MCX User to forward media received from an MCX User to another MCX User or to an MCX Group.

[R-5.19.2-003] The MCX Service shall provide a mechanism for a MCX UE (whose current user is authorized) to forward a received real time communication in an MCX Group communication to a Group Broadcast Group.

5.20 Receipt notification

5.20.1 Service description

For an MCX Service such as MCVideo or MCData, a user may want to know when the MCX communication has been delivered and when it has been viewed.

5.20.2 Requirements

[R-5.20.2-001] The MCX Service shall provide a mechanism for the sender of a real time communication to receive a notification that the communication is being received and/or displayed.

5.21 Additional services for MCX Service communications

5.21.1 Remotely initiated MCX Service communication

5.21.1.1 Overview

A Remotely initiated MCX Communication is a feature that allows an authorized user, typically a dispatcher, to cause a remote MCX UE to initiate a communication by itself, without its user explicitly initiating the communication by depressing the MCX switch. The purpose of this feature allows the dispatcher to listen to activities at the Location of the remote MCX UE to find out what is happening around that MCX UE. This feature is also known as "Remote Unit Monitoring" in P25 systems.

5.21.1.2 Requirements

[R-5.21.1.2-001] The MCX Service shall provide a mechanism for an authorized MCX User (e.g. dispatch operator) to remotely initiate an MCX Service Private Communication or MCX Service Group Communication from another user’s MCX UE.

[R-5.21.1.2-002] The MCX Service shall provide a mechanism for an authorized MCX User (e.g. dispatch operator) to request remote activation of an MCX Service Group Communication from another user’s (e.g. officer in the field with wearable camera) MCX UE.

[R-5.21.1.2-003] The MCX Service shall provide a mechanism for an authorized MCX User (e.g. officer in the field with wearable camera) to accept or deny access to an MCX Service Group Communication from their MCX UE.

[R-5.21.1.2-004] The MCX Service shall provide a mechanism for an MCX User to request an authorized MCX User (e.g., a dispatcher) to send an MCX Communication (e.g., video or data) to the MCX UE (downlink pull).

NOTE: A video could be stored on the MCX UE or taken on line by the camera.

5.21.2 Remotely terminated MCX Service communication

5.21.2.1 Requirements

[R-5.21.2.1-001] The MCX Service shall provide a mechanism for an authorized MCX User (e.g. dispatch operator) to remotely terminate an MCX Service Private Communication or MCX Service Group Communication from another user’s MCX UE.

6 MCX Service requirements specific to on-network use

6.1 General administrative – groups and users

[R-6.1-001] The MCX Service shall provide a mechanism for an MCX Service Administrator to limit the total number (Nc6) of MCX Service Group Members of an MCX Service Group.

[R-6.1-002] The MCX Service shall provide a mechanism for an MCX Service Administrator to remove MCX Service Groups from the MCX Service system.

[R-6.1-003] The MCX Service shall provide a mechanism for an MCX Service Administrator to disable and re-enable MCX Service Groups.

[R-6.1-004] The MCX Service shall provide a mechanism to log MCX Service Administrators' activities (e.g., cryptographic key updates, MCX Service User Profile changes, password changes, invalid access attempts).

[R-6.1-005] The MCX Service shall provide a mechanism for an MCX Service Administrator to define geographic areas that can be associated to dispatchers for the purpose of routing Location dependent communications and alerts, as part of handling MCX Service Private Communication requests and MCX Service Group Communications, when the receiving/alerted party is based on the MCX User's current Location.

6.2 MCX Service communications

6.2.1 Notification and acknowledgement for MCX Service Group Communications

[R-6.2.1-001] The MCX Service shall be capable of allowing an MCX Service Group Communication to proceed without prior acknowledgement by any MCX User of that MCX Service Group.

[R-6.2.1-002] The MCX Service shall provide a notification and acknowledgement function for an MCX User currently affiliated to an MCX Service Group to acknowledge receipt of an MCX Service Group Communication, if configured to do so.

[R-6.2.1-003] The MCX User's acknowledgement may require direct interaction of the MCX UE with the human user, or may be automatically executed by the MCX UE, in accordance with policy established by an MCX Service Administrator.

[R-6.2.1-004] If the MCX Service has knowledge that some affiliated members of a group cannot be Participants in an MCX Service Group Communication, the MCX Service shall provide an indication to the requester that the communication is proceeding without all affiliated members, and shall provide the list of the missing members based on policy established by the MCX Service Administrator.

[R-6.2.1-005] If MCX User(s) are excluded from an MCX Service communication as there is insufficient capacity to support their participation the MCX Service shall notify the MCX User(s) that they have been excluded from the communication for reasons of lack of capacity.

6.2.2 Queuing

[R-6.2.2-001] The MCX Service shall prioritize the transmit request queue based on the type of communication (e.g., group, private), urgency of the communication (e.g., general group, MCX Service Emergency, Imminent Peril), attributes (e.g., priority level) of the MCX Service Group (if a group communication), and attributes (e.g., priority level) of the requesting MCX User.

[R-6.2.2-002] When prioritizing the transmit queue, the MCX Service may assign higher priority to communications of the MCX Service Groups and MCX Users operating within the boundaries of their jurisdictions, if known.

[R-6.2.2-003] When prioritizing the transmit queue, the MCX Service may assign higher priority to communications of the MCX Service Groups and MCX Users during hours of operation or while on duty, if known.

[R-6.2.2-004] The MCX Service shall allow MCX Users with queued requests for permission to transmit to cancel their requests.

[R-6.2.2-005] If an MCX Service Group Communication request to transmit has been queued, the MCX Service shall provide, upon request, that MCX User's current position in the queue.

[R-6.2.2-006] If a request for an MCX Service Group Communication is queued, the MCX Service shall provide an indication to the requester when the communication continues.

6.3 General requirements

[R-6.3-001] A PLMN shall support multiple MCX Service systems.

[R-6.3-002] An MCX Service system shall be capable of providing MCX Services to MCX Users in multiple PLMNs.

[R-6.3-003] The MCX Service shall provide a means by which changes performed by an MCX Service Administrator take effect immediately.

[R-6.3-004] The MCX Service shall provide a means by which changes performed by an MCX Service Administrator take effect at a specified date/time.

6.4 General MCX Service Group Communications

6.4.1 General aspects

[R-6.4.1-001] Interruption to an MCX Service Group Communication shall be minimized when participants move from one area to another.

6.4.2 Group status/information

[R-6.4.2-001] The MCX Service shall provide a mechanism by which an authorized MCX User determines which MCX Service Groups have at least one other MCX User affiliated.

[R-6.4.2-002] The MCX Service shall provide a mechanism by which an authorized MCX UE determines what MCX Service Groups have at least one active receiving member.

[R-6.4.2-003] The MCX Service shall provide a mechanism by which an authorized MCX UE determines that a number (Nc1) of receiving members are present for an MCX Service Group.

[R-6.4.2-004] The MCX Service shall provide a mechanism by which an authorized MCX UE determines that a particular receiving member(s) is present for an MCX Service Group.

[R-6.4.2-005] The MCX Service shall provide a notification, for example audio and/or visual, to a user that there are no members on an MCX Service Group being used/monitored by the user and that the user is the only user affiliated to that MCX Service Group.

[R-6.4.2-006] The MCX Service shall provide a mechanism by which an authorized MCX User can determine which MCX Service Group(s) another MCX User has affiliated to.

[R-6.4.2-007] The MCX Service shall provide a mechanism by which an authorized MCX User can determine which MCX Service Group(s) another MCX User has selected.

6.4.3 Identification

[R-6.4.3-001] The MCX Service shall provide the MCX Service User ID, associated MCX Service User ID alias(es), MCX Service Group ID, group aliases and, if available, the identity of the Mission Critical Organization name of the transmitting Participant to the receiving MCX UEs unless the transmitting Participant's identity is restricted.

[R-6.4.3-002] The MCX Service shall present users with human readable identifiers (with a minimum length of Nc3) for MCX Users (i.e., MCX Service User ID alias(es)) and for the MCX Service Groups (i.e., group alias(es)).

6.4.4 Membership/affiliation

[R-6.4.4-001] The MCX Service shall support automatic affiliation of the MCX UE to a Group-Broadcast Group or User-Broadcast Group within that MCX Service.

[R-6.4.4-002] The MCX Service shall support an MCX User's ability to revoke his affiliation with an MCX Service Group.

6.4.5 Membership/affiliation list

[R-6.4.5-001] The MCX Service shall provide, upon request, the list of currently affiliated members on an MCX Service Group to an authorized user regardless of the user's affiliation.

[R-6.4.5-002] The MCX Service shall provide a mechanism for an MCX Service Administrator to authorize an MCX User to request the list of currently affiliated members on an MCX Service Group regardless of the MCX User's affiliation or group membership.

[R-6.4.5-003] The MCX Service shall provide, upon request, the list of currently affiliated members of an MCX Service Group to an authorized MCX UE.

[R-6.4.5-004] When a list of affiliated members is provided, the list shall reference each member by MCX Service User ID and/or associated aliases.

[R-6.4.5-005] The MCX Service shall provide, upon request, the current list of members of an MCX Service Group to an authorized user.

[R-6.4.5-006] The MCX Service shall provide, upon request, the current list of members of an MCX Service Group to an authorized MCX UE regardless of the MCX UE's membership.

[R-6.4.5-007] The MCX Service shall provide a mechanism for an MCX Service Administrator to authorize an MCX User to request the complete list of members of an MCX Service Group, regardless of the MCX User's membership.

[R-6.4.5-008] When a list of members is provided, the list shall reference each member by MCX Service User ID and/or associated aliases.

6.4.6 Authorized user remotely changes another MCX User's affiliated and/or Selected MCX Service Group(s)

6.4.6.1 Mandatory change

[R-6.4.6.1-001] The MCX Service shall provide a mechanism that allows an authorized MCX User (e.g., dispatcher) to change an on-network MCX User's Selected MCX Service Group(s) and then the MCX Service shall send a notification to the on-network MCX User.

[R-6.4.6.1-002] The MCX Service shall provide a mechanism that allows an authorized MCX User (e.g., dispatcher) to make changes to the group(s) that an on-network MCX User is affiliated to and then the MCX Service shall send a notification to the on-network MCX User.

[R-6.4.6.1-003] The MCX Service shall provide a mechanism that allows an authorized MCX User (e.g., dispatcher) to change multiple other on-network MCX Users' Affiliated MCX Service Group(s) to a specific MCX Service Group, and the MCX Service shall notify this to the on-network MCX Users.

[R-6.4.6.1-004] The MCX Service shall provide a mechanism that allows an authorized MCX User (e.g., dispatcher) to change multiple other on-network MCX Users' Selected MCX Service Group(s) to a specific MCX Service Group, and the MCX Service shall notify this to the on-network MCX Users.

6.4.6.2 Negotiated change

[R-6.4.6.2-001] The MCX Service shall provide a mechanism that allows an authorized MCX User (e.g., dispatcher) to send a notification that proposes that another on-network MCX User should affiliate to a specific MCX Service Group.

[R-6.4.6.2-002] The MCX Service shall provide a mechanism that allows an authorized MCX User (e.g., dispatcher) to send a notification that proposes that multiple other on-network MCX Users should affiliate to a specific MCX Service Group.

[R-6.4.6.2-003] The MCX Service shall provide a mechanism that allows an authorized MCX User (e.g., dispatcher) to send a notification that proposes that another on-network MCX User should select a specific MCX Service Group.

[R-6.4.6.2-004] The MCX Service shall provide a mechanism that allows an authorized MCX User (e.g., dispatcher) to send a notification that proposes that multiple on-network MCX Users should select a specific MCX Service Group.

[R-6.4.6.2-005] The MCX Service shall provide a mechanism to the on-network MCX User to accept or reject a proposed change in selected or affiliated MCX Service Group(s).

[R-6.4.6.2-006] The MCX Service shall provide a notification to the authorized MCX User (e.g., dispatcher) if the change that they proposed to another on-network MCX User(s) affiliated/Selected MCX Service Group was accepted/rejected by the MCX User(s).

6.4.7 Prioritization

[R-6.4.7-001] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of different MCX Service Group Communications with respect to transport.

[R-6.4.7-002] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of different MCX Service Group Communications with respect to presentation.

[R-6.4.7-003] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of MCX Service Groups Communications and other traffic with respect to transport.

[R-6.4.7-004] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of MCX Service Groups Communications and other traffic with respect to presentation.

6.4.8 Relay requirements

[R-6.4.8-001] The MCX UE-to-Network Relay service shall provide on-network MCX Service to MCX UEs not currently connected to the serving network.

6.4.9 Administrative

[R-6.4.9-001] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure the conditions under which MCX Service communications shall be terminated (e.g., last Participant leaving, second last Participant leaving, initiator leaving).

[R-6.4.9-002] The MCX Service shall provide a mechanism for MCX Service Administrators to configure the maximum allowed time duration for MCX Service Group communications to remain active.

[R-6.4.9-003] The MCX Service shall provide a mechanism for an MCX Service Administrator to determine how many MCX Users shall remain participating for MCX Service Group Communications to remain active.

[R-6.4.9-004] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure MCX Service Groups to be receive-only for specified MCX Service Group Members.

[R-6.4.9-005] The MCX Service shall provide a mechanism for an MCX Service Administrator to set the preferred codecs for an MCX Service Group.

[R-6.4.9-006] The MCX Service shall provide a mechanism for an MCX Service Administrator to confine use of an MCX Service Group to MCX Service Group Members in a particular geographic area.

6.5 Broadcast Group

6.5.1 General Broadcast Group Communication

[R-6.5.1-001] The MCX Service shall deliver an on-Network Broadcast Group Communication within that MCX Service to the members of a Broadcast Group who are on-Network, and who may be all of the MCX Service system users, or a subset thereof.

[R-6.5.1-002] The MCX Service shall support Broadcast Group Communications within that MCX Service to a dynamically defined geographic area.

6.5.2 Group-Broadcast Group (e.g., announcement group)

[R-6.5.2-001] The MCX Service shall optionally support termination of all, or a subset of, subordinate group communications within that MCX Service upon initiation of a Broadcast Group Communication transmitted on a Group-Broadcast Group.

6.5.3 User-Broadcast Group (e.g., System Communication)

[R-6.5.3-001] The MCX Service shall optionally support termination of all group communications within that MCX Service that are not MCX Service Emergency Group Communications involving those users within the user hierarchy upon initiation of a Broadcast Group Communication transmitted on a User-Broadcast Group.

6.6 Dynamic group management (i.e., dynamic regrouping)

6.6.1 General dynamic regrouping

[R-6.6.1-001] Group Regroup and User Regroup operations shall be manageable by authorized MCX Users.

[R-6.6.1-002] The temporary group formed by Group Regroup or User Regroup operations shall persist until torn down by an authorized MCX User.

[R-6.6.1-003] The priority of the temporary group formed by a Group Regroup or User Regroup operations shall be established by the creator of the group within bounds established by MCX Service Administrators.

[R-6.6.1-004] The MCX Service shall enable an MCX Service Administrator to grant and to revoke the authorization of an MCX User to be able to perform dynamic regrouping operations.

[R-6.6.1-005] The MCX Service shall enable an MCX Service Administrator to configure whether a temporary group is encrypted.

[R-6.6.1-006] The temporary group formed by Group Regroup or User Regroup operations shall be treated like any other MCX Service Group, except the ability for a temporary group formed by a Group Regroup operation to be included in another Group Regroup operation.

6.6.2 Group regrouping

6.6.2.1 Service description

Group regrouping enables dispatchers or any authorized user to temporarily combine MCX Service Groups. A dispatcher uses group regrouping for different reasons.

Due to an incident in an area it can be necessary to temporarily enable MCX Users from different MCX Service Groups to communicate to each other to coordinate. After the incident the dispatcher cancels the group regrouping and the MCX Users continue with their original configured MCX Service Groups.

During quiet periods control room managers can decide to combine MCX Service Groups and handle their operations and communications with one dispatcher. In the busier period the group regrouping is cancelled and the MCX Service Groups are handled by separate dispatchers.

MCX Service Groups that are being combined in a Group Regroup operation may belong to the same or different MCX servers and may have different security and priority levels, different floor control methods, as well as different operational characteristics (e.g. different call start criteria, different call or session hang timers, different transmit time limits, different override settings, different floor control parameters such as queue depth, queing policy and time-to-live in the queue). However, the newly created temporary MCX Service Group can have only a single security level, priority level, floor control method, and set of operational characteristics. The MCX Service will apply the proper setting of those parameters for the new MCX Service Group.

6.6.2.2 Requirements

[R-6.6.2.2-001] The MCX Service shall provide a means of dynamically combining a multiplicity of groups into a new, temporary group (i.e., to perform a "Group Regroup operation").

[R-6.6.2.2-002] The MCX Service shall notify MCX Users when and how any of their affiliated groups are affected by a Group Regroup operation including notification of modified security, priority, floor control, and other operational characteristics.

[R-6.6.2.2-003] The MCX Service shall provide notification and information to an authorized MCX User if that user is attempting to Group Regroup MCX Service Groups of different security levels, priority levels, and/or floor control methods.

[R-6.6.2.2-004] The MCX Service shall enable an authorized MCX User to set the security level of the Group created from a Group Regroup operation. Where an MCX User does not specify the security level the MCX Service shall default the security level to be set to the lowest security level of the constituent Groups.

[R-6.6.2.2-005] The MCX Service shall notify Affiliated MCX Service Group Members of a constituent MCX Service Group when the security level of the MCX Service Group that they are using lowers as a result of a Group Regroup operation.

[R-6.6.2.2-006] The MCX Service shall enable an authorized MCX User to set the priority level of the group formed from a Group Regroup operation. Where an MCX User does not specify the priority level the MCX Service shall default the priority level to be set to the highest priority level of the constituent Groups.

[R-6.6.2.2-007] Broadcast Groups shall be able to be included in a Group Regroup operation.

[R-6.6.2.2-008] The MCX Service shall enable an authorized MCX User or MCX Service Administrator to configure default settings and rules for the operational characteristics of temporary MCX Service Groups resulting from Group Regroup operations (e.g. call start criteria, hang time).

[R-6.6.2.2-009] The MCX Service shall enable an authorized MCX User to specify the operational characteristics of temporary MCX Service Groups resulting from Group Regroup operations either explicitly, or via pre-defined implicit rules, or via pre-configured default values, or, in case all the constituent Groups have in common the same operational characteristics, to use the common settings.

[R-6.6.2.2-010] The MCX Service shall enable an authorized MCX User to set the floor control method of the Group created from a Group Regroup operation when the Group Regroup includes one or more groups configured for audio cut-in operation. Where an MCX User does not specify the floor control method the MCX Service shall default to using normal floor control for the Group Regroup (i.e. do not use audio cut-in).

6.6.3 Temporary Group-Broadcast Group

[R-6.6.3-001] The MCX Service shall enable an authorized MCX User to create a temporary Group-Broadcast Group from a multiplicity of MCX Service Groups within that MCX Service.

[R-6.6.3-002] The MCX Service shall only allow the creator of the temporary Group-Broadcast Group to transmit on it.

6.6.4 User regrouping

6.6.4.1 Service description

In the operational MCX Service environment, most tasks are covered by standard procedures and communication structures, and MCX Users can easily access the MCX Service Groups to handle their tasks.

Exceptionally it could happen that there is an urgent need for a dedicated set of individual MCX Users to communicate in an MCX Service Group, but that this is not foreseen in the communication structure. This could be due to extreme conditions or due to a cooperation that is outside normal procedures.

User Regrouping enables dispatchers or authorized users to instantaneously provide a dedicated MCX Service Group to these MCX Users to enable the required communication. Depending on configuration the MCX Users could be automatically affiliated to this MCX Service Group. After the operation this MCX Service Group is removed by the dispatcher or authorized user.

6.6.4.2 Requirements

[R-6.6.4.2-001] The MCX Service shall provide a means for combining a multiplicity of MCX Users into a new, temporary group (i.e., to perform a "User Regroup operation").

[R-6.6.4.2-002] The MCX Service shall provide a means for combining a multiplicity of MCX Users into a new, temporary group based on a parameter or a combination of parameters (e.g., particular geographic area, Participant type).

[R-6.6.4.2-003] The MCX Service shall provide a mechanism to preconfigure the parameters for a particular User Regroup operation, such that an authorized MCX User activates this preconfigured User Regroup and communicates with this temporary group with minimal delay.

NOTE: An example of the use of this functionality is for an MCX User to communicate with particular other MCX Users within a predefined radius of the MCX User's Location. This functionality is likely to be for urgent type communications such as MCX Service Emergency Group Communications.

[R-6.6.4.2-004] The MCX Service shall notify MCX Users when they are affected by a User Regroup operation.

[R-6.6.4.2-005] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure whether an MCX Service system shall automatically affiliate the MCX Users included in the temporary group created by the User Regroup operation.

6.7 Private Communication

6.7.1 Overview

Private Communications can use some form of Floor control or not.

6.7.2 General requirements

[R-6.7.2-001] The MCX Service should provide a mechanism for authorized MCX Users to query whether a particular MCX User is present on the network.

[R-6.7.2-002] The MCX Service should provide a mechanism for an MCX Service Administrator to configure which MCX Users, within their authority, are authorized to place a Private Communication (without Floor control).

[R-6.7.2-003] The MCX Service should provide a mechanism for authorized MCX Users to query whether a particular MCX User is capable of participating in a Private Communication.

[R-6.7.2-004] The MCX Service shall provide a mechanism by which an MCX User can make a Private Communication to the local dispatcher based on the MCX User's current Location.

[R-6.7.2-005] The MCX Service shall provide a mechanism for the Private Communication (without Floor control) to be set up with the MCX UE designated by the receiving MCX User to be used for Private Communications (without Floor control) when the receiving MCX User has signed on to the MCX Service with multiple MCX UEs.

6.7.3 Administrative

[R-6.7.3-001] The MCX Service should provide a mechanism for an MCX Service Administrator to configure whether the presence on the network of a particular MCX User is available.

[R-6.7.3-002] The MCX Service should provide a mechanism for an MCX Service Administrator to configure which MCX Users may determine whether a particular MCX User is present on the network.

[R-6.7.3-003] The MCX Service should provide a mechanism for an MCX Service Administrator to configure whether the ability to participate in Private Communications of a particular MCX User is available.

[R-6.7.3-004] The MCX Service should provide a mechanism for an MCX Service Administrator to configure which MCX Users may determine whether a particular MCX User is capable of participating in a Private Communication.

[R-6.7.3-005] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure which MCX Users, within their authority, are authorized to place a Manual Commencement Private Communication (without Floor control).

[R-6.7.3-006] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure which MCX Users, within their authority, are authorized to place an Automatic Commencement Private Communication (without Floor control).

[R-6.7.3-007] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure for a particular authorized MCX User, a set of MCX Users under the same authority to which a Private Communication (without Floor control) can be made.

[R-6.7.3-008] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure the maximum duration for Private Communication for MCX Users within their authority.

NOTE: The maximum duration can be set to infinite.

6.7.4 Prioritization

[R-6.7.4-001] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of Private Communications and Group Communications with respect to transport.

[R-6.7.4-002] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of Private Communications and Group Communications with respect to presentation.

[R-6.7.4-003] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of different Private Communications with respect to transport.

[R-6.7.4-004] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of different Private Communications with respect to presentation.

[R-6.7.4-005] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of Private Communications and other traffic with respect to transport.

[R-6.7.4-006] The MCX Service shall provide a mechanism to establish, dynamically and in real-time, the relative priorities of Private Communications and other traffic with respect to presentation.

[R-6.7.4-007] The MCX Service shall provide a mechanism to prioritize Private Communications based on the priorities associated with elements of the communication (e.g., service type, requesting identity, and target identity).

6.7.5 Private Communication (without Floor control) commencement requirements

[R-6.7.5-001] The MCX Service shall provide a means by which an MCX UE initiates a Private Communication (without Floor control) to any MCX User for which the MCX UE's current MCX User is authorized.

[R-6.7.5-002] The MCX Service shall provide a means by which an MCX User initiates an Automatic Commencement Private Communication (without Floor control) to any MCX User for which the MCX User is authorized.

[R-6.7.5-003] The MCX Service shall provide a means by which the transmitting authorized MCX User is notified the receiving MCX User received the Private Communication (without Floor control) request.

6.7.6 Private Communication (without Floor control) termination

[R-6.7.6-001] The MCX Service shall provide a mechanism for an MCX User to reject a Private Communication (without Floor control).

[R-6.7.6-002] The MCX Service shall provide a means by which an MCX User ends a Private Communication (without Floor control) in which the MCX User is a Participant.

6.8 MCX Service priority requirements

6.8.1 General

[R-6.8.1-001] The MCX Service shall support multiple MCX Service Application priorities, which are mapped to priority levels, based on network operator policy.

[R-6.8.1-002] MCX Service shall support multiple pre-emptive priorities.

[R-6.8.1-003] The MCX Service shall provide a mechanism for MCX Service Administrators to create, a pre-emption hierarchy for MCX Service Group transmissions and their associated users (i.e., to facilitate local management of the service and its resources).

[R-6.8.1-004] The MCX Service shall support MCX Service Groups with the permission to pre-empt other MCX Service communications.

[R-6.8.1-005] In case of resource shortage a communication made to a group with pre-emption permissions shall be given resources to complete this communication by pre-empting lower priority communications.

NOTE: An MCX Service communication that needs the use of pre-emption still needs to satisfy the communication setup requirements.

[R-6.8.1-006] MCX Service shall support queuing and retention by priority.

[R-6.8.1-007] The MCX Service shall provide a mechanism for an MCX Service Administrator to establish the priority hierarchy and characteristics of MCX Service Group transmissions.

[R-6.8.1-008] The MCX Service shall enable an MCX Service Administrator to prioritize MCX Service Groups in relation to other MCX Service Groups (with respect to transport and presentation).

[R-6.8.1-009] The MCX Service shall enable an MCX Service Administrator to set the priority for a subset of a Mission Critical Organization's MCX Service Groups relative to other subsets of a Mission Critical Organization's MCX Service Groups subordinate to the MCX Service Administrator's authority.

[R-6.8.1-010] When determining priority for an MCX Service communication, the MCX Service shall use the MCX User/Participant's attributes (e.g., first/second responder, supervisor, dispatcher, on/off duty) and the MCX Service Group's attributes (e.g., type of group, owning organization of the group, MCX Service Emergency, Imminent Peril).

[R-6.8.1-011] When determining priority for an MCX Service transmission, the MCX Service shall use the MCX User/Participant's attributes (e.g., first/second responder, supervisor, dispatcher, on/off duty) and the MCX Service Group's attributes (e.g., type of group, owning agency of the group, MCX Service Emergency, Imminent Peril).

[R-6.8.1-012] The MCX Service shall provide a means for the attributes used for determining the priority for MCX Users and Groups to influence the Priority and QoS for all MCX UEs associated with the MCX User.

[R-6.8.1-013] Based on the attributes used for determining the priority for MCX Users and Groups, the MCX Service shall provide consistent and deterministic priority for all MCX Users within their Primary MCX Service System.

[R-6.8.1-014] Based on the attributes used for determining the priority for MCX Users and Groups, subject to roaming capabilities and operator agreement, the MCX Service shall provide consistent and deterministic priority for all MCX Users that roam into Partner MCX Service Systems.

[R-6.8.1-015] The MCX Service shall provide a means for an MCX User to monitor the attributes used for determining priority of his/her communications and transmissions.

[R-6.8.1-016] The MCX Service shall provide a means for an authorized MCX User to monitor and affect a change of the attributes used for determining the priority of another MCX User's communications and transmissions.

6.8.2 3GPP system access controls

[R-6.8.2-001] The 3GPP system shall, subject to operator policy, provide a means for the MCX Service to influence the modification of the access parameters used by the network to admit MCX UEs within a defined area.

NOTE: It is believed that the existing UE network access mechanisms could be utilized to meet the above requirement.

6.8.3 3GPP system admission controls

[R-6.8.3-001] The 3GPP system shall, subject to operator policy, provide a means for the MCX Service to influence the selection and/or modification of admission and retention controls for the bearers assigned or about to be assigned to an MCX UE based on the MCX User's and MCX Service Group attributes used for the priority determination.

NOTE: It is believed that the existing 3GPP mechanisms for network priority and QoS could be utilized to meet the above requirement.

6.8.4 3GPP system scheduling controls

[R-6.8.4-001] The 3GPP system shall, subject to operator policy, provide a means for the MCX Service to influence the selection and/or modification of the bearer scheduling controls for the bearers assigned or about to be assigned to an MCX UE based on the MCX User's and MCX Service Group attributes used for the priority determination.

NOTE: It is believed that the existing 3GPP mechanisms for network priority and QoS could be utilized to meet the above requirement.

6.8.5 UE access controls

[R-6.8.5-001] The MCX Service shall allow the MCX UE to temporarily modify selected 3GPP system access parameters, according to configuration established by an MCX Service Administrator in agreement with the operator's policy.

NOTE: It is believed that the existing network access mechanisms, e.g., ACDC (see 3GPP TS 22.011 [7] and 3GPP TS 23.122 [8]), could be utilized to meet the above requirement.

6.8.6 Mobility and load management

6.8.6.1 Mission Critical mobility management according to priority

[R-6.8.6.1-001] A Mission Critical System shall minimize the interruption to an on-going MCX Service communication when the UE transitions its connection to that communication from one network to another, taking into account that priority management is done in the visited Mission Critical System.

[R-6.8.6.1-002] Mobility shall be subject to authorization from home and visited networks consistent with operational priority management mechanisms. The authorization may be pre-negotiated or in an *ad hoc* manner.

6.8.6.2 Load management

[R-6.8.6.2-001] MCX Users shall be able to use dedicated 3GPP networks as well as public 3GPP networks. When possible, private 3GPP networks are preferably used. But public 3GPP networks may be used e.g., when no private 3GPP network coverage is available or for lower priority data flows while under an overloaded private 3GPP network coverage.

[R-6.8.6.2-002] MCX Services shall be able to propose, according to operational priorities and available resources, adjustments in quality of service and delay of communications.

[R-6.8.6.2-003] MCX Services shall be able to propose to request to pre-empt other on-going communications (for communications that can be pre-empted).

[R-6.8.6.2-004] MCX Services shall be able to notify users of actions taken by the dispatcher that result in a change in priority for a data flow.

[R-6.8.6.2-005] MCX Services shall be able to notify users when the network is not able to provide the requested quality of service.

6.8.7 Application layer priorities

6.8.7.1 Overview

Dispatchers from different critical communication organizations access the same networks and network resources. Depending on the event, the priority is given to an organization and/or a group rather than to another. For instance, in case of a fire priority is given to the fire brigades dealing with it, while in case of a criminal arrest priority is given to the police officers in charge of the arrest.

6.8.7.2 Requirements

[R-6.8.7.2-001] The MCX Service system shall be able to give application priorities to each communication according to the event in addition to the priority given according to groups.

[R-6.8.7.2-002] The 3GPP system shall inform the MCX Service system if a new MCX Service communication cannot be set up.

[R-6.8.7.2-003] The MCX Service system shall assign to each communication:

- an application layer pre-emption capability;
- a capability to be pre-empted; and
- an application layer priority value.

[R-6.8.7.2-004] If there are no MCX Service communications with the capability to be pre-empted, the MCX Service communications with the lowest application layer priorities may be terminated, even if the MCX Service communications are set as not pre-emptable.

[R-6.8.7.2-005] There shall be at least 8 and preferably 30 configurable levels of priority.

6.8.8 Communication types based on priorities

6.8.8.1 MCX Service Emergency Group Communication requirements

[R-6.8.8.1-001] The MCX Service shall be capable of requesting increased priority for all Participants of an MCX Service Emergency Group Communication.

[R-6.8.8.1-002] The MCX Service may inform affiliated group members that an MCX Service Emergency Group Communication was requested but resources were not available for the communication to be granted.

[R-6.8.8.1-003] The MCX Service shall provide a mechanism for an MCX Service Emergency Group Communication to transmit to a temporary MCX Service Group created by a preconfigured User Regroup operation.

NOTE: This type of MCX Service Emergency Group Communication could be used by MCX Users who need to communicate urgently to specific other MCX Users within a predefined radius of their current Location.

[R-6.8.8.1-004] The MCX Service shall ensure that if there is an MCX Emergency Group Communication on one of the MCX Groups that an MCX User is affiliated to, but that user is already in a Private Communication, that the MCX User is notified of the MCX Emergency Group Communication. In the case of MCPTT the Emergency Group Communication is immediately connected to the receiving user except when the existing Private Communication is with Floor control.

6.8.8.2 MCX Service Emergency Private Communication requirements

[R-6.8.8.2-001] The MCX Service shall ensure that MCX Emergency Private Communication have the highest priority over all other Private Communications.

[R-6.8.8.2-002] The MCX Service shall be capable of requesting increased priority for the Participants of an MCX Emergency Private Communication.

[R-6.8.8.2-003] The MCX Service shall be capable of changing a Private Communication in progress to an MCX Emergency Private Communication.

[R-6.8.8.2-004] MCX Emergency Private Communications, including their content and signalling, shall have pre-emptive priority over all other types of MCX Service communications, except System Communications, MCX Emergency Group Communications and other MCX Emergency Private Communications.

6.8.8.3 Imminent Peril Group Communication requirements

[R-6.8.8.3-001] The MCX Service shall be capable of requesting increased priority for all Participants of an Imminent Peril group communication.

[R-6.8.8.3-002] The MCX Service shall maintain knowledge of the Affiliated MCX Service Group Member(s) that initiated the Imminent Peril group communication.

[R-6.8.8.3-003] The MCX Service shall maintain an In-progress Imminent Peril condition for a group from the time the initial Imminent Peril group communication was requested until the In-progress Imminent Peril condition is cancelled.

Editor's Note: Whether imminent peril and MCX Service Emergency Group Communications can be generalized is FFS.

6.8.8.4 MCX Service Emergency Alert

6.8.8.4.1 Requirements

[R-6.8.8.4.1-001] The MCX Service may allow MCX UEs that are unauthorized, not registered, or authenticated to activate the MCX Service Emergency Alert capability.

[R-6.8.8.4.1-002] The MCX User shall be notified that the MCX Service Emergency Alert was received by the MCX Service.

[R-6.8.8.4.1-003] The MCX Service shall be configurable on how the user is notified (e.g., visual, audio).

[R-6.8.8.4.1-004] The MCX Service shall maintain knowledge of the MCX Service Emergency State of the MCX UE, until cancelled.

[R-6.8.8.4.1-005] The MCX Service shall inform an MCX UE of active MCX Service Emergency Alerts after successful registration/authentication with the MCX Service.

[R-6.8.8.4.1-006] The MCX Service shall provide a mechanism for an MCX Service Emergency Alert to transmit to a temporary MCX Service Group created by a preconfigured User Regroup operation.

NOTE: This type of MCX Service Emergency Alert could be used by MCX Users who need to communicate urgently to specific other MCX Users within a predefined radius of their current Location.

6.8.8.4.2 MCX Service Emergency Alert cancellation requirements

[R-6.8.8.4.2-001] The MCX Service shall allow authorized users to cancel any MCX UE's MCX Service Emergency Alert from the system.

[R-6.8.8.4.2-002] The MCX Service shall provide a mechanism for an MCX Service Administrator to authorize a user to cancel, from the system, an MCX Service Emergency Alert initiated by another MCX User.

6.9 IDs and aliases

[R-6.9-001] The MCX Service shall provide a mechanism for permanent and temporary assignment of IDs and aliases.

[R-6.9-002] The MCX Service shall provide a mechanism for the enforcement of uniqueness of IDs and aliases.

[R-6.9-003] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure IDs and aliases.

[R-6.9-004] The MCX Service shall provide the MCX Service User ID and /or associated aliases, the identity of the Selected MCX Service Group, and, if available, the identity of the Mission Critical Organization name of the transmitting MCX User to all MCX UEs that are receiving for display by each MCX UE.

6.10 MCX Service User Profile management

[R-6.10-001] The MCX Service shall be able to dynamically modify one or more pieces of information within the MCX Service User Profile (e.g., the list of MCX Service Groups for which the user has access credentials) while in use by the MCX User.

[R-6.10-002] The MCX Service shall provide a means by which an MCX Service Administrator designates that new or updated MCX Service User Profiles are to be installed at the MCX UE for immediate use by the MCX User.

[R-6.10-003] The MCX Service shall provide a means by which an MCX Service Administrator designates a particular time and date when new or updated MCX Service User Profiles are to be installed at the MCX UE for use by the MCX User.

[R-6.10-004] The MCX Service User Profile shall be construed to be sensitive user information and shall be provided end-to-end confidentiality and integrity protection when transferred between the MCX Service and MCX UE.

6.11 Support for multiple devices

[R-6.11-001] The MCX Service shall provide a notification to the MCX User if the MCX User is already logged on to another MCX UE.

[R-6.11-002] The MCX Service shall provide the mechanisms to allow an MCX User to log off remotely from other MCX UEs.

[R-6.11-003] The MCX Service shall provide the mechanism to allow an authorized MCX User to remotely log off another MCX User from an MCX UE.

6.12 Location

[R-6.12-001] The MCX Service shall provide Location information of the transmitting MCX UE to receiving MCX UEs subject to privacy restrictions.

[R-6.12-002] The MCX Service shall support conveyance of Location information provided by 3GPP location services.

[R-6.12-003] The MCX Service shall provide a means for an authorized MCX User to restrict the dissemination of his Location information.

[R-6.12-004] The MCX Service shall provide end-to-end confidentiality of Location information.

[R-6.12-005] The MCX Service shall provide authentication of messages carrying Location information.

[R-6.12-006] The MCX Service shall provide a means for an authorized MCX User to activate a one-time Location information report of an MCX User and periodic Location information update reports of an MCX User.

[R-6.12-007] The MCX Service shall provide a means for an authorized MCX User to deactivate periodic Location information update report of an MCX User.

6.13 Security

6.13.1 Overview

Security covers areas designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted. The security requirements listed here cover the areas of cryptographic protocols, authentication, access control, regulatory issues and storage control.

6.13.2 Cryptographic protocols

[R-6.13.2-001] The MCX Service shall employ open cryptographic standards, subject to applicable local policy (e.g., Federal Information Processing Standards (FIPS) 140-2).

[R-6.13.2-002] The MCX Service shall allow for update to new cryptographic operations and methods without making obsolete existing operations and methods, or requiring upgrade of all user equipment simultaneously.

[R-6.13.2-003] The MCX Service shall allow for the coexistence of a multiplicity of cryptographic suites.

NOTE 1: A "cryptographic suite" is a consistent collection of cryptographic operations (e.g., encryption and message authentication) spanning the totality of required cryptographic operations for MCX Service. That is, if MCX Service requires a stream cipher, a message authentication code, and a secure hash, then counter-mode AES-256, CMAC with AES-256 as an underlying cipher, and SHA-512 would constitute a cryptographic suite for MCX Service.

NOTE 2: The definition and identification of cryptographic suites and algorithms need not all be within the scope of 3GPP.

6.13.3 Authentication

[R-6.13.3-001] The MCX Service shall provide a means by which an MCX UE can require authentication of the MCX Service.

6.13.4 Access control

[R-6.13.4-001] The MCX Service shall support suspending or disabling of access from an MCX UE or an MCX User to the MCX Service.

[R-6.13.4-002] An MCX User who has a profile that has been deleted or suspended shall be prevented from using that MCX Service User Profile to access the MCX Service.

[R-6.13.4-003] The MCX Service shall provide a mechanism to temporarily disable an MCX UE remotely by the MCX Service Administrator or an authorized MCX User.

[R-6.13.4-004] The MCX Service shall only allow a user to affiliate to or select an enabled MCX Service Group (i.e., not disabled).

[R-6.13.4-005] A temporarily disabled MCX UE, which has limited access capability per Mission Critical Organization policy, shall be able to be re-enabled by the MCX Service Administrator or an authorized MCX User.

[R-6.13.4-006] The MCX Service shall provide a mechanism to re-enable a temporarily disabled MCX UE by the MCX Service Administrator or an authorized MCX User.

[R-6.13.4-007] The MCX Service shall provide a mechanism to permanently disable an MCX UE by the MCX Service Administrator or an authorized MCX User.

[R-6.13.4-008] The permanently disabled MCX UE shall remove all MCX Service User Profiles stored in the MCX UE.

[R-6.13.4-009] The permanently disabled MCX UE shall have no access to MCX Services.

[R-6.13.4-010] The security solution for the MCX Service shall minimize the impact of a compromised MCX UE on other MCX UEs.

6.13.5 Regulatory issues

[R-6.13.5-001] The MCX Service shall support lawful interception.

6.13.6 Storage control

[R-6.13.6-001] The MCX Service shall provide all relevant security for media storage (e.g., video or data) on the MCX UE (e.g., data encryption, access only to authorized MCX Group Members).

6.14 Interactions for MCX Service Group Communications and MCX Service Private Communications

[R-6.14-001] The MCX Service shall allow an MCX UE to be receiving and transmitting in one MCX Private Communication (without Floor control) while simultaneously receiving transmissions from other MCX Group communications within the same MCX service.

[R-6.14-002] The MCX Service shall allow an MCX UE to be receiving and transmitting in one MCX Private Communication (without Floor control) while simultaneously receiving transmissions from other MCX Private Communications (with Floor control) within the same MCX service.

6.15 Additional services for MCX Service communications

6.15.1 Discreet listening capabilities

[R-6.15.1-001] The MCX Service shall provide a mechanism for an authorized MCX User to receive MCX Service Group or Private Communication transmissions from any MCX User within their authority without noticeable impact on or knowledge of the MCX User.

6.15.2 Ambient listening

6.15.2.1 Overview of ambient listening

Ambient listening is a feature that allows an authorized MCX User, typically a dispatcher, to cause an MCX UE to initiate a communication which results in no indication on the MCX UE that it is transmitting. Ambient listening can be initiated by an authorized MCX User who wants to be "listened" to by another remote authorized MCX User or can be initiated by a remote authorized MCX User who wants to "listen" to another MCX User. The purpose of this feature allows a dispatcher to "listen" to activities at the Location of the remote MCX UE to find out what is happening around that MCX UE without providing an indication to the MCX User or people around the user (whom the MCX User does not want to make aware of this action) that this is happening. This type of communication is different from other types of communications, as for ambient listening information is only transmitted to one party in the communication (i.e., a dispatcher or an authorized MCX User that is acting in a similar role to a dispatcher).

This is used for stolen MCX UEs, monitoring officers, officer safety and particular operations, where it is important that the MCX UE does not indicate what is happening.

6.15.2.2 Ambient listening requirements

6.15.2.2.1 General ambient listening requirements

[R-6.15.2.2.1-001] The MCX UE that is being listened to shall be the only transmitting party in the Private Communication.

[R-6.15.2.2.1-002] For an MCX UE that is being listened to there shall be no indication on the MCX UE that it is transmitting.

[R-6.15.2.2.1-003] If someone attempts to turn off an MCX UE that is being listened to it shall appear to be turned off even while Ambient Listening continues to be active.

6.15.2.2.2 Remotely initiated ambient listening requirements

[R-6.15.2.2.2-001] The MCX Service shall provide a mechanism to allow an MCX Service Administrator and/or an authorized user to set up Ambient Listening on a remote MCX UE within their authority.

[R-6.15.2.2.2-002] The MCX Service shall ensure that Ambient Listening triggered remotely is terminated only by the remote authorized MCX User (e.g., a dispatcher).

6.15.2.2.3 Locally initiated ambient listening requirements

[R-6.15.2.2.3-001] The MCX Service shall provide a mechanism to allow an authorized MCX User to use the MCX UE that the MCX User is currently using to initiate Ambient Listening to another authorized MCX User (e.g., a dispatcher).

[R-6.15.2.2.3-002] The MCX Service shall ensure that Ambient Listening triggered locally can be terminated by the MCX User being listened to or by the remote MCX Service Administrator and/or authorized user, who was the listening Participant.

6.15.3 Remotely initiated MCX Service Communication

6.15.3.1 Overview

A Remotely initiated MCX Service Communication is a feature that allows an authorized user, typically a dispatcher, to cause a remote MCX UE to initiate a communication by itself, without its user explicitly initiating the communication manually. The purpose of this feature allows the dispatcher to "listen" to activities at the Location of the remote MCX UE to find out what is happening around that MCX UE. This feature is also known as "Remote Unit Monitoring" in P25 systems.

There are two typical use cases for this feature.

The first one is the case where a user could have been incapacitated. This could be both accidentally, say a traffic accident, or deliberately, for example a violent attack. In both cases it would be necessary to remotely initiate a communication from the MCX UE in order to allow another user or a group of users to "listen" to what is happening to prepare assistance. The communication that is set up is either a Private Communication or a Group Communication, and the communication could optionally be visible to the remote MCX UE's user.

The second one is the case of a stolen MCX UE. Here it is just necessary to activate the MCX UE so that a dispatcher can "listen" to any background communication in order to make an analysis of the situation. In this situation, the initiation of the communication from the remote MCX UE, typically a Private Communication in that case, is not visible by that MCX UE's user.

Other use cases, such as undercover operations, discreet surveillance of users or investigations, could exist depending on the missions of the critical communications users and on legislations.

The behaviour of the remotely initiated Communication is not different from a normal communication initiated by the local MCX User. The same rules for resource allocation and interactions with other services apply, but the initiator of the feature can have the capability to request a pre-emptive or high priority for that Communication to ensure it is set up even in case of resource congestion or to limit disturbance by other services.

6.15.3.2 Requirements

[R-6.15.3.2-001] The MCX Service shall provide a mechanism for an MCX Service Administrator and/or authorized MCX User to cause an MCX UE that is within their authority to initiate an MCX Private Communication to the MCX Service Administrator and/or authorized MCX User and then begin transmitting to the MCX Service Administrator or authorized MCX User.

[R-6.15.3.2-002] The MCX Service shall provide a mechanism for an MCX Service Administrator and/or authorized user to provide a notification to the user of the MCX UE when a remote MCX Private Communication is initiated.

[R-6.15.3.2-003] The MCX Service shall provide a mechanism for an MCX Service Administrator and/or authorized user to cause an MCX UE that is within their authority to initiate an MCX Service Group Communication and then to begin transmitting to the Affiliated MCX Service Group Members.

[R-6.15.3.2-004] The MCX Service shall provide a mechanism for an MCX Service Administrator and/or authorized user to provide a notification to the user of the MCX UE when a remote MCX Service Group Communication is initiated.

6.15.4 Recording and audit requirements

[R-6.15.4-001] The MCX Service shall provide a mechanism for a Mission Critical Organization to log the metadata of the MCX Service Group Communications and MCX Service Private Communications under the organization's authority.

[R-6.15.4-002] Metadata shall be logged for both the transmitting Participant and the receiving Participant(s).

[R-6.15.4-003] The MCX Service shall provide a mechanism for a Mission Critical Organization to record the transmissions of the Group Communications and Private Communications under the organization's authority.

[R-6.15.4-004] The MCX Service shall provide a mechanism for a Mission Critical Organization to log at least the following metadata per communication: depending on service this may include; start time, date, MCX User ID, MCX Group ID, Location information of the transmitting Participant, end time or duration, end reason, type of communication (e.g., MCX Service Emergency, regroup, private).

[R-6.15.4-005] If an MCX Service Group Communication or MCX Service Private Communication uses end-to-end confidentiality, the MCX Service shall provide a mechanism for a Mission Critical Organization to maintain the end-to-end confidentiality when the MCX Service Group Communication or MCX Service Private Communication is logged.

[R-6.15.4-006] The MCX Service shall provide a mechanism for a Mission Critical Organization to log the metadata of non-communication related user activities under the agency's authority.

[R-6.15.4-007] The MCX Service shall provide a mechanism for a Mission Critical Organization to log at least the following non-communication activity types: MCX Service Emergency Alert, MCX Service Emergency Alert cancellation, In-progress Emergency cancellation, registration state change, overridden event, user remote logout, changing another user's affiliations, affiliation change, and change of Selected MCX Service Group.

[R-6.15.4-008] The MCX Service shall provide a mechanism for a Mission Critical Organization to log at least the following metadata per non-communication activity: time, date, MCX Service User identity, and activity type. The following metadata should be logged if applicable to the activity type: MCX Service Group ID, Location information of the MCX User, affiliation list, target MCX Service User ID and success/failure indication.

[R-6.15.4-009] The MCX Service shall provide a mechanism for a Mission Critical Organization to log metadata for all failed authorization attempts (e.g., invalid login password) by an MCX User.

[R-6.15.4-010] The MCX Service shall provide a mechanism to collect metadata for network access events (e.g., pre-emption of the 3GPP system bearer service, loss of signal, failed registration attempts).

6.16 Interaction with telephony services

[R-6.16-001] The MCX Service shall provide a mechanism to allow an MCX Service Administrator to configure whether an MCX User using an MCX UE is able to make and/or receive telephony calls.

[R-6.16-002] The MCX Service shall provide a mechanism for an MCX User authorized to use telephony services to block incoming telephony calls.

6.17 Interworking

6.17.1 Non-3GPP access

[R-6.17.1-001] Subject to security and operational constraints and limitations of the underlying access technology, the MCX Service shall provide a mechanism to allow IP-based non-3GPP access to the MCX Service system.

NOTE: An example of non-3GPP access is a dispatcher connecting to the system via a console.

6.17.2 Interworking between MCX Service systems

[R-6.17.2-001] An MCX Service shall provide mechanisms to allow an MCX User to operate in a Partner MCX Service System, subject to authorization from both the Partner and the Primary MCX Service Systems of the MCX User.

[R-6.17.2-002] The authentication of an MCX User with an MCX Service in a Partner MCX Service System shall be based on security parameters obtained from the Primary MCX Service System of the MCX User.

NOTE 1: This is an application layer authentication and not 3GPP network authentication.

[R-6.17.2-003] Any functionality needed from the visited PLMN network is subject to roaming capabilities and operator agreement.

[R-6.17.2-004] An MCX Service shall provide mechanisms to allow an MCX User on the Primary MCX Service System to affiliate to an MCX Service Group from a Partner MCX Service System, subject to authorization from the Primary MCX Service System and the Partner MCX Service System where the MCX Service Group is defined.

[R-6.17.2-005] An MCX Service shall provide mechanisms to allow a roaming MCX User to affiliate to an MCX Service Group from the Partner MCX Service System, subject to authorization from the Partner MCX Service System where the MCX Service Group is defined.

[R-6.17.2-006] An MCX Service shall provide mechanisms to allow an MCX User that receives service from a Partner MCX Service System to affiliate to an MCX Service Group from another Partner MCX Service System, subject to authorization from the Partner MCX Service System where the MCX Service Group is defined.

NOTE 2: It is assumed that once affiliation from a User to a Group is successful, subsequent communication within that Group are available to the User.

[R-6.17.2-007] End to end security of an MCX Service Group communication (including in Partner MCX Service Systems) shall be based on parameters obtained from the MCX Service system where the MCX Service Group is defined.

6.18 MCX Service coverage extension using ProSe UE-to-Network Relays

[R-6.18-001] A ProSe-enabled UE authorized to act as a ProSe UE-to-Network Relay shall, if authorized, support the bi-directional relay of signalling (control plane) and data (user plane) between an MCX UE and the on-network MCX Service.

[R-6.18-002] A ProSe UE-to-Network Relay authorized to act as an MCX Service relay shall advertise, at the ProSe interface, those MCX Services (Groups) which it is currently relaying.

[R-6.18-003] An MCX UE which is unable to gain service from a 3GPP network shall search for ProSe UE-to-Network Relay(s) offering MCX Services for the affiliated MCX Service Groups of the MCX User.

[R-6.18-004] A ProSe UE-to-Network Relay authorized to support MCX Service coverage extension relay between an MCX UE and the on-network MCX Service shall provide a mechanism for an off-network MCX UE to affiliate to one or more MCX Service Groups using the on-network MCX Service.

[R-6.18-005] The ProSe UE-to-Network Relay that has enabled an MCX UE to affiliate to an MCX Service Group using the on-network MCX Service shall subsequently support the bi-directional relay of signalling (control plane) and data (user plane) between the MCX UE and the on-network MCX Service for that MCX Service Group.

[R-6.18-006] A ProSe UE-to-Network Relay authorized to support the bi-directional relay of signalling (control plane) and data (user plane) between an MCX UE and the on-network MCX Service shall provide a mechanism for an off-network MCX UE to initiate and/or receive Private Communications using the on-network MCX Service.

6.19 Additional MCX Service requirements

6.19.1 Communication rejection and queuing

Requests to transmit appear in MCX Services in many forms and under many circumstances. Normally, requests to transmit are accompanied by priority information that is used to arbitrate the decision to assign resources for the transmission amongst competing requests to transmit. Upon arrival, a request to transmit is immediately granted, rejected, or queued. If queued, a request to transmit is normally granted when conditions which caused the queue are removed, or it can be dropped automatically for a number of reasons, or it can be cancelled by an authorized user who is usually the initiator of the request to transmit. When a request to transmit is rejected, it can be re-requested either manually by user action or automatically.

6.19.1.1 Requirements

[R-6.19.1.1-001] The MCX Service shall provide a mechanism to queue any MCX request to transmit.

[R-6.19.1.1-002] The MCX Service shall provide a mechanism to reject MCX request to transmit with a cause indication.

[R-6.19.1.1-003] The MCX Service shall notify the requesting MCX Participant and may notify one or more authorized users when a communication is queued, when a communication is rejected, when communications has started after being de-queued.

[R-6.19.1.1-004] The MCX Service shall provide a mechanism for an MCX User to remove its MCX request to transmit from the MCX request queue.

[R-6.19.1.1-005] The MCX Service shall provide a mechanism for an authorised user to remove another user’s MCX request to transmit from the MCX request queue.

[R-6.19.1.1-006] An MCX Service User shall be notified when his request to transmit is removed from the request queue.

[R-6.19.1.1-007] The MCX Service shall provide a mechanism for an MCX Administrator to configure service parameter(s) (e.g., timer) for automatic removal of an MCX request to transmit from any MCX request queue.

7 MCX Service requirements specific to off-network use

7.1 Off-network communications overview

The MCX Service while operating in off-network mode comprises a set or collection of functions necessary to provide Mission Critical Services (e.g., MCPTT, MCVideo, MCData, etc.) using a ProSe direct (UE-to-UE) Communication

path (ProSe direct communication path) for transport. The ProSe direct communication path does not traverse the network infrastructure.

Users operating off the network are either out of network coverage (not served by a 3GPP network) (e.g., in a remote mountain area fighting a forest fire 20 miles from the nearest network) or have selected a ProSe direct communication path for MCX Service while in network coverage. MCX Users operating off the network need to be in ProSe direct communication range in order to communicate.

NOTE 1: While the network is likely to be a primary, reliable transport of MCX Service communications, there are many situations where MCX Service communications are needed in areas where the network is not available, or coverage is not reliable.

MCX Users outside of the coverage of the fixed network might be first responders in a rural area assisting in a response to a plane crash, fire fighters in a remote mountain area fighting a forest fire or police officers inside a residence responding to a domestic issue. Off-network MCX Service communications are expected to be immediately accessible to users in the absence of the network.

MCX Users in network coverage might be working in a confined area, such as fire fighters fighting a structure fire where direct UE-to-UE communication is more desirable and reliable. Users can communicate directly with one another without having to overcome the resistance of a building and distance to the nearest base station to communicate with other members of their team inside the building that are nearby.

To operate off the network, an MCX UE is capable of automatically switching to a ProSe direct communication path for use of MCX Services when detecting an off-network (out of coverage) condition. In addition, a mechanism is provided for an authorized user to select (manually switch to) a ProSe direct communication path for use of off-network MCX Service communications (e.g., while in network coverage).

When operating off the network, the MCX Service is provided by the MCX Service Application on the UE as compared to operations on the network, where the MCX Service Application on the UE interacts with an MCX Service server and the network to provide the MCX Service.

NOTE 2: For MCX UEs that have selected a ProSe Direct Communication path for use of MCX Services while in network coverage, signalling with the network and MCX Service might be available (e.g., radio resource allocation, MCX Service User Profile management updates and cryptographic key management updates), while the MCX User transmissions would be direct between the MCX UEs (e.g., not traversing the network).

The Off-Network MCX Service builds upon ProSe enablers to establish, maintain and terminate the signalling and communication path(s) among the off-network users. To the extent feasible, it is expected that the end user's experience is similar regardless if the MCX Service is used with a 3GPP network or based on the use of a ProSe direct communication path.

The Off-Network MCX Service is intended to support communication between a group of users (a group communication), where each user has the ability to gain access to transmit in an arbitrated manner. However, the MCX Service also supports Private Communications between pairs of users.

When operating off the network the MCX Service allows users to request the permission to transmit (transmit voice/audio) and provides a deterministic mechanism to arbitrate between requests that are in contention (i.e., Floor control).

The Off-Network MCX Service provides a means for a user with higher priority (e.g., MCX Service Emergency condition) to override (interrupt) the current sender. The Off-Network MCX Service also supports a mechanism to limit the time a user transmits (has access to the resources) thus permitting users of the same or lower priority a chance to gain access to the resources.

The Off-Network MCX Service provides the means for a user to monitor activity on a number of separate communications and enables the user to switch focus to a chosen communication. An Off-Network MCX User might join an already established MCX Service Group Communication (Late communication entry). In addition the Off-Network MCX Service supports MCX Service User IDs, aliases and user Location determination features.

For operation off the network (e.g., when out of network coverage), an MCX UE is (pre-)provisioned by an MCX Service Administrator and/or authorized user with the following in order to use MCX Services:

a) An MCX Service User Profile associated with each of the intended MCX Users of the MCX UE that might be used for off-network operation;

1) An alphanumeric identifier (with a minimum length of Nc3) (i.e., alias) for each MCX User;

2) A number of off-network MCX Service Groups for use by the MCX User;

3) An alphanumeric identifier (i.e., alias) for the authorized off-network MCX Service Groups;

4) A Mission Critical Organization name if available, associated with each of the intended MCX Users or Administrator;

5) A number of off-network MCX Users for Private Communications for which the MCX User is authorized;

b) Authentication and end-to-end security keys.

NOTE 3: MCX UEs can be provisioned for off-network use by either configuration outside of network coverage or by attaching to the network.

An MCX UE operating off the network is capable of transmitting the sender's Location information, MCX Service User ID, alias(es), off-network MCX Service Group ID, group alias and, if available, Mission Critical Organization name of the user who is transmitting (i.e., whose UE is transmitting) to all other users in a communication including MCX UEs operating off the network that are late entering a communication in progress.

The Off-Network MCX Service uses the capabilities defined in ProSe TS 22.278 [5], including the ProSe Relay capabilities defined in ProSe TS 22.278 [5] and GCSE_LTE TS 22.468 [6].

NOTE 4: As indicated in TS 22.278 [5] use of a ProSe Direct Communication path outside of network coverage is only applicable for Public Safety ProSe enabled UEs. For non-Public Safety ProSe enabled UEs the selection of the most appropriate communication path (ProSe Communication path (direct or routed via local basestation) or 3GPP network path) is under network control and based on operator preferences.

MCX Service requirements specific to off-network use are defined in clause 7. Common MCX Service requirements defined in clause 5 apply whether the MCX Service is in use on the network or off the network.

7.2 General off-network MCX Service requirements

[R-7.2-001] In order to operate off the network using the direct communication path, an MCX UE shall be a Public Safety ProSe-enabled UE.

[R-7.2-002] The Off-Network MCX Service shall make use of the ProSe capabilities related to ProSe Communication using the direct communication path between Public Safety ProSe-enabled UEs as defined in TS 22.278 [5].

[R-7.2-003] The MCX Service shall provide a mechanism for an MCX Service Administrator and/or authorized user to pre-provision MCX UEs that may not be served by the network with the following in order to operate using off-network MCX Service:

a) An MCX Service User Profile associated with each of the intended MCX Users of the MCX UE that might be used for off-network operation:

1) alphanumeric identifier (i.e., Alias ID) for the authorized off-network MCX Service Groups;

2) a number of off-network MCX Service Groups for use by an MCX User;

3) a MCX Service User ID associated with each of the intended MCX Users;

4) an alphanumeric identifier (with a minimum length of Nc3) (i.e., alias) for each MCX Service User ID.

b) authentication and end to end security keys.

NOTE: MCX UEs can be provisioned for off-network use by either configuration outside of network coverage or by attaching to the network.

[R-7.2-004] An MCX UE operating off the network shall be capable of transmitting the MCX Service User ID, alias(es), off-network MCX Service Group and, if available, Mission Critical Organization name of the user who is talking (i.e., whose UE is transmitting) to all other users in the communication including MCX UEs operating off the network that enter the communication late.

[R-7.2-005] An MCX UE operating off the network shall be capable of transmitting the sender's Location information (i.e., whose UE is transmitting) to all other users in the communication including MCX UEs operating off the network that enter the communication late.

7.3 Admission control

7.3.1 General aspects

[R-7.3.1-001] The admission control functionality shall authorize a participant to start a communication.

[R-7.3.1-002] The admission control function shall be common to all services. That is to say resources are shared by all MCX Services depending on priorities. When a new communication is started an MCX service shall take into account priorities of all MCX Services communications as well as the resources they take/need.

[R-7.3.1-003] The off-network Floor control functionality in an MCX Service shall determine at a point in time which received transmission(s) from off-network Participant(s) shall be presented to the receiving off-network Participant(s).

7.3.2 Communication initiation

[R-7.3.2-001] An authorized participant shall be able to request to start a communication.

[R-7.3.2-002] The admission control functionality shall determine if an MCX User is allowed to start a communication and transmit according to resource management.

[R-7.3.2-003] Following an off network MCX Service request for permission to transmit on the Selected MCX Group, the Affiliated MCX Group Member that made and was granted the request shall be given an indication of being granted permission to transmit.

[R-7.3.2-004] When an MCX User is not allowed to start a communication, the MCX Service shall notify the MCX User that his communication has been queued or rejected.

[R-7.3.2-005] When an MCX User is not allowed to start a communication the request may be queued or rejected.

7.4 Communication termination

[R-7.4-001] The MCX Service when operating off the network shall provide a mechanism for an MCX Service Administrator to preconfigure separately the limit for the total length of time of an MCX Service Group Communication and an MCX Service Private Communication.

[R-7.4-002] The MCX Service when operating off the network shall provide an indication to the Participants that the communication is within a configurable amount of time before the communication time limit is reached.

[R-7.4-003] The MCX Service when operating off the network shall provide an indication to the Participants that the communication time limit has been reached.

[R-7.4-004] The MCX Service when operating off the network shall release the communication when the communication time limit has been reached.

7.5 Broadcast Group

[R-7.5-001] The MCX Service when operating off the network shall support Broadcast Group Communications within that MCX Service.

[R-7.5-002] The MCX Service shall deliver an off-Network Broadcast Group Communication to the members of a Broadcast Group within that MCX Service who are within communication range, and who may be all of the MCX Service system users, or a subset thereof.

7.6 MCX Service priority requirements

[R-7.6-001] The Off-Network MCX Service shall assign to each MCX Service Group or Private Communication:

- an application layer pre-emption capability;

- a capability to be pre-empted; and
- an application layer priority value.

[R-7.6-002] The Off-Network MCX Service shall support at least 8 configurable levels of priority.

[R-7.6-003] The Off-Network MCX Service shall support multiple MCX Service Application priorities which are mapped to ProSe priority levels, based on network operator policy.

[R-7.6-004] The Off-Network MCX Service shall enable an MCX Service Administrator to prioritize MCX Groups in relation to other MCX Groups (with respect to transport and presentation).

[R-7.6-005] When determining priority for an MCX communication, the Off-Network MCX Service shall use the MCX User/Participant's attributes (e.g., first/second responder, supervisor, dispatcher, on/off duty) and the MCX Group's attributes (e.g., type of group, owning organization of the group, MCX Emergency, Imminent Peril).

[R-7.6-006] The Off-Network MCX Service shall support multiple pre-emptive priorities.

[R-7.6-007] The Off-Network MCX Service shall provide a mechanism for MCX Administrators to create, a pre-emption hierarchy for MCX Group communications and their associated users (i.e., to facilitate local management of the service and its resources).

[R-7.6-008] The Off-Network MCX Service shall support MCX Groups with the permission to pre-empt other MCX communications.

[R-7.6-009] In case of resource shortage an MCX communication made to a group with pre-emption permissions shall be given resources to complete this communication by pre-empting lower priority MCX communications.

7.7 Communication types based on priorities

7.7.1 MCX Service Emergency Group Communication requirements

[R-7.7.1-001] The Off-Network MCX Service shall provide a mechanism for an authorized Participant of an off-network MCX Service Group Communication to change the status of the off-network MCX Service Group Communication in progress to an off-network MCX Service Emergency Group Communication.

[R-7.7.1-002] An off-network MCX UE that has initiated the MCX Service Emergency Group Communication shall maintain knowledge of the in progress off-network MCX Service Emergency Group Communication until it is cancelled.

[R-7.7.1-003] An off-network MCX UE initiating an off-network MCX Service Emergency Group Communication shall be capable of transmitting its MCX Service User ID and an indication that it is an off-network MCX Service Emergency Group Communication to all other users in the communication.

7.7.2 MCX Service Emergency Group Communication cancellation requirements

[R-7.7.2-001] An indication of the cancellation of an off-network MCX Service Emergency Communication and the identity of the cancelling user shall be transmitted to Affiliated MCX Service Group Members of the off-network MCX Service Emergency Group Communication.

7.7.3 Imminent Peril Communication

7.7.3.1 Imminent Peril Group Communication requirements

[R-7.7.3.1-001] The Off-Network MCX Service shall provide a mechanism for an Affiliated MCX Service Group Member to initiate (or join) an off-network MCX Service Group Communication and set (or change) the status of the communication to Imminent Peril.

[R-7.7.3.1-002] If an MCX Service Group has previously been configured to be used for Imminent Peril communications by the MCX User, that MCX Service Group shall be used for the communication.

[R-7.7.3.1-003] The MCX Service when operating in off-network mode shall provide a mechanism, for an authorized Participant of an in progress off-network MCX Service Group Communication, to change the status of the communication to an off-network MCX Service Imminent Peril group communication.

[R-7.7.3.1-004] The off-network MCX UE that has initiated an MCX Service Imminent Peril group communication shall be responsible for maintaining the knowledge of the Imminent Peril status until it is cancelled.

[R-7.7.3.1-005] The Off-Network MCX Service shall provide a mechanism to inform and keep updated other Participants of the MCX Service Group Communication regarding the Imminent Peril status of the communication and regarding the MCX Service User ID of the MCX User setting the status to Imminent Peril.

7.7.3.2 Imminent Peril Group Communication cancellation requirements

[R-7.7.3.2-001] An indication of the cancellation of the Imminent Peril status of an off-network MCX Service Imminent Peril group communication and the MCX Service User ID of the cancelling user shall be transmitted to Affiliated MCX Service Group Members of an off-network MCX Service Imminent Peril group communication.

[R-7.7.3.2-002] If the Imminent Peril status of an MCX Service Imminent Peril group communication is cancelled by an MCX User other than the user initiating the Imminent Peril status, then the Off-Network MCX Service shall provide a mechanism to clear the knowledge of the Imminent Peril status maintained at the UE of the initiating MCX User.

7.8 Location

[R-7.8-001] An MCX UE shall be capable of transmitting its Location, if known, to other MCX UEs when operating off the network, subject to privacy restrictions.

7.9 Security

[R-7.9-001] MCX UEs operating off the network shall be capable of protecting the confidentiality of Location and identity information conveyed to or from other MCX UEs.

[R-7.9-002] MCX UEs operating off the network shall be capable of authenticating the sender of messages carrying Location and identity information.

7.10 Off-network MCX Service operations

[R-7.10-001] Off-Network MCX Services shall be able to operate in the complete absence of any fixed infrastructure.

[R-7.10-002] Off-Network MCX Services shall only be available for authorized users.

[R-7.10-003] The MCX Service shall provide a mechanism for an MCX Service Administrator to authorize users for Off-Network MCX Services.

7.11 Off-network UE functionality

[R-7.11-001] An MCX UE shall be capable of off-network MCX Service communications and on-network MCX Service communications at the same time.

NOTE: Sub-clause 7A.2 in TS 22.278 specifies requirements for concurrent communications on and off the network within the same group, concurrent communications on and off the network with different groups, and concurrent communications on and off the network involving both groups and Private Communications. This concurrent communication is not defined as a ProSe relay.

[R-7.11-002] When switching from on-network to off-network operation (either manually or automatically), an MCX UE should attempt to notify the MCX Service that it is leaving the network.

[R-7.11-003] Prior to automatically going off the network an MCX UE should attempt to make use of suitable ProSe UE-to-Network Relay in its proximity.

7.12 Streaming for ProSe UE-to-UE Relay and UE-to-Network Relay

7.12.1 UE-to-Network Relay for all data types

[R-7.12.1-001] MCX Users shall be able to transmit and receive real time data (e.g., voice, streaming video/data) between an on-network MCX UE and an off-network MCX UE via a ProSe UE-to-Network relay using the MCX UE-to-Network Relay service.

[R-7.12.1-002] The MCX Service shall provide a mechanism for an authorized MCX User to forward real-time data (e.g. voice, streaming video/data) from an MCX User to another MCX User across a ProSe UE-to-Network relay using the MCX UE-to-Network Relay service.

[R-7.12.1-003] The MCX Service shall provide a mechanism for an MCX Service Administrator to authorize an MCX User to forward real time data (e.g. voice, streaming video/data) from one MCX User to another MCX User.

[R-7.12.1-004] The MCX Service shall provide a mechanism to select/re-select a UE-to-Network Relay node that has enough capability for the real time data (e.g. video) forwarding.

7.12.2 UE-to-UE Relay streaming

[R-7.12.2-001] MCX Users shall be able to transmit and receive streaming video or data between an off-network MCX UE and another off-network MCX UE via a ProSe UE-to-UE relay using the MCX UE-to-UE Relay service.

[R-7.12.2-002] The MCX Service shall minimize the interruption to an on-going MCX Service communication when an MCX UE transitions its connection for that communication from on-network operation to off-network operation via a ProSe UE-to-UE relay.

[R-7.12.2-003] The MCX Service shall minimize the interruption to an on-going MCX Service communication when an MCX UE transitions its connection for that communication from off-network operation via a ProSe UE-to-UE relay to on-network operation.

7.12.3 Off-Network streaming

[R-7.12.3-001] MCX Users shall be able to transmit and receive streaming video or data between an off-network MCX UE and another off-network MCX UE via ProSe communications.

[R-7.12.3-002] The MCX Service shall minimize the interruption to an on-going MCX Service communication when an MCX UE transitions its connection for that communication from a ProSe UE-to-UE relay to ProSe direct communications with another MCX UE.

[R-7.12.3-003] The MCX Service shall minimize the interruption to an on-going MCX Service communication when an MCX UE transitions its connection for that communication from ProSe direct communications with another MCX UE to a ProSe UE-to-UE relay.

7.13 Switching to off-network MCX Service

[R-7.13-001] An MCX UE shall be capable of automatically switching to a ProSe direct communications path for use of MCX Service when detecting an off-network (out of coverage) condition.

[R-7.13-002] A means shall be provided for an authorized MCX User to be able to manually switch between on-network operation and a ProSe direct communication path for use of Off-Network MCX Service while in network coverage.

[R-7.13-003] Subject to operator policy and/or network authorization, a means shall be provided for an authorized MCX User using a Public Safety ProSe-enabled UE to be able to manually switch between the on-network operation and a ProSe direct communication path for use of Off-Network MCX Service while in network coverage or out of network coverage.

[R-7.13-004] An MCX Service shall minimize the interruption to an on-going MCX Service communication when an MCX UE transitions its connection to that communication from on-network operation to off-network ProSe direct communication with another MCX UE.

[R-7.13-005] An MCX Service shall minimize the interruption to an on-going MCX Service communication when an MCX UE transitions its connection to that communication from off-network ProSe direct communication with another MCX UE to on-network operation.

7.14 Off-network recording and audit requirements

[R-7.14-001] The Off-Network MCX Service shall provide a mechanism to collect metadata for MCX Service Group Communications and MCX Service Private Communications (e.g., initiating MCX Service User ID, MCX Service Group ID) and non-communication activities (e.g., changing group settings) from MCX UEs operating in off-network mode. Metadata shall be logged for both the transmitting Participant and the receiving Participant(s).

[R-7.14-002] Upon return to on-network operation, the MCX Service shall provide a mechanism to retrieve communication and non-communication activity metadata from an MCX UE that has collected such metadata while operating in off-network mode.

7.15 Off-network UE-to-UE Relay

7.15.1 Private Communications

[R-7.15.1-001] The Off-Network MCX Service shall provide a means by which the MCX User of a (source) UE can make a Private Communication to the MCX User of a (target) UE via a ProSe UE-to-UE Relay.

[R-7.15.1-002] The Off-Network MCX Service shall provide a mechanism for a source MCX User to query whether a particular target MCX User is within ProSe direct communication range.

[R-7.15.1-003] An MCX UE shall be able to:

- discover whether the UE of the target MCX User is itself within direct communication range of the source UE; and if not;
- instead discover whether the UE of the target MCX User is within communication range of a ProSe UE-to-UE Relay that is within direct communication range of the source UE.

7.15.2 Group Communications

[R-7.15.2-001] An MCX Service Administrator or authorized user shall be able to configure a ProSe-enabled UE, authorized to act as a ProSe UE-to-UE Relay, to relay any received MCX Service transmissions for one (or more) specified MCX Service Groups.

[R-7.15.2-002] An MCX UE receiving both the original MCX Service Group transmission and a relayed transmission shall be able to associate the two transmissions, correctly order a mixture of packets (received directly and indirectly) and identify duplicate packets.

8 Inter-MCX Service interworking

8.1 Inter-MCX Service interworking overview

Clause 8 describes interworking of one MCX Service with another.

The MCData Service as defined in TS 22.282 [3] includes description of multiple independent applications and data transfer capabilities, which may themselves be subject to interworking limitations as identified in clause 8. Therefore, requirements in clause 8 should be used as guidance for MCData interworking between individual applications within that one MCX Service.

8.2 Concurrent operation of different MCX Services

8.2.1 Overview

In some cases, a User or UE will use multiple independent MCX Services. The intention in this case is that each service will operate totally independently of the other services and should not cause service, capability or capacity interaction problems. It is understood that different UE may have different abilities to cope with the demands of simultaneous

services. The requirements in sub-clause 8.2.2 identify how to handle simultaneous services which are intended to be completely independent of each other but limits in total capacity to handle multiple services and multiple instances within a service is left for suppliers to characterise for their products.

Where independent functionality between services is constrained due to transport capacity limitations, those requirements are indicated in the sub-clause on Priority between Services.

When the constraint is due to the service itself (e.g. Audio embedded within a video and MCPTT speech both delivering audible signals) any potential conflict may be avoided by action in the network part of the service but these actions are not specified. In sub-clause 8.2.2 actions taken by a single UE in case of conflict not resolved in the network are specified.

8.2.2 Requirements

[R-8.2.2-001] Except where expressly stated each MCX Service shall operate independently of each other MCX Service.

[R-8.2.2-002] Any floor control facility remains completely independent for each of simultaneous MCX Services except where expressly stated.

[R-8.2.2-003] A user shall be able to transmit on one MCX Service and receive on another without service interaction limitations.

[R-8.2.2-004] A user shall be able to transmit on different MCX Services at essentially the same time without service interaction limitations.

[R-8.2.2-005] A user shall be able to receive on different MCX Services at essentially the same time without service interaction limitations except where services are competing for the same unsharable resource which may include the display, audio transducers, etc.

[R-8.2.2-006] When operating multiple MCX Services on the same network, radio resources shall be able to be utilized in an efficient manner for all MCX Services up to certain thresholds defined for each MCX Service and/or the combination of MCX Services. The radio resource allocation for each MCX Service and the combination of MCX Services shall be flexible based on demand, or allocated in a predefined manner.

[R-8.2.2-007] The network shall be able to assign radio resources so that resources assigned to each MCX Service, or the combination of all MCX Services stays below a threshold, subject to the agreement between the 3GPP network operator and the Mission Critical Organization(s) (e.g., 3GPP network can be operated by Mission Critical Organization(s), or 3GPP network is operated by commercial operator), for resources to be used for MCX Services without impacting other non-MCX Services.

8.3 Use of unsharable resources within a UE

[R-8.3-001] An MCX UE should be able to present audio from multiple sources (e.g. MCVideo, MCPTT) in a manner that is easily distinguished.

[R-8.3-002] An MCX UE may enable the user (e.g. incident commander) to control the relative volumes and spatial rendering of concurrent audio sources (e.g. MCVideo, MCPTT) at the UE.

[R-8.3-003] The MCX Service shall provide a mechanism for a MCX User to prioritize the use of contended resources (e.g. display, loudspeaker) in the UE (e.g. most recently selected MCX Service, MCPTT voice always has priority).

[R-8.3-004] Communication marked as Emergency or Imminent Peril shall take priority use of contended resources in the UE over communication not marked as Emergency or Imminent Peril.

[R-8.3-005] When a MCX Service is denied access to contended resource in the UE, an indication shall be given to the User to alert them of the situation.

[R-8.3-006] When a MCX Service is denied access to contended resource in the UE, a facility shall be provided for the User to select their preferred MCX Service for access to contended resources for the duration of the limitation.

8.4 Single group with multiple MCX Services

8.4.1 Overview

It is useful to be able to configure any single group to be able to handle multiple MCX Services. In sub-clause 8.4 requirements are on the service to provide a solution that looks as though the services are working in a coupled and coordinated manner. The exact means of achieving this is not implied here. So, where a User may affiliate to a single group for two services, this could be a single affiliation indicating two services but handled together or it could be that the UE sends two affiliations, one for each service, in response to the single command to affiliate. There may also be other possibilities. In essence the solution should look and feel like a combined service.

8.4.2 Requirements

[R-8.4.2-001] Mission critical groups shall be able to use multiple MCX Services independently or in combination.

[R-8.4.2-002] The MCX Service shall provide a mechanism by which an authorized MCX User can affiliate to a mission critical group using that MCX Service through a single logical group affiliation for any subset of MCX Services used by the group, or independently by MCX Service.

[R-8.4.2-003] To support operation coordinated between mission critical services, an MCX Service used by a mission critical group shall be able to interact with another MCX Service used by the same group.

[R-8.4.2-004] To support combined services where the operation is intended to be coordinated, each MCX Service shall be able to apply similar geographic restrictions in use for one MCX Service to also operate in the coordinated MCX Service(s).

[R-8.4.2-005] The MCX Service shall provide a mechanism by which an authorized MCX User that is affiliated to multiple MCX Services in a single group can de-affiliate from each MCX Service independently.

8.4.3 Compatibility of UE

8.4.3.1 Advertising service capabilities required

[R-8.4.3.1-001] The MCX Service shall provide a mechanism by which an MCX User of a UE can only affiliate to a Common MCX Service Group(s) for MCX Services that the MCX User's UE is capable of supporting.

[R-8.4.3.1-002] The MCX Service shall provide a mechanism to advertise the service capabilities required to participate in a group e.g. choice of codec so that an MCX User can check the UE's compatibility before attempting to affiliate.

[R-8.4.3.1-003] The MCX Service shall provide a mechanism for a UE to advertise its capability and limitation information when its MCX User affiliates to a group.

NOTE: For example when an MCX User affiliates to an MCVideo group, the MCX User's UE may indicate the codecs and coding rates supported so that the MCVideo service will ensure that the UE receives video that it can render.

[R-8.4.3.1-004] If the MCX User affiliates to a group, but its UE does not provide capability and limitation information, then the MCX Service shall assume that any MCX Service relevant content can be handled by that UE.

8.4.3.2 Conversion between capabilities

[R-8.4.3.2-001] Where an MCX Service does not advertise the service capabilities required to participate in a group it is assumed that service capability itself is sufficient to take part in the group. For example if a specific codec is being used and a joining UE may not support that codec then the service will provide transcoding for UEs that support the service but do not support the codec.

8.4.4 Individual permissions for service access

[R-8.4.4-001] When a UE makes a combined request to affiliate to a Common MCX Service Group the MCX Service may respond by permitting access to the group for some but not all MCX Services if appropriate.

8.4.5 Common alias and user identities or mappable

[R-8.4.5-001] To support combined services where the operation is intended to be coordinated, it shall be possible for one MCX Service to access and communicate using user identifying information in use for a coordinated MCX Service.

8.4.6 Single location message

[R-8.4.6-001] The MCX Service shall provide configuration and capability so that when a UE is affiliated to a Common MCX Service Group and some or all of the MCX Services periodically require location messages to be sent then each location message sent may be configured to apply to all MCX Services or to only one specific MCX Service.

[R-8.4.6-002] The MCX Service shall provide configuration and capability so that when a UE is affiliated to multiple groups and some or all of the groups periodically require location messages to be sent then each location message sent may be configured to apply to all affiliated groups or may be applied to only one specific group.

[R-8.4.6-003] The MCX Service shall provide configuration and capability so that when a UE is affiliated to multiple Common MCX Service Groups and some or all of the Common MCX Service Groups periodically require location messages to be sent then each location message sent may be configured to apply to all Common MCX Service Groups or may be applied to only one specific Common MCX Service Group.

8.5 Priority between services

8.5.1 Overview

The 3GPP priority system using ARP and QCI is expected to be used for relative priority treatment among communications at the transport level. Further application of priority will be invoked in and by the MCX Service system according to service related requirements e. g User and situation

8.5.2 Requirements

[R-8.5.2-001] For on network communications, priority management shall manage all data flows from the different mission critical services together when applying priority decisions.

NOTE 1: No mission critical service is considered as always having priority over another.

[R-8.5.2-002] For off network communications, priority management shall manage all data flows from the different mission critical services together when applying priority decisions.

NOTE 2: No mission critical service is considered as always having priority over another.

[R-8.5.2-003] The MCX Service systems shall provide a mechanism to dynamically prioritize one MCX Service over another.

[R-8.5.2-004] The MCX Services, in coordination with each other, shall be able to give appropriate priorities to the different communications according to User, content type, device type, participant type and operational situation.

[R-8.5.2-005] MCX Services shall notify users of actions taken by the dispatcher that result in a change in priority for a data flow.

9 Air ground air Communication

9.1 Service Description

Mission critical users use aircrafts and helicopters for operational purpose. Being able to communicate in real time with helicopters and aircraft is a basic need.

Some traffic assumptions are provided in Annex D.

9.2 Requirements

[R-9.2-001] The MCX Service shall support Air ground air Communication up to 15.000 ft with a speed up to [450]km/h.

10 MCX Service in IOPS mode

[R-10-001] An MCX Service shall be able to provide services when operating in a 3GPP network in IOPS mode.

NOTE: Services may be reduced for example due to lack of back haul.

Annex A (normative): MCCoRe Requirements for MCPTT

Table A.1 provides an exhaustive list of those requirements in 3GPP TS 22.280 that are applicable to MCPTT.

Table A.1

5 MCX Service Requirements common for on the network and off the network					
NA					
5.1 General Group Communications Requirements					
NA					
5.1.1 General aspects					
R-5.1.1-001	R-5.1.1-002	R-5.1.1-003	R-5.1.1-004	R-5.1.1-005	
5.1.2 Group/status information					
R-5.1.2-001	R-5.1.2-002				
5.1.3 Group configuration					
R-5.1.3-001	R5.1.3-002				
5.1.4 Identification					
R-5.1.4-001					
5.1.5 Membership/affiliation					
R-5.1.5-001	R-5.1.5-002	R-5.1.5-003	R-5.1.5-004	R-5.1.5-005	R-5.1.5-006
R-5.1.5-007	R-5.1.5-008				
5.1.6 Group Communication administration					
R-5.1.6-001					
5.1.7 Prioritization					
R-5.1.7-001	R-5.1.7-002				
5.1.8 Charging requirements for MCX Service					
R-5.1.8-001	R-5.1.8-003	R-5.1.8-004	R-5.1.8-005	R-5.1.8-006	R-5.1.8-007
R-5.1.8-008	R-5.1.8-009	R-5.1.8-010	R-5.1.8-011		
5.1.9 MCX Service Emergency Alert triggered by location					
NA					
5.2 Broadcast Group					
NA					
5.2.1 General Broadcast Group Communication					
R-5.2.1-001	R-5.2.1-002				
5.2.2 Group-Broadcast Group (e.g., announcement group)					
R-5.2.2-001	R-5.2.2-002	R-5.2.2-003	R-5.2.2-004		
5.2.3 User-Broadcast Group (e.g., System Communication)					
R-5.2.3-001	R-5.2.3-002				
5.3 Late communication entry					
R-5.3-001	R-5.3-002	R-5.3-003	R-5.3-004	R-5.3-005	
5.4 Receiving from multiple MCX Service communications					
5.4.1 Overview					
NA					
5.4.2 Requirements					
R-5.4.2-001	R-5.4.2-002	R-5.4.2-003	R-5.4.2-004	R-5.4.2-005	R-5.4.2-006

R-5.4.2-007	R-5.4.2-008	R-5.4.2-009			
5.5 Private Communication					
NA					
5.5.1 Private Communication general requirements					
NA					
5.5.2 Charging requirement for MCX Service					
R-5.5.2-001					
5.6 MCX Service priority requirements					
NA					
5.6.1 Overview					
NA					
5.6.2 Communication types based on priorities					
NA					
5.6.2.1 MCX Service Emergency and Imminent Peril general requirements					
NA					
5.6.2.1.1 Overview					
NA					
5.6.2.1.2 Requirements					
R-5.6.2.1.2-001	R-5.6.2.1.2-002	R-5.6.2.1.2-003	R-5.6.2.1.2-004	R-5.6.2.1.2-005	
5.6.2.2 MCX Service Emergency Group Communication					
NA					
5.6.2.2.1 MCX Service Emergency Group Communication requirements					
R-5.6.2.2.1-001	R-5.6.2.2.1-002	R-5.6.2.2.1-003	R-5.6.2.2.1-004	R-5.6.2.2.1-005	R-5.6.2.2.1-006
R-5.6.2.2.1-007	R-5.6.2.2.1-008	R-5.6.2.2.1-009	R-5.6.2.2.1-010	R-5.6.2.2.1-011	R-5.6.2.2.1-012
R-5.6.2.2.1-013	R-5.6.2.2.1-014				
5.6.2.2.2 MCX Service Emergency Group Communication cancellation requirements					
R-5.6.2.2.2-001	R-5.6.2.2.2-002	R-5.6.2.2.2-003	R-5.6.2.2.2-004	R-5.6.2.2.2-005	
5.6.2.3 MCX Service Imminent Peril Group					
NA					
5.6.2.3.1 MCX Service Imminent Peril Group Communication requirements					
R-5.6.2.3.1-001	R-5.6.2.3.1-002	R-5.6.2.3.1-003	R-5.6.2.3.1-004	R-5.6.2.3.1-005	R-5.6.2.3.1-006
R-5.6.2.3.1-007	R-5.6.2.3.1-008	R-5.6.2.3.1-009			
5.6.2.3.2 MCX Service Imminent Peril Group Communications cancellation requirements					
R-5.6.2.3.2-001	R-5.6.2.3.2-002	R-5.6.2.3.2-003	R-5.6.2.3.2-004		
5.6.2.4 MCX Service Emergency Alert					
NA					
5.6.2.4.1 MCX Service Emergency Alert requirements					
R-5.6.2.4.1-001	R-5.6.2.4.1-002	R-5.6.2.4.1-003	R-5.6.2.4.1-004	R-5.6.2.4.1-004a	R-5.6.2.4.1-005
R-5.6.2.4.1-006	R-5.6.2.4.1-007	R-5.6.2.4.1-008	R-5.6.2.4.1-009	R-5.6.2.4.1-010	R-5.6.2.4.1-011
R-5.6.2.4.1-012					
5.6.2.4.2 MCX Service Emergency Alert cancellation requirements					
R-5.6.2.4.2-001	R-5.6.2.4.2-002	R-5.6.2.4.2-003			
5.7 MCX Service User ID					
R-5.7-001	R-5.7-002	R-5.7-003			
5.8 MCX UE Management					

R-5.8-001	R-5.8-002				
5.9 MCX Service User Profile					
R-5.9-001	R-5.9-002				
5.9A Functional alias					
R-5.9a-001	R-5.9a-002	R-5.9a-003	R-5.9a-004	R-5.9a-005	R-5.9a-006
R-5.9a-007	R-5.9a-008	R-5.9a-009	R-5.9a-010	R-5.9a-011	R-5.9a-012
R-5.9a-013					
5.10 Support for multiple devices					
R-5.10-001	R-5.10-002				
5.11 Location					
R-5.11-001	R-5.11-002	R-5.11-003	R-5.11-004	R-5.11-005	R-5.11-006
R-5.11-007	R-5.11-008	R-5.11-009	R-5.11-010	R-5.11-011	R-5.11-012
R-5.11-013	R-5.11-014	R-5.11-015			
5.12 Security					
R-5.12-001	R-5.12-002	R-5.12-003	R-5.12-004	R-5.12-005	R-5.12-006
R-5.12-007	R-5.12-008	R-5.12-009	R-5.12-010	R-5.12-011	R-5.12-012
R-5.12-013	R5-12-014				
5.13 Media quality					
R-5.13-001					
5.14 Relay requirements					
R-5.14-001	R-5.14-002	R-5.14-003	R-5.14-004		
5.15 Gateway requirements					
R-5.15-001					
5.16 Control and management by Mission Critical Organizations					
NA					
5.16.1 Overview					
NA					
5.16.2 General requirements					
R-5.16.2-001	R-5.16.2-002	R-5.16.2-003	R-5.16.2-004	R-5.16.2-005	
5.16.3 Operational visibility for Mission Critical Organizations					
R-5.16.3-001					
5.17 General administrative – groups and users					
R-5.17-001	R-5.17-002	R-5.17-003	R-5.17-004	R-5.17-005	R-5.17-006
R-5.17-007	R-5.17-008				
5.18 Open interfaces for MCX services					
NA					
5.18.1 Overview					
NA					
5.18.2 Requirements					
NA					
5.19 Media forwarding					
NA					
5.19.1 Service description					
NA					
5.19.2 Requirements					
NA					

5.20 Receipt notification					
NA					
5.20.1 Service description					
NA					
5.20.2 Requirements					
NA					
5.21 Additional services for MCX Service communications					
NA					
5.21.1 Remotely initiated MCX Service communication					
NA					
5.21.1.1 Overview					
NA					
5.21.1.2 Requirements					
NA					
5.21.2 Remotely terminated MCX Service communication					
NA					
5.21.2.1 Requirements					
R-5.21.2.1-001					
6 MCX Service requirements specific to on-network use					
NA					
6.1 General administrative – groups and users					
R-6.1-001	R-6.1-002	R-6.1-003	R-6.1-004	R-6.1-005	
6.2 MCX Service communications					
NA					
6.2.1 Notification and acknowledgement for MCX Service Group Communications					
NA					
6.2.2 Queuing					
R-6.2.2-001	R-6.2.2-002	R-6.2.2-003	R-6.2.2-004	R-6.2.2-005	R-6.2.2-006
6.3 General requirements					
R-6.3-001	R-6.3-002	R-6.3-003	R-6.3-004		
6.4 General group communication					
NA					
6.4.1 General aspects					
R-6.4.1-001					
6.4.2 Group status/information					
R-6.4.2-005	R-6.4.2-001	R-6.4.2-002	R-6.4.2-003	R-6.4.2-004	R-6.4.2-006
R-6.4.2-007					
6.4.3 Identification					
R-6.4.3-001	R-6.4.3-002				
6.4.4 Membership/affiliation					
R-6.4.4-001	R-6.4.4-002				
6.4.5 Membership/affiliation list					
R-6.4.5-001	R-6.4.5-002	R-6.4.5-003	R-6.4.5-004	R-6.4.5-005	R-6.4.5-006
R-6.4.5-007	R-6.4.5-008				
6.4.6 Authorized user remotely changes another MCX User's affiliated and/or Selected MCX Service Group(s)					

NA					
6.4.6.1 Mandatory change					
R-6.4.6.1-001	R-6.4.6.1-002	R-6.4.6.1-003	R-6.4.6.1-004		
6.4.6.2 Negotiated change					
R-6.4.6.2-001	R-6.4.6.2-002	R-6.4.6.2-003	R-6.4.6.2-004	R-6.4.6.2-005	R-6.4.6.2-006
6.4.7 Prioritization					
R-6.4.7-001	R-6.4.7-002	R-6.4.7-003	R-6.4.7-004		
6.4.8 Relay requirements					
R-6.4.8-001					
6.4.9 Administrative					
R-6.4.9-001	R-6.4.9-002	R-6.4.9-003	R-6.4.9-004	R-6.4.9-005	R-6.4.9-006
6.5 Broadcast Group					
NA					
6.5.1 General Broadcast Group Communication					
R-6.5.1-001	R-6.5.1-002				
6.5.2 Group-Broadcast Group (e.g., announcement group)					
R-6.5.2-001					
6.5.3 User-Broadcast Group (e.g., system communication)					
R-6.5.3-001					
6.6 Dynamic group management (i.e., dynamic reporting)					
NA					
6.6.1 General dynamic regrouping					
R-6.6.1-001	R-6.6.1-002	R-6.6.1-003	R-6.6.1-004	R-6.6.1-005	R-6.6.1-006
6.6.2 Group regrouping					
NA					
6.6.2.1 Service description					
NA					
6.6.2.2 Requirements					
R-6.6.2.2-001	R-6.6.2.2-002	R-6.6.2.2-003	R-6.6.2.2-004	R-6.6.2.2-005	R-6.6.2.2-006
R-6.6.2.2-007					
6.6.3 Temporary Group-Broadcast Group					
R-6.6.3-001	R-6.6.3-002				
6.6.4 User regrouping					
NA					
6.6.4.1 Service description					
NA					
6.6.4.2 Requirements					
R-6.6.4.2-001	R-6.6.4.2-002	R-6.6.4.2-003	R-6.6.4.2-004	R-6.6.4.2-005	
6.7 Private Communication					
NA					
6.7.1 Overview					
NA					
6.7.2 General requirements					
R-6.7.2-001	R-6.7.2-002	R-6.7.2-003	R-6.7.2-004	R-6.7.2-005	
6.7.3 Administrative					
R-6.7.3-001	R-6.7.3-002	R-6.7.3-003	R-6.7.3-004	R-6.7.3-005	R-6.7.3-006

R-6.7.3-007	R-6.7.3-008				
6.7.4 Prioritization					
R-6.7.4-001	R-6.7.4-002	R-6.7.4-003	R-6.7.4-004	R-6.7.4-005	R-6.7.4-006
R-6.7.4-007					
6.7.5 Private Communication (without Floor control) commencement requirements					
R-6.7.5-001	R-6.7.5-002	R-6.7.5-003			
6.7.6 Private Communication (without Floor control) termination					
R-6.7.6-001	R-6.7.6-002				
6.8 MCX Service priority requirements					
NA					
6.8.1 General					
R-6.8.1-001	R-6.8.1-002	R-6.8.1-003	R-6.8.1-004	R-6.8.1-005	R-6.8.1-006
R-6.8.1-007	R-6.8.1-008	R-6.8.1-009	R-6.8.1-010	R-6.8.1-011	R-6.8.1-012
R-6.8.1-013	R-6.8.1-014	R-6.8.1-015	R-6.8.1-016		
6.8.2 3GPP system access controls					
R-6.8.2-001					
6.8.3 3GPP system admission controls					
R-6.8.3-001					
6.8.4 3GPP system scheduling controls					
R-6.8.4-001					
6.8.5 UE access controls					
R-6.8.5-001					
6.8.6 Mobility and load management					
NA					
6.8.6.1 Mission Critical mobility management according to priority					
R-6.8.6.1-001	R-6.8.6.1-002				
6.8.6.2 Load management					
R-6.8.6.2-001	R-6.8.6.2-002	R-6.8.6.2-003	R-6.8.6.2-004	R-6.8.6.2-005	
6.8.7 Application layer priorities					
NA					
6.8.7.1 Overview					
NA					
6.8.7.2 Requirements					
R-6.8.7.2-001	R-6.8.7.2-002	R-6.8.7.2-003	R-6.8.7.2-004	R-6.8.7.2-005	
6.8.8 Communication types based on priorities					
NA					
6.8.8.1 MCX Service Emergency Group Communication requirements					
R-6.8.8.1-001	R-6.8.8.1-002	R-6.8.8.1-003	R-6.8.8.1-004		
6.8.8.2 MCX Service Emergency Private Communication requirements					
NA					
6.8.8.3 Imminent Peril Group Communication requirements					
R-6.8.8.3-001	R-6.8.8.3-002	R-6.8.8.3-003			
6.8.8.4 MCX Service Emergency Alert					
NA					
6.8.8.4.1 Requirements					
R-6.8.8.4.1-001	R-6.8.8.4.1-002	R-6.8.8.4.1-003	R-6.8.8.4.1-004	R-6.8.8.4.1-005	R-6.8.8.4.1-006

6.8.8.4.2 MCX Service Emergency Alert cancellation requirements					
R-6.8.8.4.2-001	R-6.8.8.4.2-002				
6.9 IDs and aliases					
R-6.9-001	R-6.9-002	R-6.9-003	R-6.9-004		
6.10 User Profile management					
R-6.10-001	R-6.10-002	R-6.10-003	R-6.10-004		
6.11 Support for multiple devices					
R-6.11-001	R-6.11-002	R-6.11-003			
6.12 Location					
R-6.12-001	R-6.12-002	R-6.12-003	R-6.12-004	R-6.12-005	R-6.12-006
R-6.12-007					
6.13 Security					
NA					
6.13.1 Overview					
NA					
6.13.2 Cryptographic protocols					
R-6.13.2-001	R-6.13.2-002	R-6.13.2-003			
6.13.3 Authentication					
R-6.13.3-001					
6.13.4 Access control					
R-6.13.4-001	R-6.13.4-002	R-6.13.4-003	R-6.13.4-004	R-6.13.4-005	R-6.13.4-006
R-6.13.4-007	R-6.13.4-008	R-6.13.4-009	R-6.13.4-010		
6.13.5 Regulatory issues					
R-6.13.5-001					
6.13.6 Storage control					
NA					
6.14 Interactions for MCX Service Group Communications and MCX Service Private Communications					
R-6.14-001	R-6.14-002				
6.15 Additional services for MCX Service communications					
NA					
6.15.1 Discreet listening capabilities					
R-6.15.1-001					
6.15.2 Ambient listening					
NA					
6.15.2.1 Overview of ambient listening					
NA					
6.15.2.2 Ambient listening requirements					
NA					
6.15.2.2.1 General ambient listening requirements					
R-6.15.2.2.1-001	R-6.15.2.2.1-002	R-6.15.2.2.1-003			
6.15.2.2.2 Remotely initiated ambient listening requirements					
R-6.15.2.2.2-001	R-6.15.2.2.2-002				
6.15.2.2.3 Locally initiated ambient listening requirements					
R-6.15.2.2.3-001	R-6.15.2.2.3-002				

6.15.3 Remotely initiated MCX Service Communication					
NA					
6.15.3.1 Overview					
NA					
6.15.3.2 Requirements					
R-6.15.3.2-001	R-6.15.3.2-002	R-6.15.3.2-003	R-6.15.3.2-004		
6.15.4 Recording and audit requirements					
R-6.15.4-001	R-6.15.4-002	R-6.15.4-003	R-6.15.4-004	R-6.15.4-005	R-6.15.4-006
R-6.15.4-007	R-6.15.4-008	R-6.15.4-009	R-6.15.4-010		
6.16 Interaction with telephony services					
R-6.16-001	R-6.16-002				
6.17 Interworking					
NA					
6.17.1 Non-3GPP access					
R-6.17.1-001					
6.17.2 Interworking between MCX Service systems					
R-6.17.2-001	R-6.17.2-002	R-6.17.2-003	R-6.17.2-004	R-6.17.2-005	R-6.17.2-006
R-6.17.2-007					
6.18 MCX Service coverage extension using ProSe UE-to-Network Relays					
R-6.18-001	R-6.18-002	R-6.18-003	R-6.18-004	R-6.18-005	R-6.18-006
6.19 Additional MCX Service requirements					
NA					
6.19.1 Communication rejection and queuing					
NA					
6.19.1.1 Requirements					
R-6.19.1.1-001	R-6.19.1.1-002	R-6.19.1.1-003	R-6.19.1.1-004	R-6.19.1.1-005	R-6.19.1.1-006
R-6.19.1.1-007					
7 MCX Service requirements specific to off-network use					
NA					
7.1 Off-network communications overview					
NA					
7.2 General off-network MCX Service requirements					
R-7.2-001	R-7.2-002	R-7.2-003	R-7.2-004	R-7.2-005	
7.3 Admission control					
NA					
7.3.1 General aspects					
R-7.3.1-001	R-7.3.1-002	R-7.3.1-003			
7.3.2 Communication initiation					
R-7.3.2-001	R-7.3.2-002	R-7.3.2-003	R-7.3.2-004	R-7.3.2-005	
7.4 Communication termination					
R-7.4-001	R-7.4-002	R-7.4-003	R-7.4-004		
7.5 Broadcast Group					
R-7.5-001	R-7.5-002				
7.6 MCX Service priority requirements					
R-7.6-001	R-7.6-002	R-7.6-003	R-7.6-004	R-7.6-005	R-7.6-006
R-7.6-007	R-7.6-008	R-7.6-009			

7.7 Communication types based on priorities					
NA					
7.7.1 MCX Service Emergency Group Communication requirements					
R-7.7.1-001	R-7.7.1-002	R-7.7.1-003			
7.7.2 MCX Service Emergency Group Communication cancellation requirements					
R-7.7.2-001					
7.7.3 Imminent Peril Communication					
NA					
7.7.3.1 Imminent Peril Group Communication requirements					
R-7.7.3.1-001	R-7.7.3.1-002	R-7.7.3.1-003	R-7.7.3.1-004	R-7.7.3.1-005	
7.7.3.2 Imminent Peril Group Communication cancellation requirements					
R-7.7.3.2-001	R-7.7.3.2-002				
7.8 Location					
R-7.8-001					
7.9 Security					
R-7.9-001	R-7.9-002				
7.10 Off-network MCX Service operations					
R-7.10-001	R-7.10-002	R-7.10-003			
7.11 Off-network UE functionality					
R-7.11-001	R-7.11-002	R-7.11-003			
7.12 Streaming for ProSe UE-to-UE Relay and UE-to-Network Relay					
NA					
7.12.1 UE-to-Network Relay for all data types					
R-7.12.1-001	R-7.12.1-002	R-7.12.1-003	R-7.12.1-004		
7.12.2 UE-to-UE Relay streaming					
R-7.12.2-001	R-7.12.2-002	R-7.12.2-003			
7.12.3 Off-Network streaming					
R-7.12.3-001	R-7.12.3-002	R-7.12.3-003			
7.13 Switching to off-network MCX Service					
R-7.13-001	R-7.13-002	R-7.13-003	R-7.13-004	R-7.13-005	
7.14 Off-network recording and audit requirements					
R-7.14-001	R-7.14-002				
7.15 Off-network UE-to-UE relay					
NA					
7.15.1 Private Communications					
R-7.15.1-001	R-7.15.1-002	R-7.15.1-003			
7.15.2 Group Communications					
R-7.15.2-001	R-7.15.2-002				
8 Inter-MCX Service interworking					
NA					
8.1 Inter-MCX Service interworking overview					
NA					
8.2 Concurrent operation of different MCX Services					
NA					
8.2.1 Overview					
NA					

8.2.2 Requirements					
R-8.2.2-001	R-8.2.2-002	R-8.2.2-003	R-8.2.2-004	R-8.2.2-005	R-8.2.2-006
R-8.2.2-007					
8.3 Use of unsharable resources within a UE					
R-8.3-001	R-8.3-002	R-8.3-003	R-8.3-004	R-8.3-005	R-8.3-006
8.4 Single group with multiple MCX Services					
NA					
8.4.1 Overview					
NA					
8.4.2 Requirements					
R-8.4.2-001	R-8.4.2-002	R-8.4.2-003	R-8.4.2-004	R-8.4.2-005	
8.4.3 Compatibility of UE					
NA					
8.4.3.1 Advertising service capabilities required					
R-8.4.3.1-001	R-8.4.3.1-002	R-8.4.3.1-003	R-8.4.3.1-004		
8.4.3.2 Conversion between capabilities					
R-8.4.3.2-001					
8.4.4 Individual permissions for service access					
R-8.4.4-001					
8.4.5 Common alias and user identities or mappable					
R-8.4.5-001					
8.4.6 Single location message					
R-8.4.6-001	R-8.4.6-002	R-8.4.6-003			
8.5 Priority between services					
NA					
8.5.1 Overview					
NA					
8.5.2 Requirements					
R-8.5.2-001	R-8.5.2-002	R-8.5.2-003	R-8.5.2-004	R-8.5.2-005	
9 Air Ground Air Communications					
NA					
9.1 Service description					
NA					
9.2 Requirements					
R-9.2-001					
10 MCX Service in IOPS mode					
R-10-001					

Annex B (normative): MCCoRe Requirements for MCVideo

Table B.1 provides an exhaustive list of those requirements in 3GPP TS 22.280 that are applicable to MCVideo.

Table B.1

5 MCX Service Requirements common for on the network and off the network					
NA					
5.1 General Group Communications requirements					
NA					
5.1.1 General aspects					
R-5.1.1-001	R-5.1.1-002	R-5.1.1-003	R-5.1.1-004	R-5.1.1-005	R-5.1.1-006
5.1.2 Group/status information					
R-5.1.2-001	R-5.1.2-002				
5.1.3 Group configuration					
R-5.1.3-001	R5.1.3-002				
5.1.4 Identification					
R-5.1.4-001					
5.1.5 Membership/affiliation					
R-5.1.5-001	R-5.1.5-002	R-5.1.5-003	R-5.1.5-004	R-5.1.5-005	R-5.1.5-006
R-5.1.5-007	R-5.1.5-008				
5.1.6 Group Communication administration					
R-5.1.6-001					
5.1.7 Prioritization					
R-5.1.7-001	R-5.1.7-002				
5.1.8 Charging requirements for MCX Service					
R-5.1.8-001	R-5.1.8-003	R-5.1.8-004	R-5.1.8-005	R-5.1.8-006	R-5.1.8-007
R-5.1.8-008	R-5.1.8-009	R-5.1.8-010	R-5.1.8-011		
5.1.9 MCX Service Emergency Alert triggered by location					
R-5.1.9-001	R-5.1.9-002				
5.2 Broadcast Group					
NA					
5.2.1 General Broadcast Group Communication					
R-5.2.1-001	R-5.2.1-002				
5.2.2 Group-Broadcast Group (e.g., announcement group)					
R-5.2.2-001	R-5.2.2-002	R-5.2.2-003	R-5.2.2-004		
5.2.3 User-Broadcast Group (e.g., System Communication)					
R-5.2.3-001	R-5.2.3-002				
5.3 Late communication entry					
R-5.3-001	R-5.3-002	R-5.3-003	R-5.3-004	R-5.3-005	
5.4 Receiving from multiple MCX Service communications					
5.4.1 Overview					
NA					
5.4.2 Requirements					
R-5.4.2-001	R-5.4.2-002	R-5.4.2-003	R-5.4.2-004	R-5.4.2-005	R-5.4.2-006

R-5.4.2-007	R-5.4.2-008	R-5.4.2-009			
5.5 Private Communication					
NA					
5.5.1 Private Communication general requirements					
R-5.5.1-001					
5.5.2 Charging requirement for MCX Service					
R-5.5.2-001					
5.6 MCX Service priority requirements					
NA					
5.6.1 Overview					
NA					
5.6.2 Communication types based on priorities					
NA					
5.6.2.1 MCX Service Emergency and Imminent Peril general requirements					
NA					
5.6.2.1.1 Overview					
NA					
5.6.2.1.2 Requirements					
R-5.6.2.1.2-001	R-5.6.2.1.2-002	R-5.6.2.1.2-003	R-5.6.2.1.2-004	R-5.6.2.1.2-005	
5.6.2.2 MCX Service Emergency Group Communication					
NA					
5.6.2.2.1 MCX Service Emergency Group Communication requirements					
R-5.6.2.2.1-001	R-5.6.2.2.1-002	R-5.6.2.2.1-003	R-5.6.2.2.1-004	R-5.6.2.2.1-005	R-5.6.2.2.1-006
R-5.6.2.2.1-007	R-5.6.2.2.1-008	R-5.6.2.2.1-009	R-5.6.2.2.1-010	R-5.6.2.2.1-011	R-5.6.2.2.1-012
R-5.6.2.2.1-013	R-5.6.2.2.1-014				
5.6.2.2.2 MCX Service Emergency Group Communication cancellation requirements					
R-5.6.2.2.2-001	R-5.6.2.2.2-002	R-5.6.2.2.2-003	R-5.6.2.2.2-004	R-5.6.2.2.2-005	
5.6.2.3 MCX Service Imminent Peril Group					
NA					
5.6.2.3.1 MCX Service Imminent Peril Group Communication requirements					
R-5.6.2.3.1-001	R-5.6.2.3.1-002	R-5.6.2.3.1-003	R-5.6.2.3.1-004	R-5.6.2.3.1-005	R-5.6.2.3.1-006
R-5.6.2.3.1-007	R-5.6.2.3.1-008	R-5.6.2.3.1-009			
5.6.2.3.2 MCX Service Imminent Peril Group Communications cancellation requirements					
R-5.6.2.3.2-001	R-5.6.2.3.2-002	R-5.6.2.3.2-003	R-5.6.2.3.2-004		
5.6.2.4 MCX Service Emergency Alert					
NA					
5.6.2.4.1 MCX Service Emergency Alert requirements					
R-5.6.2.4.1-001	R-5.6.2.4.1-002	R-5.6.2.4.1-003	R-5.6.2.4.1-004	R-5.6.2.4.1-004a	R-5.6.2.4.1-005
R-5.6.2.4.1-006	R-5.6.2.4.1-007	R-5.6.2.4.1-008	R-5.6.2.4.1-009	R-5.6.2.4.1-010	R-5.6.2.4.1-011
R-5.6.2.4.1-012					
5.6.2.4.2 MCX Service Emergency Alert cancellation requirements					
R-5.6.2.4.2-001	R-5.6.2.4.2-002	R-5.6.2.4.2-003			
5.7 MCX Service User ID					
R-5.7-001	R-5.7-002	R-5.7-003			
5.8 MCX UE Management					

R-5.8-001	R-5.8-002				
5.9 MCX Service User Profile					
R-5.9-001	R-5.9-002				
5.9A Functional alias					
R-5.9a-001	R-5.9a-002	R-5.9a-003	R-5.9a-004	R-5.9a-005	R-5.9a-006
R-5.9a-007	R-5.9a-008	R-5.9a-009	R-5.9a-010	R-5.9a-011	R-5.9a-012
R-5.9a-013					
5.10 Support for multiple devices					
R-5.10-001	R-5.10-002				
5.11 Location					
R-5.11-001	R-5.11-002	R-5.11-003	R-5.11-004	R-5.11-005	R-5.11-006
R-5.11-007	R-5.11-008	R-5.11-009	R-5.11-010	R-5.11-011	R-5.11-012
R-5.11-013	R-5.11-014	R-5.11-015			
5.12 Security					
R-5.12-001	R-5.12-002	R-5.12-003	R-5.12-004	R-5.12-005	R-5.12-006
R-5.12-007	R-5.12-008	R-5.12-009	R-5.12-010	R-5.12-011	R-5.12-012
R-5.12-013	R-5.12-014				
5.13 Media quality					
R-5.13-001					
5.14 Relay requirements					
R-5.14-001	R-5.14-002	R-5.14-003	R-5.14-004		
5.15 Gateway requirements					
R-5.15-001					
5.16 Control and management by Mission Critical Organizations					
NA					
5.16.1 Overview					
NA					
5.16.2 General requirements					
R-5.16.2-001	R-5.16.2-002	R-5.16.2-003	R-5.16.2-004	R-5.16.2-005	
5.16.3 Operational visibility for Mission Critical Organizations					
R-5.16.3-001					
5.17 General administrative – groups and users					
R-5.17-001	R-5.17-002	R-5.17-003	R-5.17-004	R-5.17-005	R-5.17-006
R-5.17-007	R-5.17-008				
5.18 Open interfaces for MCX services					
NA					
5.18.1 Overview					
NA					
5.18.2 Requirements					
R-5.18.2-001	R-5.18.2-002	R-5.18.2-003	R-5.18.2-004		
5.19 Media forwarding					
NA					
5.19.1 Service description					
NA					
5.19.2 Requirements					
R-5.19.2-001	R-5.19.2-002	R-5.19.2-003			

5.20 Receipt notification					
NA					
5.20.1 Service description					
NA					
5.20.2 Requirements					
R-5.20.2-001					
5.21 Additional services for MCX Service communications					
NA					
5.21.1 Remotely initiated MCX Service communication					
NA					
5.21.1.1 Overview					
NA					
5.21.1.2 Requirements					
R-5.21.1.2-001	R-5.21.1.2-002	R-5.21.1.2-003	R-5.21.1.2-004		
5.21.2 Remotely terminated MCX Service communication					
NA					
5.21.2.1 Requirements					
R-5.21.2.1-001					
6 MCX Service requirements specific to on-network use					
NA					
6.1 General administrative – groups and users					
R-6.1-001	R-6.1-002	R-6.1-003	R-6.1-004	R-6.1-005	
6.2 MCX Service communications					
NA					
6.2.1 Notification and acknowledgement for MCX Service Group Communications					
R-6.2.1-001	R-6.2.1-002	R-6.2.1-003	R-6.2.1-004	R-6.2.1-005	
6.2.2 Queuing					
R-6.2.2-001	R-6.2.2-002	R-6.2.2-003	R-6.2.2-004	R-6.2.2-005	R-6.2.2-006
6.3 General requirements					
R-6.3-001	R-6.3-002	R-6.3-003	R-6.3-004		
6.4 General group communication					
NA					
6.4.1 General aspects					
R-6.4.1-001					
6.4.2 Group status/information					
R-6.4.2-005	R-6.4.2-001	R-6.4.2-002	R-6.4.2-003	R-6.4.2-004	R-6.4.2-006
R-6.4.2-007					
6.4.3 Identification					
R-6.4.3-001	R-6.4.3-002				
6.4.4 Membership/affiliation					
R-6.4.4-001	R-6.4.4-002				
6.4.5 Membership/affiliation list					
R-6.4.5-001	R-6.4.5-002	R-6.4.5-003	R-6.4.5-004	R-6.4.5-005	R-6.4.5-006
R-6.4.5-007	R-6.4.5-008				
6.4.6 Authorized user remotely changes another MCX User's affiliated and/or Selected MCX Service Group(s)					

NA					
6.4.6.1 Mandatory change					
R-6.4.6.1-001	R-6.4.6.1-002	R-6.4.6.1-003	R-6.4.6.1-004		
6.4.6.2 Negotiated change					
R-6.4.6.2-001	R-6.4.6.2-002	R-6.4.6.2-003	R-6.4.6.2-004	R-6.4.6.2-005	R-6.4.6.2-006
6.4.7 Prioritization					
R-6.4.7-001	R-6.4.7-002	R-6.4.7-003	R-6.4.7-004		
6.4.8 Relay requirements					
R-6.4.8-001					
6.4.9 Administrative					
R-6.4.9-001	R-6.4.9-002	R-6.4.9-003	R-6.4.9-004	R-6.4.9-005	R-6.4.9-006
6.5 Broadcast Group					
NA					
6.5.1 General Broadcast Group Communication					
R-6.5.1-001	R-6.5.1-002				
6.5.2 Group-Broadcast Group (e.g., announcement group)					
R-6.5.2-001					
6.5.3 User-Broadcast Group (e.g., system communication)					
R-6.5.3-001					
6.6 Dynamic group management (i.e., dynamic reporting)					
NA					
6.6.1 General dynamic regrouping					
R-6.6.1-001	R-6.6.1-002	R-6.6.1-003	R-6.6.1-004	R-6.6.1-005	R-6.6.1-006
6.6.2 Group regrouping					
NA					
6.6.2.1 Service description					
NA					
6.6.2.2 Requirements					
R-6.6.2.2-001	R-6.6.2.2-002	R-6.6.2.2-003	R-6.6.2.2-004	R-6.6.2.2-005	R-6.6.2.2-006
R-6.6.2.2-007					
6.6.3 Temporary Group-Broadcast Group					
R-6.6.3-001	R-6.6.3-002				
6.6.4 User regrouping					
NA					
6.6.4.1 Service description					
NA					
6.6.4.2 Requirements					
R-6.6.4.2-001	R-6.6.4.2-002	R-6.6.4.2-003	R-6.6.4.2-004	R-6.6.4.2-005	
6.7 Private Communication					
NA					
6.7.1 Overview					
NA					
6.7.2 General requirements					
R-6.7.2-001	R-6.7.2-002	R-6.7.2-003	R-6.7.2-004	R-6.7.2-005	
6.7.3 Administrative					
R-6.7.3-001	R-6.7.3-002	R-6.7.3-003	R-6.7.3-004	R-6.7.3-005	R-6.7.3-006

R-6.7.3-007	R-6.7.3-008				
6.7.4 Prioritization					
R-6.7.4-001	R-6.7.4-002	R-6.7.4-003	R-6.7.4-004	R-6.7.4-005	R-6.7.4-006
R-6.7.4-007					
6.7.5 Private Communication (without Floor control) commencement requirements					
R-6.7.5-001	R-6.7.5-002	R-6.7.5-003			
6.7.6 Private Communication (without Floor control) termination					
R-6.7.6-001	R-6.7.6-002				
6.8 MCX Service priority requirements					
NA					
6.8.1 General					
R-6.8.1-001	R-6.8.1-002	R-6.8.1-003	R-6.8.1-004	R-6.8.1-005	R-6.8.1-006
R-6.8.1-007	R-6.8.1-008	R-6.8.1-009	R-6.8.1-010	R-6.8.1-011	R-6.8.1-012
R-6.8.1-013	R-6.8.1-014	R-6.8.1-015	R-6.8.1-016		
6.8.2 3GPP system access controls					
R-6.8.2-001					
6.8.3 3GPP system admission controls					
R-6.8.3-001					
6.8.4 3GPP system scheduling controls					
R-6.8.4-001					
6.8.5 UE access controls					
R-6.8.5-001					
6.8.6 Mobility and load management					
NA					
6.8.6.1 Mission Critical mobility management according to priority					
R-6.8.6.1-001	R-6.8.6.1-002				
6.8.6.2 Load management					
R-6.8.6.2-001	R-6.8.6.2-002	R-6.8.6.2-003	R-6.8.6.2-004	R-6.8.6.2-005	
6.8.7 Application layer priorities					
NA					
6.8.7.1 Overview					
NA					
6.8.7.2 Requirements					
R-6.8.7.2-001	R-6.8.7.2-002	R-6.8.7.2-003	R-6.8.7.2-004	R-6.8.7.2-005	
6.8.8 Communication types based on priorities					
NA					
6.8.8.1 MCX Service Emergency Group Communication requirements					
R-6.8.8.1-001	R-6.8.8.1-002	R-6.8.8.1-003	R-6.8.8.1-004		
6.8.8.2 MCX Service Emergency Private Communication requirements					
R-6.8.8.2-001	R-6.8.8.2-002	R-6.8.8.2-003	R-6.8.8.2-004		
6.8.8.3 Imminent Peril Group Communication requirements					
R-6.8.8.3-001	R-6.8.8.3-002	R-6.8.8.3-003			
6.8.8.4 MCX Service Emergency Alert					
NA					
6.8.8.4.1 Requirements					
R-6.8.8.4.1-001	R-6.8.8.4.1-002	R-6.8.8.4.1-003	R-6.8.8.4.1-004	R-6.8.8.4.1-005	R-6.8.8.4.1-006

6.8.8.4.2 MCX Service Emergency Alert cancellation requirements					
R-6.8.8.4.2-001	R-6.8.8.4.2-002				
6.9 IDs and aliases					
R-6.9-001	R-6.9-002	R-6.9-003	R-6.9-004		
6.10 User Profile management					
R-6.10-001	R-6.10-002	R-6.10-003	R-6.10-004		
6.11 Support for multiple devices					
R-6.11-001	R-6.11-002	R-6.11-003			
6.12 Location					
R-6.12-001	R-6.12-002	R-6.12-003	R-6.12-004	R-6.12-005	R-6.12-006
R-6.12-007					
6.13 Security					
NA					
6.13.1 Overview					
NA					
6.13.2 Cryptographic protocols					
R-6.13.2-001	R-6.13.2-002	R-6.13.2-003			
6.13.3 Authentication					
R-6.13.3-001					
6.13.4 Access control					
R-6.13.4-001	R-6.13.4-002	R-6.13.4-003	R-6.13.4-004	R-6.13.4-005	R-6.13.4-006
R-6.13.4-007	R-6.13.4-008	R-6.13.4-009	R-6.13.4-010		
6.13.5 Regulatory issues					
R-6.13.5-001					
6.13.6 Storage control					
R-6.13.6-001					
6.14 Interactions for MCX Service Group Communications and MCX Service Private Communications					
R-6.14-001	R-6.14-002				
6.15 Additional services for MCX Service communications					
NA					
6.15.1 Discreet listening capabilities					
R-6.15.1-001					
6.15.2 Ambient listening					
NA					
6.15.2.1 Overview of ambient listening					
NA					
6.15.2.2 Ambient listening requirements					
NA					
6.15.2.2.1 General ambient listening requirements					
R-6.15.2.2.1-001	R-6.15.2.2.1-002	R-6.15.2.2.1-003			
6.15.2.2.2 Remotely initiated ambient listening requirements					
R-6.15.2.2.2-001	R-6.15.2.2.2-002				
6.15.2.2.3 Locally initiated ambient listening requirements					
R-6.15.2.2.3-001	R-6.15.2.2.3-002				

6.15.3 Remotely initiated MCX Service Communication					
NA					
6.15.3.1 Overview					
NA					
6.15.3.2 Requirements					
R-6.15.3.2-001	R-6.15.3.2-002	R-6.15.3.2-003	R-6.15.3.2-004		
6.15.4 Recording and audit requirements					
R-6.15.4-001	R-6.15.4-002	R-6.15.4-003	R-6.15.4-004	R-6.15.4-005	R-6.15.4-006
R-6.15.4-007	R-6.15.4-008	R-6.15.4-009	R-6.15.4-010		
6.16 Interaction with telephony services					
R-6.16-001	R-6.16-002				
6.17 Interworking					
NA					
6.17.1 Non-3GPP access					
R-6.17.1-001					
6.17.2 Interworking between MCX Service systems					
R-6.17.2-001	R-6.17.2-002	R-6.17.2-003	R-6.17.2-004	R-6.17.2-005	R-6.17.2-006
R-6.17.2-007					
6.18 MCX Service coverage extension using ProSe UE-to-Network Relays					
R-6.18-001	R-6.18-002	R-6.18-003	R-6.18-004	R-6.18-005	R-6.18-006
6.19 Additional MCX Service requirements					
NA					
6.19.1 Communication rejection and queuing					
NA					
6.19.1.1 Requirements					
R-6.19.1.1-001	R-6.19.1.1-002	R-6.19.1.1-003	R-6.19.1.1-004	R-6.19.1.1-005	R-6.19.1.1-006
R-6.19.1.1-007					
7 MCX Service requirements specific to off-network use					
NA					
7.1 Off-network communications overview					
NA					
7.2 General off-network MCX Service requirements					
R-7.2-001	R-7.2-002	R-7.2-003	R-7.2-004	R-7.2-005	
7.3 Admission control					
NA					
7.3.1 General aspects					
R-7.3.1-001	R-7.3.1-002	R-7.3.1-003			
7.3.2 Communication initiation					
R-7.3.2-001	R-7.3.2-002	R-7.3.2-003	R-7.3.2-004	R-7.3.2-005	
7.4 Communication termination					
R-7.4-001	R-7.4-002	R-7.4-003	R-7.4-004		
7.5 Broadcast Group					
R-7.5-001	R-7.5-002				
7.6 MCX Service priority requirements					
R-7.6-001	R-7.6-002	R-7.6-003	R-7.6-004	R-7.6-005	R-7.6-006
R-7.6-007	R-7.6-008	R-7.6-009			

7.7 Communication types based on priorities					
NA					
7.7.1 MCX Service Emergency Group Communication requirements					
R-7.7.1-001	R-7.7.1-002	R-7.7.1-003			
7.7.2 MCX Service Emergency Group Communication cancellation requirements					
R-7.7.2-001					
7.7.3 Imminent Peril Communication					
NA					
7.7.3.1 Imminent Peril Group Communication requirements					
R-7.7.3.1-001	R-7.7.3.1-002	R-7.7.3.1-003	R-7.7.3.1-004	R-7.7.3.1-005	
7.7.3.2 Imminent Peril Group Communication cancellation requirements					
R-7.7.3.2-001	R-7.7.3.2-002				
7.8 Location					
R-7.8-001					
7.9 Security					
R-7.9-001	R-7.9-002				
7.10 Off-network MCX Service operations					
R-7.10-001	R-7.10-002	R-7.10-003			
7.11 Off-network UE functionality					
R-7.11-001	R-7.11-002	R-7.11-003			
7.12 Streaming for ProSe UE-to-UE Relay and UE-to-Network Relay					
NA					
7.12.1 UE-to-Network Relay for all data types					
R-7.12.1-001	R-7.12.1-002	R-7.12.1-003	R-7.12.1-004		
7.12.2 UE-to-UE Relay streaming					
R-7.12.2-001	R-7.12.2-002	R-7.12.2-003			
7.12.3 Off-Network streaming					
R-7.12.3-001	R-7.12.3-002	R-7.12.3-003			
7.13 Switching to off-network MCX Service					
R-7.13-001	R-7.13-002	R-7.13-003	R-7.13-004	R-7.13-005	
7.14 Off-network recording and audit requirements					
R-7.14-001	R-7.14-002				
7.15 Off-network UE-to-UE relay					
NA					
7.15.1 Private Communications					
R-7.15.1-001	R-7.15.1-002	R-7.15.1-003			
7.15.2 Group Communications					
R-7.15.2-001	R-7.15.2-002				
8 Inter-MCX Service interworking					
NA					
8.1 Inter-MCX Service interworking overview					
NA					
8.2 Concurrent Operation of Different MCX Services					
NA					
8.2.1 Overview					
NA					

8.2.2 Requirements					
R-8.2.2-001	R-8.2.2-002	R-8.2.2-003	R-8.2.2-004	R-8.2.2-005	R-8.2.2-006
R-8.2.2-007					
8.3 Use of unsharable resources within a UE					
R-8.3-001	R-8.3-002	R-8.3-003	R-8.3-004	R-8.3-005	R-8.3-006
8.4 Single Group with multiple MCX Services					
NA					
8.4.1 Overview					
NA					
8.4.2 Requirements					
R-8.4.2-001	R-8.4.2-002	R-8.4.2-003	R-8.4.2-004	R-8.4.2-005	
8.4.3 Compatibility of UE					
NA					
8.4.3.1 Advertising service capabilities required					
R-8.4.3.1-001	R-8.4.3.1-002	R-8.4.3.1-003	R-8.4.3.1-004		
8.4.3.2 Conversion between capabilities					
R-8.4.3.2-001					
8.4.4 Individual permissions for service access					
R-8.4.4-001					
8.4.5 Common alias and user identities or mappable					
R-8.4.5-001					
8.4.6 Single location message					
R-8.4.6-001	R-8.4.6-002	R-8.4.6-003			
8.5 Priority between services					
NA					
8.5.1 Overview					
NA					
8.5.2 Requirements					
R-8.5.2-001	R-8.5.2-002	R-8.5.2-003	R-8.5.2-004	R-8.5.2-005	
9 Air Ground Air Communications					
NA					
9.1 Service description					
NA					
9.2 Requirements					
R-9.2-001					
10 MCX Service in IOPS mode					
R-10-001					

Annex C (normative): MCCoRe Requirements for MCData

Table C.1 provides an exhaustive list of those requirements in 3GPP TS 22.280 that are applicable to MCData.

Table C.1

5 MCX Service requirements common for on the network and off the network					
NA					
5.1 General Group Communications requirements					
NA					
5.1.1 General aspects					
R-5.1.1-001	R-5.1.1-002	R-5.1.1-003	R-5.1.1-006		
5.1.2 Group/status information					
NA					
5.1.3 Group configuration					
R-5.1.3-001	R5.1.3-002				
5.1.4 Identification					
R-5.1.4-001					
5.1.5 Membership/affiliation					
R-5.1.5-001	R-5.1.5-002	R-5.1.5-003	R-5.1.5-005	R-5.1.5-007	R-5.1.5-008
5.1.6 Group Communication administration					
NA					
5.1.7 Prioritization					
R-5.1.7-001	R-5.1.7-002				
5.1.8 Charging requirements for MCX Service					
R-5.1.8-001	R-5.1.8-003	R-5.1.8-004	R-5.1.8-005	R-5.1.8-006	R-5.1.8-007
R-5.1.8-008	R-5.1.8-009	R-5.1.8-010	R-5.1.8-011		
5.1.9 MCX Service Emergency Alert triggered by location					
R-5.1.9-001	R-5.1.9-002				
5.2 Broadcast Group					
NA					
5.2.1 General Broadcast Group Communication					
R-5.2.1-002					
5.2.2 Group-Broadcast Group (e.g., announcement group)					
R-5.2.2-001	R-5.2.2-002	R-5.2.2-003	R-5.2.2-004		
5.2.3 User-Broadcast Group (e.g., System Communication)					
R-5.2.3-001	R-5.2.3-002				
5.3 Late communication entry					
NA					
5.4 Receiving from multiple MCX Service communications					
5.4.1 Overview					
NA					
5.4.2 Requirements					
R-5.4.2-001	R-5.4.2-004	R-5.4.2-005	R-5.4.2-006	R-5.4.2-007	R-5.4.2-008
R-5.4.2-009					

5.5 Private Communication					
NA					
5.5.1 Private Communication general requirements					
R-5.5.1-001					
5.5.2 Charging requirement for MCX Service					
R-5.5.2-001					
5.6 MCX Service priority requirements					
NA					
5.6.1 Overview					
NA					
5.6.2 Communication types based on priorities					
NA					
5.6.2.1 MCX Service Emergency and Imminent Peril general requirements					
NA					
5.6.2.1.1 Overview					
NA					
5.6.2.1.2 Requirements					
R-5.6.2.1.2-001	R-5.6.2.1.2-002	R-5.6.2.1.2-003	R-5.6.2.1.2-004	R-5.6.2.1.2-005	
5.6.2.2 MCX Service Emergency Group Communication					
NA					
5.6.2.2.1 MCX Service Emergency Group Communication requirements					
R-5.6.2.2.1-001	R-5.6.2.2.1-002	R-5.6.2.2.1-003	R-5.6.2.2.1-004	R-5.6.2.2.1-005	R-5.6.2.2.1-006
R-5.6.2.2.1-007	R-5.6.2.2.1-008	R-5.6.2.2.1-009	R-5.6.2.2.1-010	R-5.6.2.2.1-011	R-5.6.2.2.1-012
R-5.6.2.2.1-013	R-5.6.2.2.1-014				
5.6.2.2.2 MCX Service Emergency Group Communication cancellation requirements					
R-5.6.2.2.2-001	R-5.6.2.2.2-002	R-5.6.2.2.2-003	R-5.6.2.2.2-004	R-5.6.2.2.2-005	
5.6.2.3 MCX Service Imminent Peril Group					
NA					
5.6.2.3.1 MCX Service Imminent Peril Group Communication requirements					
R-5.6.2.3.1-001	R-5.6.2.3.1-002	R-5.6.2.3.1-003	R-5.6.2.3.1-004	R-5.6.2.3.1-005	R-5.6.2.3.1-006
R-5.6.2.3.1-007	R-5.6.2.3.1-008	R-5.6.2.3.1-009			
5.6.2.3.2 MCX Service Imminent Peril Group Communications cancellation requirements					
R-5.6.2.3.2-001	R-5.6.2.3.2-002	R-5.6.2.3.2-003	R-5.6.2.3.2-004		
5.6.2.4 MCX Service Emergency Alert					
NA					
5.6.2.4.1 MCX Service Emergency Alert requirements					
R-5.6.2.4.1-001	R-5.6.2.4.1-002	R-5.6.2.4.1-003	R-5.6.2.4.1-004	R-5.6.2.4.1-004a	R-5.6.2.4.1-005
R-5.6.2.4.1-006	R-5.6.2.4.1-007	R-5.6.2.4.1-008	R-5.6.2.4.1-009	R-5.6.2.4.1-010	R-5.6.2.4.1-011
R-5.6.2.4.1-012					
5.6.2.4.2 MCX Service Emergency Alert cancellation requirements					
R-5.6.2.4.2-001	R-5.6.2.4.2-002	R-5.6.2.4.2-003			
5.7 MCX Service User ID					
R-5.7-001	R-5.7-002	R-5.7-003			
5.8 MCX UE Management					
R-5.8-001	R-5.8-002				

5.9 MCX Service User Profile					
R-5.9-001	R-5.9-002				
5.9A Functional alias					
R-5.9a-001	R-5.9a-002	R-5.9a-003	R-5.9a-004	R-5.9a-005	R-5.9a-006
R-5.9a-007	R-5.9a-008	R-5.9a-009	R-5.9a-010	R-5.9a-011	R-5.9a-012
R-5.9a-013					
5.10 Support for multiple devices					
R-5.10-001	R-5.10-002				
5.11 Location					
R-5.11-001	R-5.11-002	R-5.11-003	R-5.11-004	R-5.11-005	R-5.11-006
R-5.11-007	R-5.11-008	R-5.11-009	R-5.11-010	R-5.11-011	R-5.11-012
R-5.11-013	R-5.11-014	R-5.11-015			
5.12 Security					
R-5.12-001	R-5.12-002	R-5.12-003	R-5.12-004	R-5.12-005	R-5.12-006
R-5.12-007	R-5.12-008	R-5.12-009	R-5.12-010	R-5.12-011	R-5.12-012
R-5.12-013	R-5.12-014				
5.13 Media quality					
NA					
5.14 Relay requirements					
R-5.14-001	R-5.14-002	R-5.14-003	R-5.14-004		
5.15 Gateway requirements					
R-5.15-001					
5.16 Control and management by Mission Critical Organizations					
NA					
5.16.1 Overview					
NA					
5.16.2 General requirements					
R-5.16.2-001	R-5.16.2-002	R-5.16.2-003	R-5.16.2-004	R-5.16.2-005	
5.16.3 Operational visibility for Mission Critical Organizations					
R-5.16.3-001					
5.17 General administrative – groups and users					
R-5.17-001	R-5.17-002	R-5.17-003	R-5.17-004	R-5.17-005	R-5.17-006
R-5.17-007	R-5.17-008				
5.18 Open interfaces for MCX services					
NA					
5.18.1 Overview					
NA					
5.18.2 Requirements					
R-5.18.2-001	R-5.18.2-002	R-5.18.2-003	R-5.18.2-004		
5.19 Media forwarding					
NA					
5.19.1 Service description					
NA					
5.19.2 Requirements					
R-5.19.2-001	R-5.19.2-002	R-5.19.2-003			
5.20 Receipt notification					

NA					
5.20.1 Service description					
NA					
5.20.2 Requirements					
R-5.20.2-001					
5.21 Additional services for MCX Service communications					
NA					
5.21.1 Remotely initiated MCX Service communication					
NA					
5.21.1.1 Overview					
NA					
5.21.1.2 Requirements					
R-5.21.1.2-001	R-5.21.1.2-002	R-5.21.1.2-003	R-5.21.1.2-004		
5.21.2 Remotely terminated MCX Service communication					
NA					
5.21.2.1 Requirements					
R-5.21.2.1-001					
6 MCX Service requirements specific to on-network use					
NA					
6.1 General administrative – groups and users					
R-6.1-001	R-6.1-002	R-6.1-003	R-6.1-004	R-6.1-005	
6.2 MCX Service communications					
NA					
6.2.1 Notification and acknowledgement for MCX Service Group Communications					
R-6.2.1-001	R-6.2.1-002	R-6.2.1-003	R-6.2.1-004	R-6.2.1-005	
6.2.2 Queuing					
NA					
6.3 General requirements					
R-6.3-001	R-6.3-002	R-6.3-003	R-6.3-004		
6.4 General group communication					
NA					
6.4.1 General aspects					
R-6.4.1-001					
6.4.2 Group status/information					
R-6.4.2-005	R-6.4.2-001	R-6.4.2-002	R-6.4.2-003	R-6.4.2-004	R-6.4.2-006
R-6.4.2-007					
6.4.3 Identification					
R-6.4.3-001	R-6.4.3-002				
6.4.4 Membership/affiliation					
R-6.4.4-001	R-6.4.4-002				
6.4.5 Membership/affiliation list					
R-6.4.5-001	R-6.4.5-002	R-6.4.5-003	R-6.4.5-004	R-6.4.5-005	R-6.4.5-006
R-6.4.5-007	R-6.4.5-008				
6.4.6 Authorized user remotely changes another MCX User's affiliated and/or Selected MCX Service Group(s)					
NA					

6.4.6.1 Mandatory change					
R-6.4.6.1-001	R-6.4.6.1-002	R-6.4.6.1-003	R-6.4.6.1-004		
6.4.6.2 Negotiated change					
R-6.4.6.2-001	R-6.4.6.2-002	R-6.4.6.2-003	R-6.4.6.2-004	R-6.4.6.2-005	R-6.4.6.2-006
6.4.7 Prioritization					
R-6.4.7-001	R-6.4.7-002	R-6.4.7-003	R-6.4.7-004		
6.4.8 Relay requirements					
R-6.4.8-001					
6.4.9 Administrative					
R-6.4.9-001	R-6.4.9-004	R-6.4.9-006			
6.5 Broadcast Group					
NA					
6.5.1 General Broadcast Group Communication					
NA					
6.5.2 Group-Broadcast Group (e.g., announcement group)					
NA					
6.5.3 User-Broadcast Group (e.g., system communication)					
NA					
6.6 Dynamic group management (i.e., dynamic reporting)					
NA					
6.6.1 General dynamic regrouping					
R-6.6.1-001	R-6.6.1-002	R-6.6.1-003	R-6.6.1-004	R-6.6.1-005	R-6.6.1-006
6.6.2 Group regrouping					
NA					
6.6.2.1 Service description					
NA					
6.6.2.2 Requirements					
R-6.6.2.2-001	R-6.6.2.2-002	R-6.6.2.2-003	R-6.6.2.2-004	R-6.6.2.2-005	R-6.6.2.2-006
R-6.6.2.2-007					
6.6.3 Temporary Group-Broadcast Group					
R-6.6.3-001	R-6.6.3-002				
6.6.4 User regrouping					
NA					
6.6.4.1 Service description					
NA					
6.6.4.2 Requirements					
R-6.6.4.2-001	R-6.6.4.2-002	R-6.6.4.2-003	R-6.6.4.2-004	R-6.6.4.2-005	
6.7 Private Communication					
NA					
6.7.1 Overview					
NA					
6.7.2 General requirements					
R-6.7.2-001	R-6.7.2-002	R-6.7.2-003	R-6.7.2-004	R-6.7.2-005	
6.7.3 Administrative					
R-6.7.3-001	R-6.7.3-002	R-6.7.3-003	R-6.7.3-004	R-6.7.3-005	R-6.7.3-006
R-6.7.3-007	R-6.7.3-008				

6.7.4 Prioritization					
R-6.7.4-001	R-6.7.4-002	R-6.7.4-003	R-6.7.4-004	R-6.7.4-005	R-6.7.4-006
R-6.7.4-007					
6.7.5 Private Communication (without Floor control) commencement requirements					
R-6.7.5-001	R-6.7.5-002	R-6.7.5-003			
6.7.6 Private Communication (without Floor control) termination					
R-6.7.6-001	R-6.7.6-002				
6.8 MCX Service priority Requirements					
NA					
6.8.1 General					
R-6.8.1-001	R-6.8.1-002	R-6.8.1-003	R-6.8.1-004	R-6.8.1-005	R-6.8.1-006
R-6.8.1-007	R-6.8.1-008	R-6.8.1-009	R-6.8.1-010	R-6.8.1-011	R-6.8.1-012
R-6.8.1-013	R-6.8.1-014	R-6.8.1-015	R-6.8.1-016		
6.8.2 3GPP system access controls					
R-6.8.2-001					
6.8.3 3GPP system admission controls					
R-6.8.3-001					
6.8.4 3GPP system scheduling controls					
R-6.8.4-001					
6.8.5 UE access controls					
R-6.8.5-001					
6.8.6 Mobility and load Management					
NA					
6.8.6.1 Mission Critical mobility management according to priority					
R-6.8.6.1-001	R-6.8.6.1-002				
6.8.6.2 Load management					
R-6.8.6.2-001	R-6.8.6.2-002	R-6.8.6.2-003	R-6.8.6.2-004	R-6.8.6.2-005	
6.8.7 Application layer priorities					
NA					
6.8.7.1 Overview					
NA					
6.8.7.2 Requirements					
R-6.8.7.2-001	R-6.8.7.2-002	R-6.8.7.2-003	R-6.8.7.2-004	R-6.8.7.2-005	
6.8.8 Communication types based on priorities					
NA					
6.8.8.1 MCX Service Emergency Group Communication requirements					
R-6.8.8.1-001	R-6.8.8.1-002	R-6.8.8.1-003	R-6.8.8.1-004		
6.8.8.2 MCX Service Emergency Private Communication requirements					
R-6.8.8.2-001	R-6.8.8.2-002	R-6.8.8.2-003	R-6.8.8.2-004		
6.8.8.3 Imminent Peril Group Communication requirements					
R-6.8.8.3-001	R-6.8.8.3-002	R-6.8.8.3-003			
6.8.8.4 MCX Service Emergency Alert					
NA					
6.8.8.4.1 Requirements					
R-6.8.8.4.1-001	R-6.8.8.4.1-002	R-6.8.8.4.1-003	R-6.8.8.4.1-004	R-6.8.8.4.1-005	R-6.8.8.4.1-006
6.8.8.4.2 MCX Service Emergency Alert cancellation requirements					

R-6.8.8.4.2-001	R-6.8.8.4.2-002				
6.9 IDs and aliases					
R-6.9-001	R-6.9-002	R-6.9-003	R-6.9-004		
6.10 User Profile management					
R-6.10-001	R-6.10-002	R-6.10-003	R-6.10-004		
6.11 Support for multiple devices					
R-6.11-001	R-6.11-002	R-6.11-003			
6.12 Location					
R-6.12-001	R-6.12-002	R-6.12-003	R-6.12-004	R-6.12-005	R-6.12-006
R-6.12-007					
6.13 Security					
NA					
6.13.1 Overview					
NA					
6.13.2 Cryptographic protocols					
R-6.13.2-001	R-6.13.2-002	R-6.13.2-003			
6.13.3 Authentication					
R-6.13.3-001					
6.13.4 Access control					
R-6.13.4-001	R-6.13.4-002	R-6.13.4-003	R-6.13.4-004	R-6.13.4-005	R-6.13.4-006
R-6.13.4-007	R-6.13.4-008	R-6.13.4-009	R-6.13.4-010		
6.13.5 Regulatory issues					
R-6.13.5-001					
6.13.6 Storage control					
R-6.13.6-001					
6.14 Interactions for MCX Service Group Communications and MCX Service Private Communications					
R-6.14-001	R-6.14.002				
6.15 Additional services for MCX Service communications					
NA					
6.15.1 Discreet listening capabilities					
R-6.15.1-001					
6.15.2 Ambient listening					
NA					
6.15.2.1 Overview of ambient listening					
NA					
6.15.2.2 Ambient listening requirements					
NA					
6.15.2.2.1 General ambient listening requirements					
R-6.15.2.2.1-001	R-6.15.2.2.1-002	R-6.15.2.2.1-003			
6.15.2.2.2 Remotely initiated ambient listening requirements					
R-6.15.2.2.2-001	R-6.15.2.2.2-002				
6.15.2.2.3 Locally initiated ambient listening requirements					
R-6.15.2.2.3-001	R-6.15.2.2.3-002				
6.15.3 Remotely initiated MCX Service communication					

NA					
6.15.3.1 Overview					
NA					
6.15.3.2 Requirements					
R-6.15.3.2-002	R-6.15.3.2-001				
6.15.4 Recording and audit requirements					
R-6.15.4-001	R-6.15.4-002	R-6.15.4-003	R-6.15.4-004	R-6.15.4-005	R-6.15.4-006
R-6.15.4-007	R-6.15.4-008	R-6.15.4-009	R-6.15.4-010		
6.16 Interaction with telephony services					
R-6.16-001	R-6.16-002				
6.17 Interworking					
NA					
6.17.1 Non-3GPP access					
R-6.17.1-001					
6.17.2 Interworking between MCX Service systems					
R-6.17.2-001	R-6.17.2-002	R-6.17.2-003	R-6.17.2-004	R-6.17.2-005	R-6.17.2-006
R-6.17.2-007					
6.18 MCX Service coverage extension using ProSe UE-to-Network Relays					
R-6.18-001	R-6.18-002	R-6.18-003	R-6.18-004	R-6.18-005	R-6.18-006
6.19 Additional MCX Service requirements					
NA					
6.19.1 Communication rejection and queuing					
NA					
6.19.1.1 Requirements					
R-6.19.1.1-001	R-6.19.1.1-002	R-6.19.1.1-003	R-6.19.1.1-004	R-6.19.1.1-005	R-6.19.1.1-006
R-6.19.1.1-007					
7 MCX Service requirements specific to off-network use					
NA					
7.1 Off-network communications overview					
NA					
7.2 General off-network MCX Service requirements					
R-7.2-001	R-7.2-002	R-7.2-003	R-7.2-004	R-7.2-005	
7.3 Admission control					
NA					
7.3.1 General aspects					
R-7.3.1-001	R-7.3.1-002	R-7.3.1-003			
7.3.2 Communication initiation					
R-7.3.2-001	R-7.3.2-002	R-7.3.2-003	R-7.3.2-004	R-7.3.2-005	
7.4 Communication termination					
R-7.4-001	R-7.4-002	R-7.4-003	R-7.4-004		
7.5 Broadcast Group					
NA					
7.6 MCX Service priority requirements					
R-7.6-001	R-7.6-002	R-7.6-003	R-7.6-004	R-7.6-005	R-7.6-006
R-7.6-007	R-7.6-008	R-7.6-009			
7.7 Communication types based on priorities					

NA					
7.7.1 MCX Service Emergency Group Communication requirements					
NA					
7.7.2 MCX Service Emergency Group Communication cancellation requirements					
NA					
7.7.3 Imminent Peril Communication					
NA					
7.7.3.1 Imminent Peril Group Communication requirements					
NA					
7.7.3.2 Imminent Peril Group Communication cancellation requirements					
NA					
7.8 Location					
R-7.8-001					
7.9 Security					
R-7.9-001	R-7.9-002				
7.10 Off-network MCX Service operations					
R-7.10-001	R-7.10-002	R-7.10-003			
7.11 Off-network UE functionality					
R-7.11-001	R-7.11-002	R-7.11-003			
7.12 Streaming for ProSe UE-to-UE Relay and UE-to-Network Relay					
NA					
7.12.1 UE-to-Network Relay for all data types					
R-7.12.1-001	R-7.12.1-002	R-7.12.1-003	R-7.12.1-004		
7.12.2 UE-to-UE Relay streaming					
R-7.12.2-001	R-7.12.2-002	R-7.12.2-003			
7.12.3 Off-Network streaming					
R-7.12.3-001	R-7.12.3-002	R-7.12.3-003			
7.13 Switching to off-network MCX Service					
R-7.13-001	R-7.13-002	R-7.13-003	R-7.13-004	R-7.13-005	
7.14 Off-network recording and audit requirements					
R-7.14-001	R-7.14-002				
7.15 Off-network UE-to-UE relay					
NA					
7.15.1 Private Communications					
R-7.15.1-001	R-7.15.1-002	R-7.15.1-003			
7.15.2 Group Communications					
R-7.15.2-001	R-7.15.2-002				
8 Inter-MCX Service interworking					
NA					
8.1 Inter-MCX Service interworking overview					
NA					
8.2 Concurrent operation of different MCX Services					
NA					
8.2.1 Overview					
NA					
8.2.2 Requirements					

R-8.2.2-001	R-8.2.2-002	R-8.2.2-003	R-8.2.2-004	R-8.2.2-005	R-8.2.2-006
R-8.2.2-007					
8.3 Use of unsharable resources within a UE					
R-8.3-001	R-8.3-002	R-8.3-003	R-8.3-004	R-8.3-005	R-8.3-006
8.4 Single Group with multiple MCX Services					
NA					
8.4.1 Overview					
NA					
8.4.2 Requirements					
R-8.4.2-001	R-8.4.2-002	R-8.4.2-003	R-8.4.2-004	R-8.4.2-005	
8.4.3 Compatibility of UE					
NA					
8.4.3.1 Advertising service capabilities required					
R-8.4.3.1-001	R-8.4.3.1-002	R-8.4.3.1-003	R-8.4.3.1-004		
8.4.3.2 Conversion between capabilities					
R-8.4.3.2-001					
8.4.4 Individual permissions for service access					
R-8.4.4-001					
8.4.5 Common alias and user identities or mappable					
R-8.4.5-001					
8.4.6 Single location message					
R-8.4.6-001	R-8.4.6-002	R-8.4.6-003			
8.5 Priority between services					
NA					
8.5.1 Overview					
NA					
8.5.2 Requirements					
R-8.5.2-001	R-8.5.2-002	R-8.5.2-003	R-8.5.2-004	R-8.5.2-005	
9 Air Ground Air Communications					
NA					
9.1 Service description					
NA					
9.2 Requirements					
R-9.2-001					
10 MCX Service in IOPS mode					
R-10-001					

Annex D (informative): Characteristics and traffic assumptions for air ground air communications

The mission critical air ground air communications will be used as described below.

D.1 Environment

Helicopters are used for rescue and providing reconnaissance information to support events/incidents in rural (including mountains) environments and urban environments. Helicopters are also used for rescue and providing reconnaissance support for events/incidents in the ocean within a limited range of land or ship.

Planes are often used in rural (including forests and mountains) environment, but they can also be used in and near urban areas.

D.2 Altitudes

Helicopters have an altitude of 1.500 ft in general but in mountains it goes up to 15.000 ft.

Planes have an altitude between 2.000 ft and 15.000 ft.

The system will have to operate from 500 ft above ground level/above the sea with service continuity between ground communications and air ground air communications.

D.3 Maximum speed and mobility

Helicopters are moving at a speed of 250 km/h, planes are moving at 450 km/h. The ascent and descent speed are up to 1.000 ft per minute.

D.4 Traffic assumptions

For a region of 90.000 km2, a minimum of 18 communications per regions are supported with at least 6 simultaneous communications for helicopters and at least 6 simultaneous communications for planes.

Annex E (informative): Variables

Table E.1: List of variables

Variable	Meaning	Reference
Bc1	Number of levels of group hierarchy within an MCX Service	5.2.2
Bc2	Number of levels of user hierarchy within an MCX Service	5.2.3
Nc1	Number of receiving members present for an MCX Group.	6.4.2
Nc2	Total number of MCX Groups that an MCX User can be affiliated to simultaneously	5.1.5
Nc3	Minimum length of alphanumeric identifiers (i.e., Alias ID)	5.7, 6.4.3, 7.1, and 7.2
Nc4	Number of simultaneous MCX Group communications received by an MCX UE	5.4.2
Nc5	Number of simultaneous MCX Group communications received by a user	5.4.2
Nc6	Total number of MCX Group Members of an MCX Group	6.1

Annex F (informative): Change history

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	WI
SP-73	SP-160543	S1-162406	22.280	0001	1	Rel-14	F	Corrections to referenced sub-clauses in Annex B and Annex C	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162407	22.280	0003	1	Rel-14	D	Add an Informative Annex table in MCCoRe TS 22.280 with a List of Variables used	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162403	22.280	0004	1	Rel-14	F	Add definitions for participant and participant type to MCCoRe TS 22.280 sub-clause 3.1.	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162019	22.280	0005		Rel-14	D	Editorial changes to MCCoRe TS 22.280 Informative Annex D sub-clause D.1	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162020	22.280	0006		Rel-14	F	In MCCoRe TS 22.280 provide changes to References 1, 2, and 3 in clause 2.	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162408	22.280	0007	1	Rel-14	D	Provide editorial changes to several sub-clauses in MCCoRe TS 22.280 for consistency and to improve understanding and readability. MCC Note: 25th change (removing Annexes a, B and C) not implemented since contradicting other CRs (i.e. CR#0001r1, 0008r2, 0010r1, 0012r1 and 0021r1)	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162497	22.280	0008	2	Rel-14	C	In MCCoRe TS 22.280 provide editorial changes to the service description in sub-clause 6.19.1 Call rejection and queuing.	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162036	22.280	0009		Rel-14	B	In MCCoRe TS 22.280 Add a requirement in sub-clause 8.4.2 Requirements for a single group with multiple MCX Services.	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162266	22.280	0010	1	Rel-14	B	In MCCoRe TS 22.280 Add sub-clause 7.4 requirements to normative Annex C MCCoRe Requirements for MCData.	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162410	22.280	0012	1	Rel-14	F	Insertion of new clause 5.5.2 with requirement [R-5.1.8-002] from clause 5.1.8	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162411	22.280	0013	1	Rel-14	F	Corrections to Clause 4.2	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162124	22.280	0014		Rel-14	F	Correction of inconsistency between header 6.7 and overview text 6.7.1	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162125	22.280	0015		Rel-14	F	Correction to clause 5.1.1 requirement [R-5.1.1-005]	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162412	22.280	0016	1	Rel-14	F	Clarification of text in clause 5.4.1	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162127	22.280	0017		Rel-14	F	Clarification of text in clause 5.6.1	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162413	22.280	0018	1	Rel-14	F	Moving of informative text within requirements to NOTEs	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162414	22.280	0019	1	Rel-14	F	Correction [R-7.12.3-003]	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162415	22.280	0020	1	Rel-14	F	Correction of the entity that affiliates	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162416	22.280	0021	1	Rel-14	F	Single requirement label [R-5.6.2.4.1-004] with two requirements	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162132	22.280	0022		Rel-14	F	Corrections to definitions	14.0.0	14.1.0	MCImp-MCCoRe
SP-73	SP-160543	S1-162401	22.280	0023	1	Rel-14	F	Corrections to Group Regroup triggered by the need to support of Audio Cut-in capability	14.0.0	14.1.0	MCImp-MCCoRe

SP-74	SP-160891	S1-163008	22.280	0024		Rel-14	F	Corrections to referenced sub-clauses in Annex C	14.1.0	14.2.0	MCImp-MCCoRe
SP-74	SP-160891	S1-163009	22.280	0025		Rel-14	D	Editorial changes to 3 sub-clauses	14.1.0	14.2.0	MCImp-MCCoRe
SP-74	SP-160891	S1-163010	22.280	0026		Rel-14	D	Provide editorial changes to the service description in sub-clause 6.19.1 Communication rejection and queuing for readability.	14.1.0	14.2.0	MCImp-MCCoRe
SP-75	SP-170150	S1-170191	22.280	0027	1	Rel-14	F	Corrections to requirement references in the applicability annexes	14.2.0	14.3.0	MCImp-MCCoRe
SP-75	SP-170150	S1-171025	22.280	0030		Rel-14	F	Correct inconsistent use of the term 'one-to-many'	14.2.0	14.3.0	MCImp-MCCoRe
SP-76	SP-170445	S1-172428	22.280	0031	7	Rel-15	B	FRMCS Role management and presence	14.3.0	15.0.0	MONASTERY
SP-77	SP-170696	S1-173361	22.280	0042	1	Rel-15	F	Correction to requirement on usage of ulisted functional alias	15.0.0	15.1.0	MONASTERY
SP-77	SP-170696	S1-173362	22.280	0043	1	Rel-15	C	update requirement for functional alias	15.0.0	15.1.0	MONASTERY
SP-77	SP-170696	S1-173510	22.280	0045	2	Rel-15	C	update requirement for functional alias	15.0.0	15.1.0	MONASTERY
SP-78	SP-170985	S1-174042	22.280	0046		Rel-15	F	Updates to the wording in the specification to clarify that the requirements are applicable from LTE onwards	15.1.0	15.2.0	MCOver
SP-80	SP-180306	S1-181583	22.280	0072	2	Rel-15	F	Generalisation of EPS into 3GPP system	15.2.0	15.3.0	MCOver
SP-80	SP-180307	S1-181384	22.280	0062	1	Rel-15	F	User profile presentation priority	15.2.0	15.3.0	MCImp-MCCoRe

History

Document history		
V15.3.0	July 2018	Publication