Future Railway Mobile Communication System

Functional Interface Specification

Source	**FRMCS FIS Working Group**
Date	**13 February 2023**
Reference	**FIS-7970**
Version	**1.0.0**
Number of pages	**72**

ISBN 978-2-7461-3127-9

Document History

Version	Date	Details
0.0.1	21/07/2021	Creation of the first draft
0.0.2	30/07/2021	Adding of some draft dataflows to initiate the discussion during FIS Meeting#2
0.0.3	10/08/2021	Text and comments update based on FIS Meeting#3 discussion
0.0.4	17/12/2021	Version discussed and amended during FIS meeting #11
0.1.0	23/12/2021	Stable draft for final validation within the S2R MoU Consortium
0.1.1	18/12/2021	Text and comments update during review in FIS Meeting#12
0.2.0	21/01/2022	Stable draft for input to EECT process
0.3.0	14/04/2022	Amendments from the first round of EECT review process and from parallel FIS WG work.
0.4.0	06/05/2022	Amendments from the second round of EECT review process.
0.4.1	07/06/2022	Amendments after review within FIS Meeting #16.
0.4.2	24/06/2022	Amendments after review within FIS Meeting #17.
0.5.0	19/08/2022	Amendments based on latest outcomes from FIS WI.1 (IDs), WI.2 (REC) and WI.3 (ETCS), taking into account the latest ATWG decisions for open topics highlighted in EECT review process.
0.6.0	23/09/2022	Amendments from last EECT review round (EECT meeting on 9/09/2022)
0.7.0	10/10/2022	Amendments from last EECT review round (EECT meeting on 7/10/2022)
1.0.0	13/02/2023	Amendments related to FIS/FFFIS definitions alignment, categorisation annex and some other remarks received from EUAR on 08/02/2023

List of definitions

Agent	A person or entity that is acting or being used in the place of someone or something else.
Addressed area	Geographical area used in the addressing mechanism of a communication to determine whether a user has to be included in the communication. An addressed area could correspond to a targeted area.
Application	Provides functionality to the end user to cover a certain communication need necessary for current and future railway operations.
On-Board FRMCS (gateway)	System enabling FRMCS communication to on-board applications. The On-Board FRMCS achieves a decoupling between On-Board Application(s) and transport service. For some applications, the decoupling is also achieved for the communication service.
Trackside FRMCS (gateway)	System enabling FRMCS communication to trackside applications. The Trackside FRMCS achieves a decoupling between Trackside Application(s) and transport service. For some applications, the decoupling is also achieved for the communication service.
Home service domain	The MC user's primary security domain.
Local binding	Establishment of a mandatory secure link between an On-Board Application and the On-Board FRMCS, ensuring mutual authentication of both parties through the OB_{app} as well as the integrity and confidentiality of their information exchanges related to the OB_{app} control plane.
Location area	Geographical area used in the addressing mechanism of a communication (e.g. targeted and addressed area).
Service domain	Implementation of (parts of) the Service Stratum which belongs to and/or is operated by a unique organisation.
Service stratum	Communication Services and Complementary Services.
Session / Service session	FRMCS service session between FRMCS service clients.
Targeted area	Predefined geographical area where is located the initiator of a communication and which determines the addressing rules used for the selection of the users to be included in the communication.
User	A human user or an application making use of the FRMCS.
User Functional Alias	An MCX Functional Alias used as User Identity and possibly assigned to a user upon user login.
User authentication	The process to verify the identity of an MC user in the Identity Management Server which provides the access to MCX services.
User service authorisation	The process that validates if an MC user has the authority to use a specific MCX service.

User equipment	Combination of hardware and software required to use the FRMCS system
User identity	An identity which is available after the user is logged in to the FRMCS system via the credentials.
User registration	The union of the user authentication and the user service authorisation processes.
Visited service domain	A MCX service domain delivering services to an MC user having another service domain as primary security domain.

List of abbreviations

3GPP	3rd Generation Partnership Project
API	Application Programming Interface
ATO	Automatic Train Operation
ATO-TS	ATO Trackside entity
ATP	Automatic Train Protection
CCTV	Closed-Circuit Television
DNS	Domain Name Service
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
EUAR	European Union Agency for Railways
FFS	For Further Study
FIS	Functional Interface Specification
FRMCS	Future Railway Mobile Communication System
GNSS	Global navigation satellite system
GSM-R	Global System for Mobile communications – Railway
HSS	Home Subscriber Service
IdMS	Identity Management Server
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPcon	IP Connectivity
KMC	Key Management Centre
KMS	Key Management System
LAN	Local Area Network
LC	Loose-Coupled
MCX	Mission Critical Services (MCX stands for MCPTT or MCVIDEO or MCDATA)
MC Data	Mission Critical Data
MC ID	Mission Critical user Identity
MC PTT	Mission Critical Push-To-Talk
MC Video	Mission Critical Video
OB	On-Board
OB_{app}	On-Board Application reference point/interface
PDN	Packet Data Network
PIS	Passenger Information System
PKI	Public Key Infrastructure
RBC	Radio Block Centre

REC	Railway Emergency Communication
SIP	Session Initiation Protocol
SLC	Super Loose-Coupled
TC	Tight-Coupled
TCMS	Train Control and Management System
TR	Technical Report
TS	Technical Specification
TS_{app}	Trackside Application reference point/interface
UE	User Equipment
UIC	Union Internationale des Chemins de fer
UNISIG	Union Industry of Signaling
URI	Uniform Resource Identifier

Normative references

N1 [FRMCS FRS]	FRMCS Functional Requirements Specification FU-7120 Version 1.0.0 UIC
N2 [FRMCS SRS]	FRMCS System Requirements Specification FW-AT-7800 Version 1.0.0 UIC
N3 [FRMCS FFFIS]	FRMCS Form Fit Functional Interface Specification FW-AT-7950 Version 1.0.0 UIC
N4 [FRMCS TOBA FRS]	FRMCS Telecom On-Board System – Functional Requirements Specification TOBA-7510 Version 1.0.0 UIC
N5 [TS 22.280]	Mission Critical Services Common Requirements (MCCoRe); Stage 1 TS 22.280 3GPP
N6 [TS 23.280]	Common functional architecture to support mission critical services; Stage 2 TS 23.280 3GPP
N7 [TS 23.282]	Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2 TS 23 282 3GPP
N8 [TS 24.282]	Mission Critical Data (MCData) signalling control; Protocol specification TS 24.282 3GPP
N9 [TS 24.379]	Mission Critical Push To Talk (MCPTT) call control; Protocol specification TS 24.379 3GPP
N10 [TS 24.482]	Mission Critical Services (MCS) identity management; Protocol specification TS 24.482 3GPP
N11 [TS 24.483]	Technical Specification Group Core Network and Terminals; Mission Critical Services (MCS) Management Object (MO) TS 24.483 3GPP
N12 [TS 33.180]	Security of the Mission Critical (MC) service; TS 33.180 3GPP
N13 [ERA_ERTMS-040001]	Assignments of Values to ETCS Variables ERA_ERTMS_040001 EUAR
N14 [SUBSET-098]	RBC-RBC Safe Communication Interface Subset-098 UNISIG
N15 [SUBSET-037-1]	EuroRadio FIS - CS/PS Communication Function Module Subset-037-1 UNISIG
N16 [SUBSET-026-7]	System Requirements Specification Chapter 7 - ERTMS/ETCS language Subset-026-7 UNISIG

Notes:

- normative 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 case of contradicting or incomplete definitions and specifications within 3GPP documents, the so-called "stage 3" specifications (protocol specifications) shall take precedence over other 3GPP technical specifications.

Informative references

I1 [FU-7100]	FRMCS User Requirements Specification FU-7100 UIC
I2 [FU-7110]	FRMCS Functional Use Cases FU-7110 UIC
I3 [TR 103.459]	Future Rail Mobile Communication System (FRMCS); Study on system architecture TR 103 459 ETSI
I4 [FIS-7971]	FRMCS FRS Compliancy Statement FIS-7971 (FFS) UIC

Table of Contents

Table of figures and tables

1. Introduction

1.1. Purpose

1.1.1.1.1. This document is defining the end-to-end transactions flows required to achieve the functional requirements specified in [FRMCS FRS]. It specifies which telecommunication service primitives have to be used and how they have to be used by any client application using the services of the FRMCS system. (I)

1.1.1.1.2. This document only covers the communication applications based on the use of the 3GPP MCX services, whatever the underlying transport network consist of. The FRMCS service client defined in [TR 103.459] is consequently a 3GPP MCX client. (I)

[Editor's Note1]	*In the current version of the document, only the MCX service layer requirements are explicitly specified. The potential requirements related to the IMS/SIPCore service layer are FFS. (I)*

1.1.1.1.3. It is important to understand that this specification is completing the other FRMCS specifications ([FRMCS FRS], [FRMCS SRS], [FRMCS FFFIS] and [FRMCS TOBA FRS]) and that it can't be used separately from those ones. (I)

1.1.1.1.4. The FRMCS FIS is part of the FRMCS specifications as depicted in Figure 1. (I)

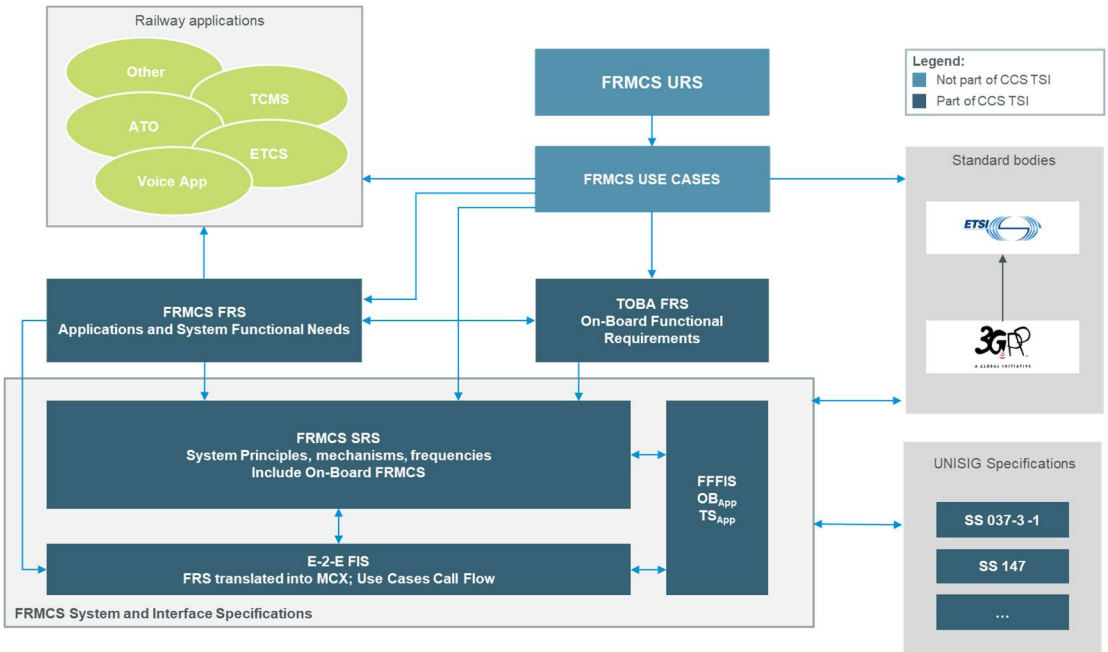

Figure 1: FRMCS specifications

1.2. Scope

1.2.1.1.1. In the figure below (Figure 2), the elements coloured in blue represent the main scope of the FRMCS functional requirements specifications (see [FRMCS FRS] and [FRMCS TOBA FRS]). (I)

1.2.1.1.2. The functional requirements of several of the applications represented in Figure 2 are partially or totally out of the FRMCS specifications scope but, at least, the way these have to request the services of the FRMCS system must be specified. (I)

1.2.1.1.3. In Figure 2, the continuous blue lines represent the scope of this FIS i.e. are representing the interfaces for which the service primitives and their corresponding parameters must be specified. (I)

1.2.1.1.4. This FIS only covers the interface requirements related to the service stratum and is valid whatever is the transport technology used to enable the telecommunication path beyond the On-Board/Trackside FRMCS. (I)

1.2.1.1.5. Figure 2 intends to cover the communication between an on-board entity and a trackside entity but also between two trackside entities or two on-board entities. (I)

1.2.1.1.6. Some of the applications represented in Figure 2 deliver a function to a human user (e.g. REC). The human user is the FRMCS user. (I)

1.2.1.1.7. Some of the applications represented in Figure 2 act as a FRMCS user (e.g. ETCS ATP). (I)

1.2.1.1.8. The term “voice apps” used in Figure 2 is mainly covering applications based on voice communication but could also cover other media used for human-to-human communication as instant messaging. Moreover, the voice communication could also be complemented with information based on video and/or data stream. (I)

1.2.1.1.9. Figure 2 is not intended to be exhaustive and is not representing all the applications in the scope of [FRMCS FRS]. (I)

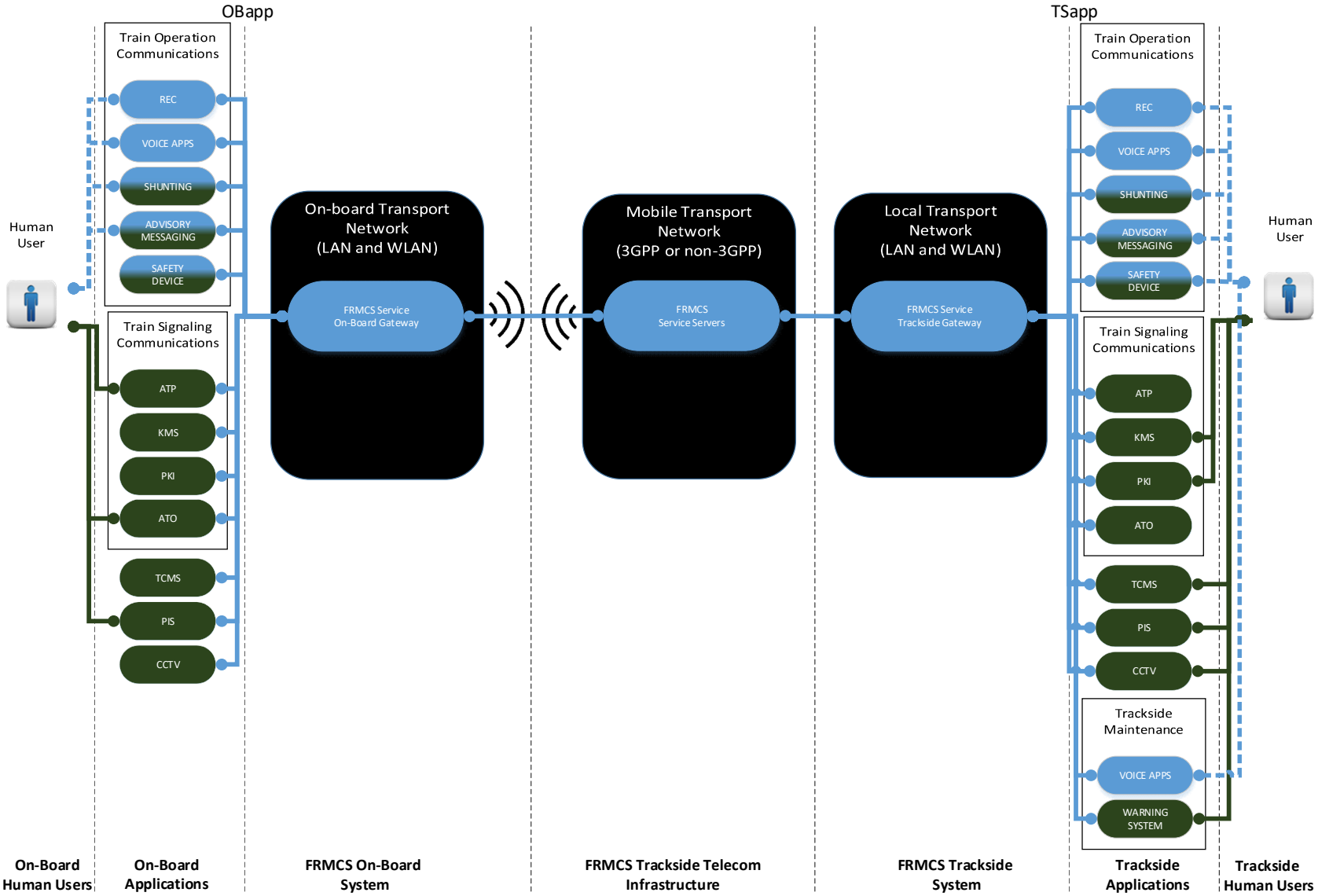

Figure 2: functional interface specification scope

1.3. Categorisation of the clauses

1.3.1.1.1. The clauses of this document are categorised as follows: (I)

- Mandatory for the System (indicated by '(M)' at the end of the clause). These requirements mean a condition set out in this specification that must be met without exception in order to deliver a system ensuring the fulfilment of essential functional and system needs, compliance to relevant standards and technical integration. The mandatory requirements are identified as sentences using the keyword "shall".
- Optional for the system (indicated by '(O)' at the end of the clause). These requirements may be used based on the implementers' choice. When an option is selected, the related requirement(s) of this specification becomes mandatory for the system. The optional requirements are identified as sentences using the keyword "should".
- Information (indicated by "(I)" at the end of the clause). These statements provide additional information to help the reader understanding a requirement.

1.3.1.1.2. Contrary to what is defined for clauses indicated with "(O)", when a section of this document is preceded with [OPTION …] and followed by [END OF OPTION], it doesn't mean that the implementer can choose the option to implement but it means that the topic is still under discussion and is waiting for a decision. The same applies for the use of options related to the REC implementation (see section 4.3). (I)

1.4. FRMCS services access modes

1.4.1. Foreword

1.4.1.1.1. There are two main ways to access to the FRMCS services: (I)

a) Direct access mode
b) Gateway access mode

1.4.1.1.2. An application using the direct access mode is an application which doesn't require the use of an On-board/Trackside FRMCS to access the FRMCS services. For example, an MCX-enabled handheld embedding the application, an MCX client, a mobile radio and the antenna is able to work in direct access mode. (I)

1.4.1.1.3. An application using the gateway access mode is an application which is accessing the FRMCS services through an On-Board/Trackside FRMCS (e.g. ETCS application). The communication between the application and the On-Board/Trackside FRMCS is performed through a local on-board/trackside transport network. The radio access is managed by the On-Board FRMCS which is responsible for supporting the communication services towards the onboard applications. (I)

1.4.1.1.4. The gateway access mode can be divided into two main categories: (I)

a) An MCX client managed by the application (e.g. on-board REC application) is used to access the FRMCS services.

b) An MCX client managed by the On-Board/Trackside FRMCS (e.g. associated with the on-board ETCS application) is used to access the FRMCS services.

1.4.1.1.5. An application from the category a) directly uses the service primitives specified by the 3GPP technical specifications related to Mission Critical Services (MCX). These service primitives are then relayed by the On-Board/Trackside FRMCS. This way to access the FRMCS services is called tight-coupled mode (TC mode). (I)

1.4.1.1.6. An application from the category b) doesn't directly use the MCX service primitives because the telecommunications technology independency is a strong requirement for this type of applications. This way to access the FRMCS services is called loose-coupled mode (LC mode). (I)

1.4.1.1.7. The specific API primitives to be used by the applications in LC mode are specified in [FRMCS FFFIS]. When required, the On-Board/Trackside FRMCS is addressing the MCX service primitives to the MCX services servers based on the API primitives received from the application. (I)

1.4.1.1.8. An implementation variant of the category b) is to use an MCX client managed by the On-Board/Trackside FRMCS but through a third-party entity (called "agent") placed between the application and the On-Board/Trackside FRMCS. However, the interface between the application and this entity is considered as out of the scope of the FRMCS specification and this variant is considered as covered by LC mode in this document. This variant of implementation is called super loose-coupled mode (SLC mode). Such an application is qualified as "not OB_{app} aware" because it is not able to use API primitives specified in [FRMCS FFFIS]. (I)

1.4.1.1.9. It is possible to use different access modes (LC or TC mode) for the end points of a given service session. (I)

1.4.1.1.10. A mode bypassing the MCX services is out of the scope of this version of the document. (I)

1.4.1.1.11. The OB_{app} and TS_{app} interfaces accommodate different protocols levels for both TC and LC modes, see [FRMCS FFFIS] for details. (I)

1.4.2. OB_{app} tight-coupled mode

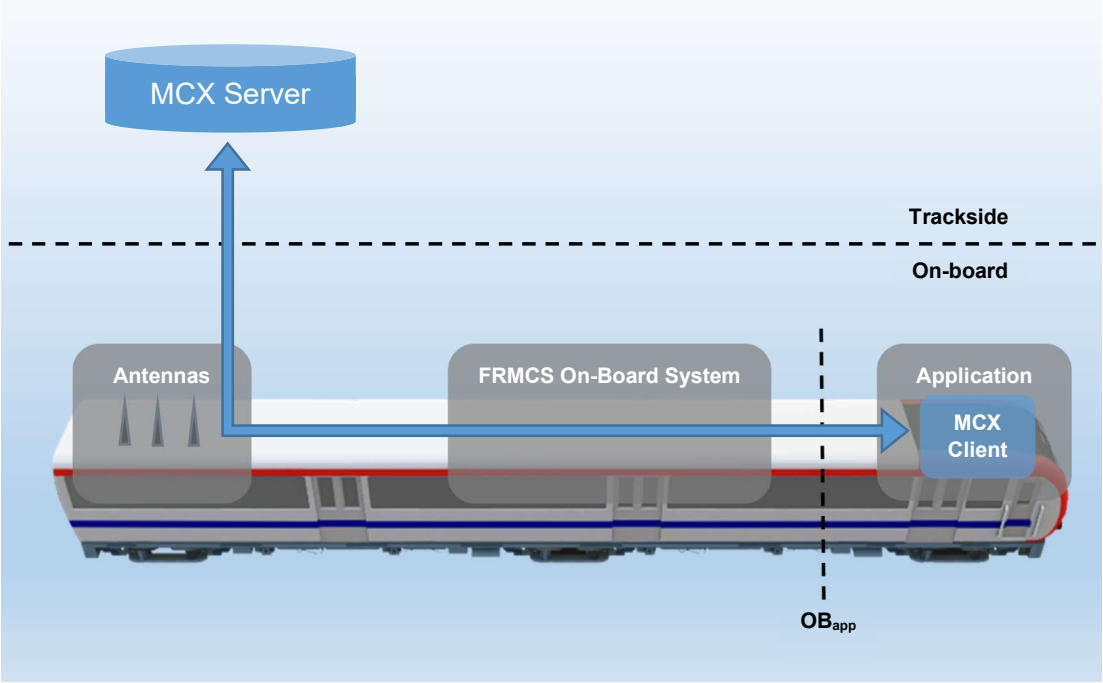

Figure 3: OB_{app} tight-coupled mode

1.4.2.1.1. With the tight-coupled mode, the MCX requests sent from the on-board application entity towards the MCX server are relayed by the On-Board FRMCS through its own mobile radio access devices (e.g. 3GPP UEs). The On-Board FRMCS is accessed by the application through a local transport network. (I)

1.4.2.1.2. In the case of an application working in the TC mode, the present FIS is (at least) defining the messages exchanged between the entities illustrated in the figure below. (I)

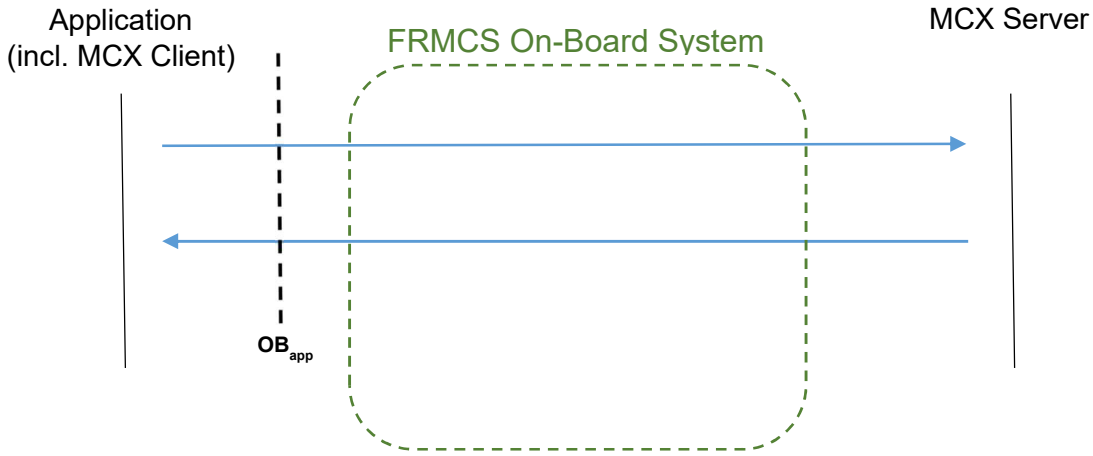

Figure 4: entities involved in OB_{app} TC mode end-to-end dialog

1.4.3. OB_{app} Loose-coupled mode

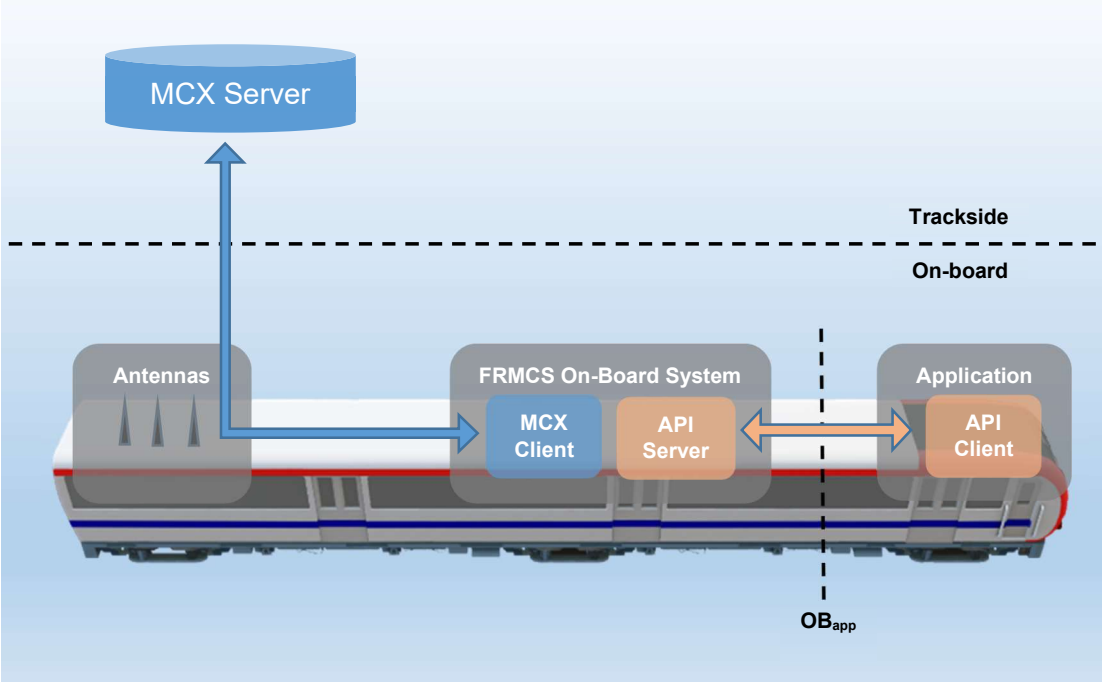

Figure 5: OB_{app} loose-coupled mode

1.4.3.1.1. With the loose-coupled mode, to enable a FRMCS communication path, the on-board application uses a dedicated API to send requests towards the On-Board FRMCS through a local transport network. Then, the On-Board FRMCS uses its own MCX clients and its own mobile radio devices (e.g. 3GPP UEs) in order to initiate the MCX primitives required to fulfil the requests of the application. (I)

1.4.3.1.2. In the case of an application working in the LC mode, the present FIS is defining the messages exchanged between the entities illustrated in the figure below while they are directly or indirectly related to an end-to-end MCX flow (I)

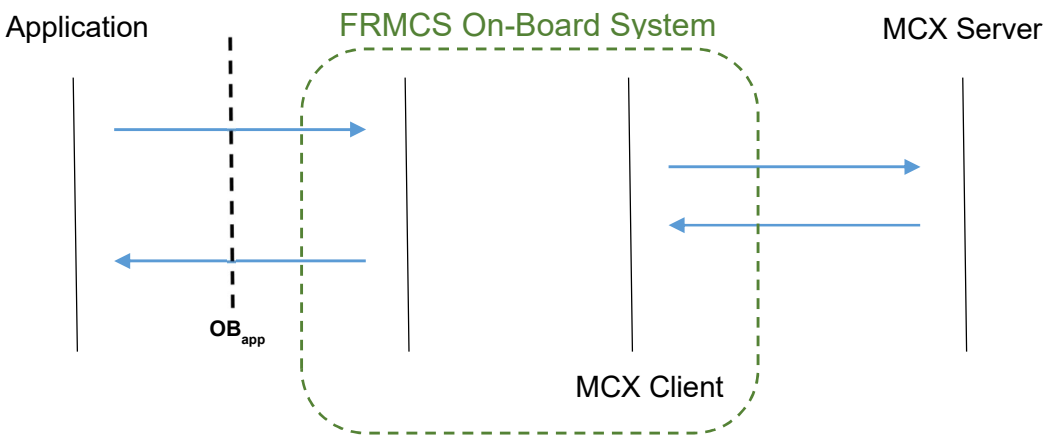

Figure 6: entities involved in OB_{app} LC mode end-to-end dialog

1.4.4. TS_{app} Tight-coupled mode

[Editor's Note2]	*It's assumed from FIS perspective that functions supported at TS_{APP} interface level will be very similar to the functions supported at OB_{APP} interface level. FFS. (I)*

1.4.5. TS_{app} Loose-coupled mode

[Editor's Note3]	*It's assumed from FIS perspective that functions supported at TS_{APP} interface level will be very similar to the functions supported at OB_{APP} interface level. FFS. (I)*

1.5. Local binding function

1.5.1.1.1. When the application is accessing the FRMCS services through an On-Board/Trackside FRMCS (in TC mode or LC mode), the local binding process is a prerequisite for the access of the application to the FRMCS services. (I)

1.5.1.1.2. For more details about the local binding process, see [FRMCS TOBA FRS] and [FRMCS FFFIS]. (I)

2. Service session in gateway access mode

2.1. Service session for LC and SLC mode

2.1.1. Introduction

2.1.1.1.1. When the application is using the MCX client embedded in an On-Board/Trackside FRMCS to access the FRMCS services (LC and SLC mode), the way to request any FRMCS service is based on [FRMCS FFFIS]. (I)

[Editor's Note4]	*Some of the figures in this chapter will be updated as soon as TS_{app} is defined in [FRMCS FFFIS]. (I)*

2.1.1.1.2. For the SLC mode, there is an additional step which is not represented in the figures of this paragraph because it is out of the scope of the present document (interface between application and agent). In that case the depicted messages are not directly sent from the application but from the agent. (I)

2.1.1.1.3. The following paragraphs provides the requirements related to the MCX service primitives and API primitives having to be used when LC/SLC mode is applicable. (I)

2.1.2. User Registration request

2.1.2.1.1. The user registration is a prerequisite for the use of the MCX services. Upon successful user registration, a user can request the initiation of a MCX communication and can be invited to participate in a MCX communication established by another user. (I)

2.1.2.1.2. The user registration request shall be initiated from the On-Board/Trackside FRMCS when considered as required by the On-Board/Trackside FRMCS. (M)

2.1.2.1.3. The user registration process includes the MCX user authentication and the MCX user service authorisation. (I)

2.1.2.1.4. The On-Board/Trackside FRMCS shall provide the user name and password required for user registration to the MCX client. (M)

2.1.2.1.5. Upon local binding (see [FRMCS FFFIS]) the application category information (e.g. etcs, ato, cabRadio) and the static identifier is provided by the application/agent to the On-Board FRMCS. (I)

2.1.2.1.6. The FRMCS system shall determine the MCX user and the corresponding MCX client associated to each application based on the static identifier (see [FRMCS FFFIS]) provided by the application/agent through the OB_{app} interface. (M)

2.1.2.1.7. The user registration could occur before or after local registration of the application, these two processes being specified as independent processes. This is left open for technical implementation. (I)

[Editor's Note5]	*The use of types of credentials other than a password is FFS. (I)*

2.1.2.1.8. During the user registration process, the MCX client of the On-Board/Trackside FRMCS shall use the user name as mission critical user identity (MC ID) and the password to perform the user authentication in accordance with [TS 33.180]. (M)

2.1.2.1.9. During the user registration process, the MCX client of the On-Board/Trackside FRMCS shall use for the authorization process the MC service user identity (MC Service ID) received upon the user authentication in accordance with [TS 33.180]. (M)

2.1.2.1.10. The MCX client shall authenticate the user to the MCX user's primary security domain. (M)

2.1.2.1.11. The user will always use the IdMS owned by its home service domain (also called primary domain within MCX specifications) for authentication but this will not imply that the home MCX service server has to be always used for session establishment. (I)

[Editor's Note6]	*It is assumed that the selection of the FRMCS service domain to use for user service authorisation is performed by the On-Board/Trackside FRMCS based on predefined rules. This is FFS. (I)*

2.1.2.1.12. The MCX client shall authenticate the user according to [TS 24.482] and to [TS 33.180] section 5.1.2. (M)

2.1.2.1.13. The user service (MCDATA) authorisation shall be performed according to [TS 33.180] section 5.1.3, where the SIP PUBLISH method according to [TS 33.180] section 5.1.3.2.3 shall be used. (M)

2.1.2.1.14. Depending on the type of application, the service authorisation could be requested towards the home service domain or could be requested towards the visited service domain (e.g. for ATP use case). (I)

2.1.3. Session Start request

2.1.3.1.1. The session start is the API primitive used to request the initiation of a MCX communication in LC mode (see [FRMCS FFFIS]). (I)

2.1.3.1.2. After a successful user registration, it shall be possible for a user to start an end-to-end service session. (M)

2.1.3.1.3. For an application in LC/SLC mode, a Session Start request shall be sent by the application/agent to request the establishment of an end-to-end service session. (M)

2.1.3.1.4. The FRMCS system shall determine the destination address in SIP URI format based on the static identifier of the recipient provided by the application/agent through the remote address parameter over the OB_{app} interface (see [FRMCS FFFIS]). (M)

[Editor's Note7]	*The mechanism used to determine the SIP URI on the basis of the static identifier is FFS.*

2.1.3.1.5. The On-Board/Trackside FRMCS shall provide the destination address in SIP URI format to the MCX client associated to the application requesting the session start. (M)

2.1.3.1.6. The destination address can represent the endpoint of the communication (Host-to-Host addressing) but can also represent a gateway entity providing access to a network (Host-to-Network addressing). (I)

2.1.3.1.7. The MCX client of the On-Board/Trackside FRMCS shall support the setup of the MCDATA session based on a destination address provided as MC Service ID. (M)

2.1.3.1.8. The MCX client of the On-Board/Trackside FRMCS should support the setup of the MCDATA session based on a destination address provided as MC Functional alias. (O)

2.1.3.1.9. The MCX client associated with the application/agent shall request the priority level based on the communication category as specified within [FRMCS SRS] and [FRMCS FFFIS]. (M)

[Editor's Note8]	*In the "host-to-network" addressing mode the QoS/Priority is assumed to be "best effort".*
[Editor's Note9]	*Still to be clarified whether the QoS level would be explicitly requested from the MCX client or autonomously applied by MCX server based on certain criteria (e.g. destination address).*

2.1.3.1.10. If the session setup is using a partner domain service, i.e. a visited service domain, an inter-domain MC user service authorization according to [TS 33.180] section 5.1.4 shall be performed. (M)

[Editor's Note10]	*It is assumed that the On-Board/Trackside FRMCS is responsible to select the FRMCS Domain (MCX service domain and transport network) from which the service must be delivered – and*

consequently on which the authorisation has to be processed – based on predefined rules and/or on predefined triggering events. (I)

2.1.3.1.11. The MCX client shall request the setup of an IP point-to-point connection using the MCDATA IP connectivity (IPcon) service as defined in [TS 23.282] section 7.14. (M)

2.1.3.1.12. An overview of the session start request flow is illustrated in following figure. (I)

[Editor's Note11] *Only the normal (successful) case is currently covered. Failure case to be defined. Current assumption is that the failure case will be handled by the application, e.g. by retrying or going into a failure mode. (I)*

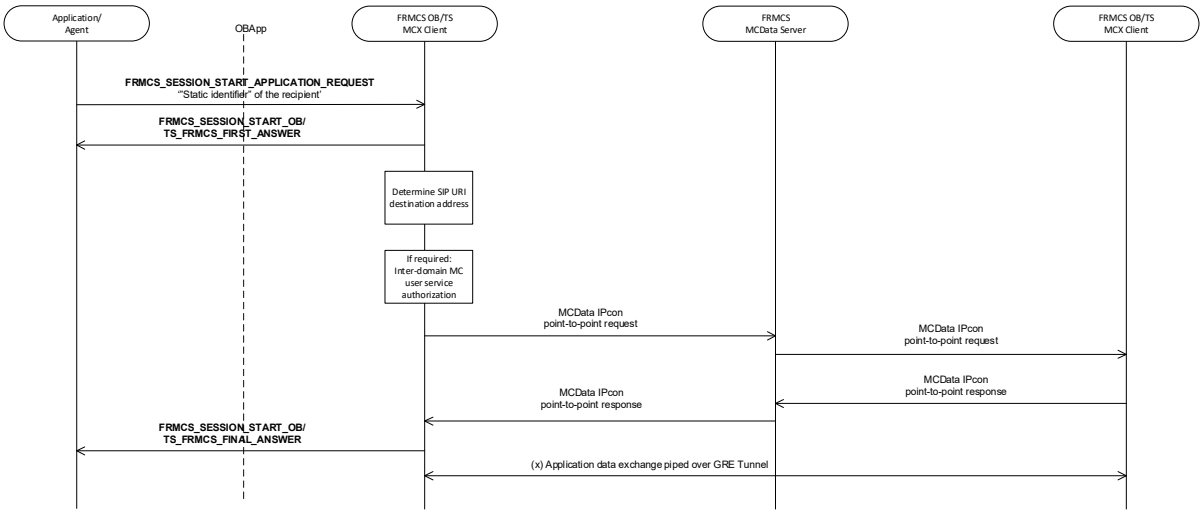

Figure 7: Session Start request for MCDATA IPcon

2.1.4. Session end request

2.1.4.1.1. The session end is the API primitive used to request the termination of a MCX communication in LC mode. (I)

2.1.4.1.2. For an application in LC/SLC mode, a Session End request shall be sent by the application/agent to request the end of the service session. (M)

2.1.4.1.3. The MCX client shall release the IP connection using the communication release procedure defined in [TS 23.282] section 7.7. (M)

[Editor's Note12]	*The session end notification specified in FFFIS still to be reflected in this document. (I)*

2.1.4.1.4. An overview of the session end request flow is illustrated in Figure 8 below. (I)

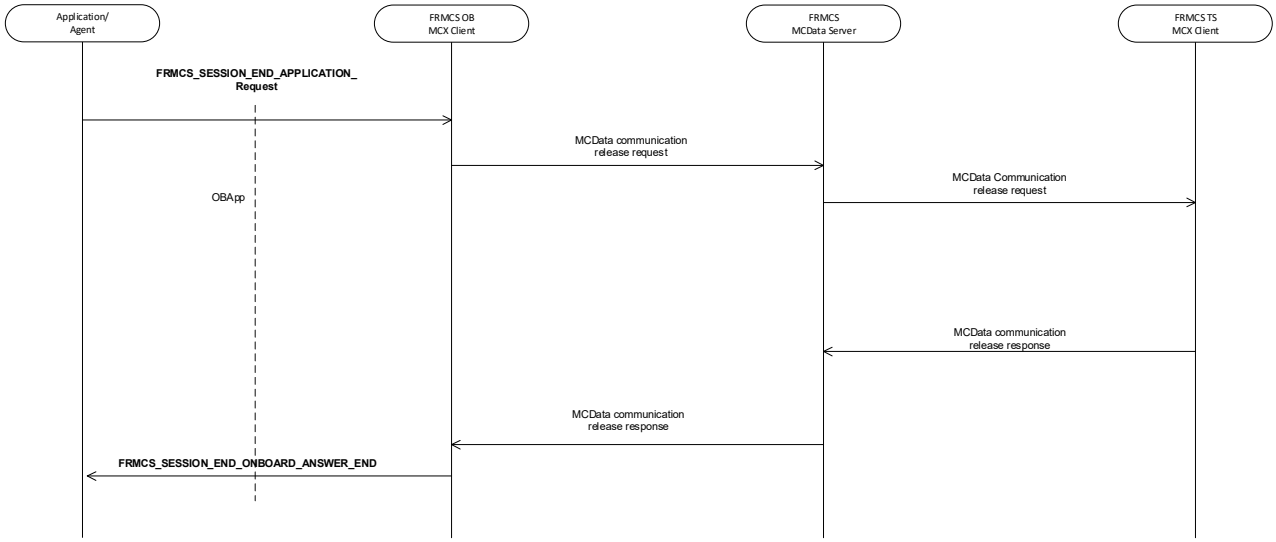

Figure 8: Session End request

2.1.5. Incoming session start notification

2.1.5.1.1. The incoming session start notification is the API primitive used to invite a user to a MCX communication in LC mode. (I)

2.1.5.1.2. After a successful user registration, it shall be possible for a user to receive an incoming session start. (M)

2.1.5.1.3. An application in LC/SLC mode, shall accept an incoming MCDATA IP connection setup using the 'incoming session start feature' specified in [FRMCS FFFIS]. (M)

2.1.5.1.4. An overview of the incoming session start notification flow is illustrated in Figure 9 below. (I)

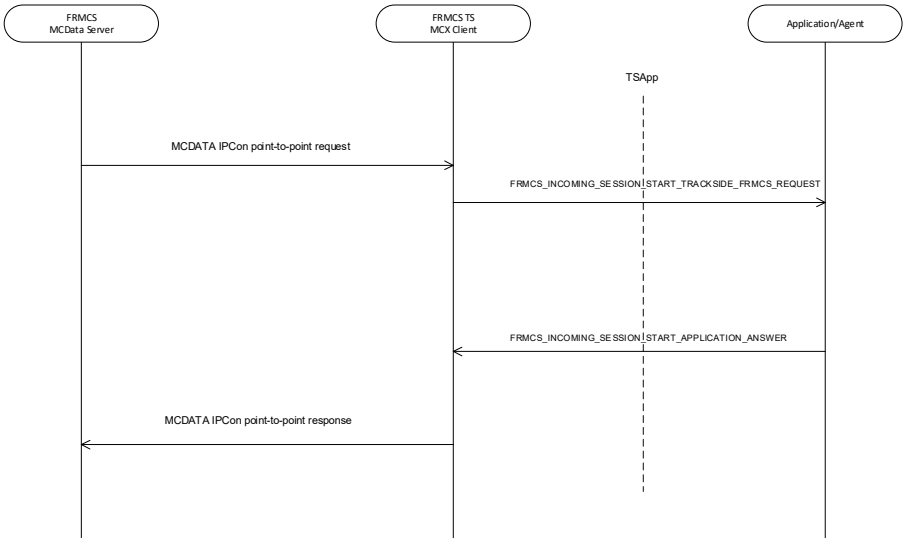

Figure 9: Incoming Session notification

2.2. Service session for TC mode

2.2.1. Introduction

2.2.1.1.1. When the application is using its own dedicated MCX client to access the FRMCS services (TC mode), the way to request any FRMCS service from that application will be solely based on 3GPP and ETSI specifications and further specified in the chapters 3 and 4. However, the local binding process is also a prerequisite for this mode and the Local Registration request procedure in accordance with [FRMCS FFFIS] is also applicable to TC mode. (I)

2.2.2. User registration request

2.2.2.1.1. The user registration request shall be initiated by the application. (M)

2.2.2.1.2. The user registration process includes the MCX user authentication and the MCX user service authorisation. (I)

2.2.2.1.3. The user name shall be provided by the application. (M)

2.2.2.1.4. The password associated with the user name shall be provided by the application. (M)

2.2.2.1.5. The use of types of credentials other than a password is FFS. (I)

2.2.2.1.6. During the user registration process, the application shall use the username as mission critical user identity (MC ID) and the password to perform the user authentication in accordance with [TS 33.180]. (M)

2.2.2.1.7. During the user registration process, the application shall use for the authorization process the MC service user identity (MC Service ID) received upon the user authentication in accordance with [TS 33.180]. (M)

2.2.2.1.8. The selection of the FRMCS service domain to use for authentication shall be performed by the application. (M)

[Editor's Note13]	*Depending on the needs of the application it could be requested to use the IdMS (for authentication) of the visited service domain or the IdMS of the home service domain. This is FFS. (I)*

2.2.2.1.9. The application shall authenticate the user according to [TS 24.482] and to [TS 33.180] section 5.1.2. (M)

2.2.2.1.10. The user service authorisation shall be performed according to [TS 33.180] section 5.1.3, where the SIP PUBLISH method according to [TS 33.180] section 5.1.3.2.3 shall be used. (M)

2.2.2.1.11. The selection of the FRMCS service domain from which the service must be delivered - and consequently on which the authorisation has to be processed – shall be performed by the application. (M)

2.2.2.1.12. The selection of the FRMCS service domain could be based on predefined rules and/or triggering events. (I)

2.2.2.1.13. A triggering event could be e.g. an input from the user or a message from a beacon reader. (I)

2.2.2.1.14. The selection of the FRMCS service domain from which the service must be delivered could imply the selection of a specific associated radio transport network by the On-Board FRMCS. E.g. it could be the case for application under control of an Infrastructure Manager. However, this is out of the scope of this document. (I)

2.2.2.1.15. An overview of the user registration flow is illustrated in Figure 10 below. (I)

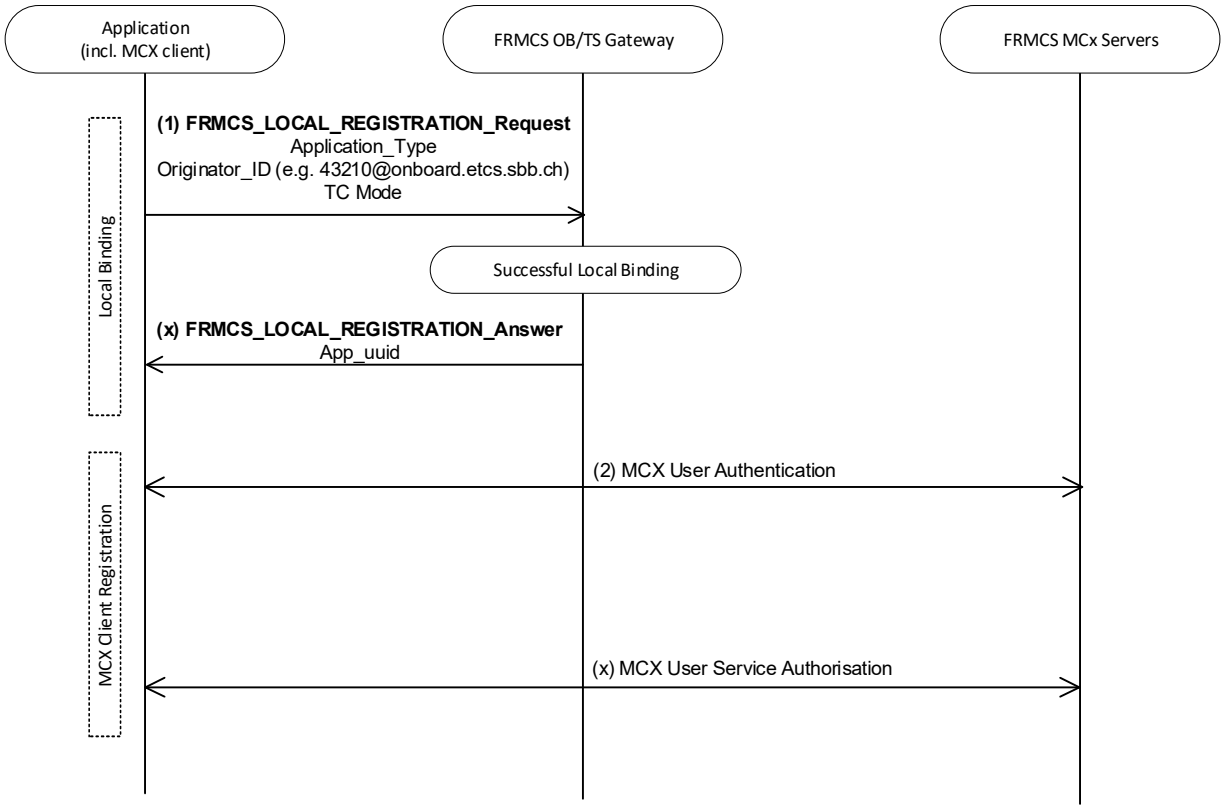

Figure 10: Local Registration request followed by MCX registration

3. Common functions requirements

3.1. Role management

3.1.1. Introduction

3.1.1.1.1. This section of the document describes how the functional requirements related to the Role Management functions (see [FRMCS FRS]) are built on the basis of the MCX services framework. (I)

3.1.1.1.2. As specified in [FRMCS FRS], the FRMCS system allows the addressing of a specific user among the users associated to a specific user's equipment. (I)

3.1.1.1.3. As specified in [FRMCS FRS], when the user is logged into multiple user's equipment, the user is addressed through each of them. (I)

3.1.1.1.4. In order to achieve these addressing capabilities, each user is assigned with one or more identities. (I)

3.1.1.1.5. To have a user identity is a prerequisite to use MC services while functional identities are optional. (I)

3.1.1.1.6. The mission critical user identity (MC ID) is used for user authentication at the Identity Management Server and must be provided by a user, an application or a client. (I)

3.1.1.1.7. The MC Service ID is configured at the Identity Management Server and is returned to the client upon user authentication. (I)

3.1.1.1.8. The MC Service ID is used for service authorization at the application server. (I)

3.1.1.1.9. One specific MC ID has up to three MC Service IDs mapped to it (one for each service), where the MC Service IDs can be identical or different from each other. (I)

3.1.1.1.10. One specific MC Service ID can activate multiple Functional Aliases, subject to user and service configuration. (I)

3.1.1.1.11. The scope of a Functional Alias is restricted to a MC service (MCPTT, MCData, or MCVideo). (I)

3.1.1.1.12. A same value can be defined for Functional Aliases of different MC services, they are handled as different Functional Aliases by the MC services even if seen as the same identity from the user perspectives. (I)

3.1.2. User identities

3.1.2.1. User login

3.1.2.1.1. In order to be able to address a communication to a user, this user needs at least to be assigned with a User Identity (see [FRMCS FRS]). (I)

3.1.2.1.2. The FRMCS system shall support the following MCX identities as User Identity in the communication addressing process: (M)

a) MC service user identity (MC Service ID)
b) MCX Functional Alias

3.1.2.1.3. The user registration as described in sections 2.1.2 and 2.2.2 is a prerequisite to get a MC Service ID. (I)

3.1.2.1.4. The user registration and the MCX Functional Alias activation as described in sections 3.1.3 are the prerequisites to get a MCX Functional Alias. (I)

3.1.2.1.5. An example format of User Identity based on a MC Service ID is sarah.connor@mcptt.mnc010.mcc262.3gppnetwork.org. See [FRMCS SRS] for further details about MC Service ID. (I)

3.1.2.1.6. A single User Identity may be identical for all MC services (i.e. MCPTT ID, MCDATA ID and MCVIDEO ID are identical) or it may be specific for the MC services (i.e. MCPTT ID, MCDATA ID and MCVIDEO ID are different). Whether a User Identity is identical or specific for MC services is FFS and will be specified in the next version of this document. (I)

3.1.2.1.7. An example format of User Identity based on a MCX Functional Alias is sarah.connor@infrabel.be or cabradio1234@infrabel.be. (I)

3.1.2.1.8. The User Identity based on an MCX Functional Alias is further called User Functional Alias. (I)

3.1.2.1.9. The User Functional Alias shall be unique for a user. (M)

3.1.2.1.10. The User Functional Alias shall include the following information elements: (M)

a) user information (e.g. sarah.connor, cabradio1234)
b) company information (company responsible for the user e.g. “infrabel”)
c) country information (country where is located the IdMS e.g. “be”)

3.1.2.1.11. A company information shall be univocally assigned to a corresponding MNC value. (M)

3.1.2.1.12. A country information shall be univocally assigned to a corresponding MCC value in accordance with [FRMCS SRS]. (M)

3.1.2.1.13. The format of the MC Service ID used to initiate a communication shall be the one specified within [FRMCS SRS]. (M)

3.1.2.1.14. The outcome of the login of a user into a FRMCS service domain is the assignment of one or more MC Service IDs with an associated user profile and optionally the assignment of one User Alias. (I)

3.1.2.1.15.

[Editor's Note14]	*Basically, the MC service IDs of a MC user and its corresponding functional aliases can be addressed only by another MC user. The possibility to address a MC user from outside the MCX framework is FFS. (I)*
[Editor's Note15]	*The identities used in the underlying transport layer as the IMS identities are of course needed for the set up the communication*

but could not directly correspond to a FRMCS user. This is out scope of this document (see [Editor's Note1] . (I)

3.1.2.2. User identities for ETCS ATP and ATO applications

3.1.2.2.1. This chapter specify how ETCS entities are identified within FRMCS system (I).

3.1.2.2.2. The addressing scheme specified in this section is applicable to ATP and ATO applications. (I)

3.1.2.2.3. In ETCS, an entity whether it is an onboard or trackside entity can be identified by its ETCS ID and ETCS ID type. See [SUBSET-026-7] and [SUBSET-037-1] for further details. (I)

3.1.2.2.4. The trackside ETCS IDs consist of two parts, one 14 bits number identifying the device within its type, and one 10 bits number (termed as NID_C) identifying the country or region where the equipment is located. (I)

3.1.2.2.5. The onboard ETCS ID consist of a 24 bits number (termed as NID_ENGINE) identifying the equipment. Currently, there is no identifier for region/country for the onboard entity. (I)

3.1.2.2.6. To make the identity unique, the ETCS ID type, consisting of an 8 bits number identifying the type of equipment (RBC, ATO-TS entity etc…), is applied. (I)

3.1.2.2.7. The URI of the trackside entity shall be derived by the FRMCS system from the static identifier of the recipient provided upon the session start request (see §2.1.3). (M)

3.1.2.3. User identities for REC and VOICE applications

3.1.2.3.1. The user login as specified within [FRMCS FRS] shall include the User Functional Alias activation. (M)

3.1.2.3.2. Whatever is the MC service used, it should be possible to address a communication to a user identity which is common to all services, particularly for applications delivering communication services to human users. (I)

3.1.3. Functional identities

3.1.3.1. General

3.1.3.1.1. Functional identities as specified in [FRMCS FRS] shall be implemented by using MCX functional aliases as defined in [TS 22.280]. (M)

3.1.3.2. Activation of functional identities

3.1.3.2.1. The procedures for activation of functional identities shall be implemented according to [TS 23.280]. (M)

3.1.3.2.2. The protocols for activation of functional identities used for voice communication shall be implemented according to [TS 24.379]. (M)

3.1.3.2.3. The protocols for activation of functional identities used for data communication shall be implemented according to [TS 24.282]. (M)

3.1.3.3. De-activation of functional identities

3.1.3.3.1. The procedures for de-activation of functional identities shall be implemented according to [TS 23.280]. (M)

3.1.3.3.2. The protocols for de-activation of functional identities used for voice communication shall be implemented according to [TS 24.379]. (M)

3.1.3.3.3. The protocols for de-activation of functional identities used for data communication shall be implemented according to [TS 24.282]. (M)

3.1.3.4. Usage of functional identities

3.1.3.4.1. The usage of functional identities to identify a calling user shall be implemented according to [TS 24.379] and [TS 24.282]. (M)

3.1.3.4.2. The usage of functional identities to address a called user shall be implemented according to [TS 24.379] and [TS 24.282]. (M)

[Editor's Note16]	*This section will be completed in the next version of this document. (I)*

3.2. Location services common function

3.2.1. Source of Location information

3.2.1.1.1. The positioning method used by the moving clients shall be implementation specific as well as the source of the location information. Possible location sources are (examples): (I)

- Location Service of 3GPP (could be GNSS based or CellID information)
- Railway specific position system
- Combination of above

[Editor's Note17]	*Current assumption is that the auxiliary function will forward 3GPP-based location information or other type of location information via OBapp to the MCX client for applications in TC mode. This is FFS. (I)*
[Editor's Note18]	*The detailed parameters and location services are application-dependent and FFS. (I)*

3.2.2. Location reporting

3.2.2.1.1. The Location information is sent via MCX Location Report messages from the clients to the MCX Server as per [TS 23.280] and therein referenced specification. (M)

[Editor's Note19]	*Additional Location Information formats (e.g. railway specific location information) are FFS. (I)*

3.2.2.1.2. The update of the location position can use specific triggers. Triggers might be different based on Infrastructure Manager needs (e.g. time base trigger, cell change, distance based, …), depending on different requirements (e.g. high-speed line, standard line, …). (I)

3.2.2.1.3. The MCX based location reporting triggering methods as specified in [TS 23.280] shall be used as report triggering methods. (M)

3.2.2.1.4. Location reporting configuration is done by location management server to the location management client as per [TS 23.280]. (I)

3.2.2.1.5. An authorized client (e.g. dispatcher) shall be able to initiate event-triggered location reporting procedure from other clients based on [TS 23.280] “Client-triggered location reporting procedure”, “Client-triggered one-time location information report” or “Client-triggered periodic location information report”. (M)

3.2.2.1.6. In case of implementation specific (MCX external) trigger method (e.g. based on On-Board FRMCS internal information, or other train based positioning methods) the following procedure shall be used: (M)

a) Location reporting configuration information shall be part of the MCX user profile or service user profile.

b) Location reporting Configuration shall be event triggered based on implementation specific (external) event triggering the MCX client to send a location report.

[Editor's Note20]	*In case of tight coupling the auxiliary function may need to deliver such status update via OB_{app} to the application/MCX client, including the reason for triggering (e.g. ECGI (cell id) so that the MCX client can act accordingly). This is FFS. (I)*
[Editor's Note21]	*The implementation specific trigger method may only apply to train-based applications/MCX clients (not applicable to handhelds). This is FFS. (I)*

3.3. Arbitration common function

[Editor's Note22]	*This section will be specified in the next version of this document. (I)*

4. Applications requirements

4.1. Automatic train protection

4.1.1. Introduction

4.1.1.1.1. The present version of the document only covers the ATP requirements related to the European Train Control System (ETCS). (I)

4.1.1.1.2. The backward compatibility with GSM-R for ETCS application is not in the scope of the FRMCS specifications. This compatibility shall be enabled by a coordinating function specified in [SUBSET-037-1]. (I)

4.1.1.1.3. There are several types of data sessions related to the ATP application, (I)

a) between on-board entity and trackside entity, enabling the automatic train protection,
b) between two trackside entities, enabling the responsibility handover mechanism required for the automatic train protection,
c) management and verification of security certificates for end-to-end communication (PKI),
d) online management of safety keys (KMS).

4.1.1.1.4. Type a) is specified below using the loose-coupled interface mode and host-to-host addressing mode. (I)

4.1.1.1.5. Type b), in the case of ETCS, is usually a permanently connected link in the fixed PDN. The communication protocol is specified in [SUBSET-098]. Type b) is FFS. (I)

4.1.1.1.6. Type c) and d) specified by section 4.1.7are using the loose-coupled interface mode in host-to-network addressing mode. (I)

4.1.2. ATP user registration

4.1.2.1.1. An ATP user (On-Board or Trackside) shall be registered to FRMCS service domain in accordance with the requirements specified by section 2.1.2 and section 3.1.2.2 of this document. (M)

4.1.3. Use of FRMCS location services

[Editor's Note23]	*The use of location services in the framework of ATP application is FFS. (I)*

4.1.4. QoS and priority

4.1.4.1.1. The ATP application is in [FRMCS FRS] categorized as CRITICAL DATA, with high priority below REC. (I)

4.1.4.1.2. The QoS and priority shall be managed according to requirements specified within section 2.1.3. (M)

4.1.5. Handling of an ATP session

4.1.5.1.1. The handling of an ATP session covers, (I)

a) Setup of an end-to-end IP communication between the onboard ETCS entity and the trackside ETCS entity via the FRMCS system.
b) Release of the communication

4.1.5.1.2. The setup and release of an end-to-end IP communication are initiated by the onboard entity. (I)

4.1.5.2. Session start

4.1.5.2.1. The On-Board ATP (ATP-OB) user shall initiate a session in accordance with the requirements specified in section 2.1.3. (M)

4.1.5.3. Session end

4.1.5.3.1. The ATP-OB user shall end a session in accordance with the requirements specified in section 2.1.4. (M)

4.1.6. Handling of ATP-TS user responsibility handover

4.1.6.1. Introduction

4.1.6.1.1. The responsibility handover from an ATP-TS to another ATP-TS relies on the session start and session end procedures described in section 4.1.5. (I)

4.1.6.1.2. The ATP-TS user responsibility handover process shall consist of the three following steps: (I)

a) Handover preparation: the ATP-OB application having an active session with the current responsible ATP-TS application (RBC) shall send a session start request to the future responsible ATP-TS.
b) Handover: the ATP-TS application reports the ATP-TS handover to ATP-OB application. The second session becomes the active one.
c) Handover closing: the ATP-OB application shall send a Session End request for the initial session.

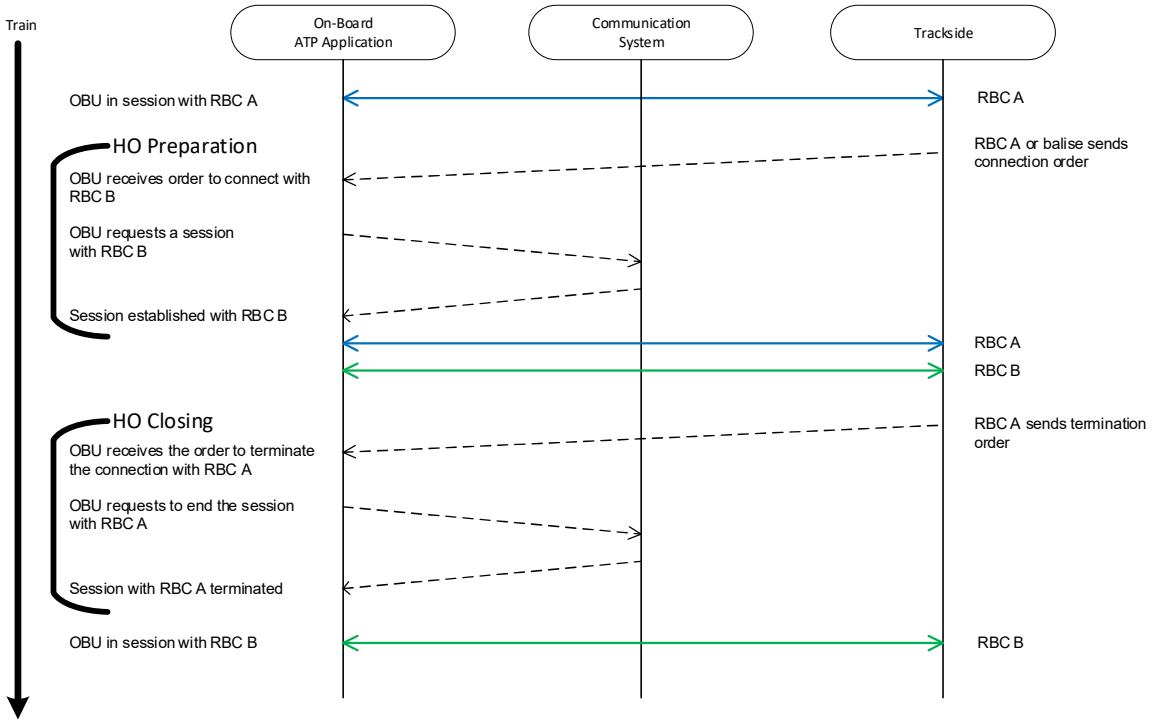

Figure 11: handling of ATP-TS user responsibility handover

4.1.6.2. Handover between ATP-TS users from a same service domain

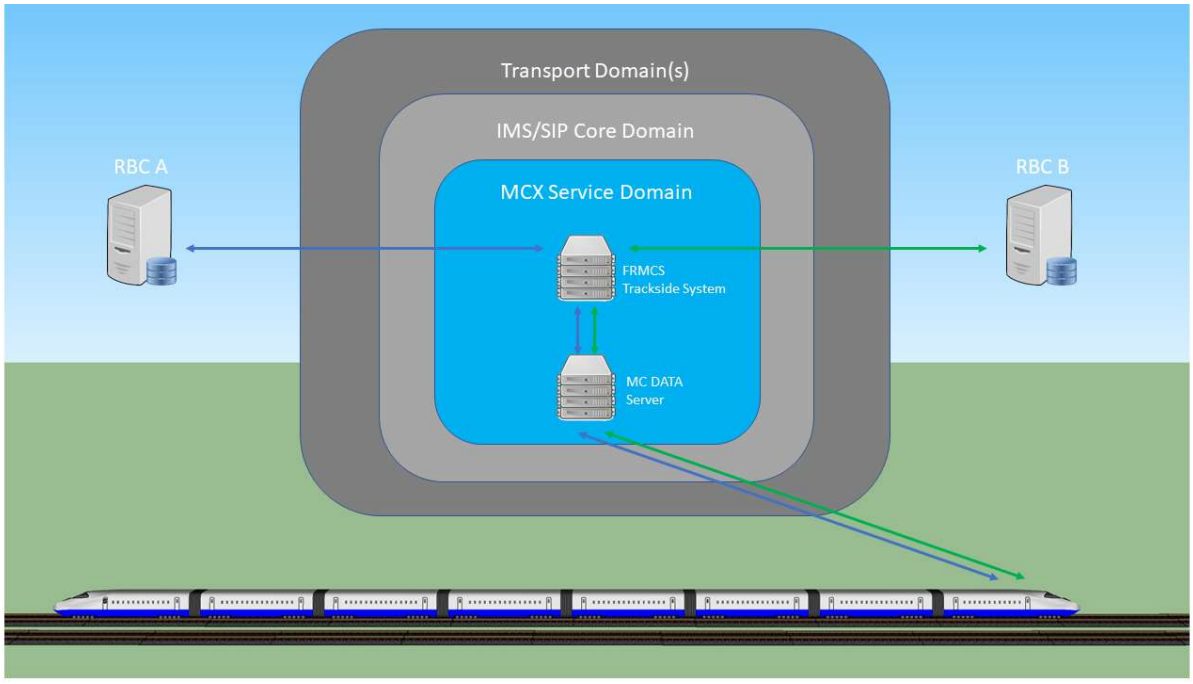

Figure 12: handover between ATP-TS users from a same service domain

4.1.6.2.1. Figure 12 is intentionally representing only the trackside infrastructure but the different transport and services layers are also applicable on-board. (I)

4.1.6.2.2. In order to perform the handover preparation, the MCX client handling the initial session shall request the setup of an MCDATA IPcon service session

as specified in section §2.1.3 by using the same serving MCX Domain as the one used for initial session. (M)

4.1.6.2.3. In order to perform the handover closing, the MCX client shall request the release of the MCDATA IPcon service session as specified in section 2.1.4. (M)

4.1.6.3. Handover between ATP-TS users from different service domains

[Editor's Note24]	*This use case is FFS.*
[Editor's Note25]	*As already noted in section 2.1.3, it is assumed that the On-Board FRMCS is responsible to select the FRMCS Domain – either the MCX Domain only or the MCX Domain and the Transport network – from which the service must be delivered – and consequently on which the authorisation has to be processed – based on predefined rules and/or on predefined triggering events. (I)*
[Editor's Note26]	*As already noted in section 2.1.2, it is assumed that the authentication is always performed on the home service domain ("home IdMS") and therefore only the service authorisation should be performed on the visited service domain. Moreover, it is assumed that it is enough to authenticate to the primary/home domain and to use services in partner domains without additional authorization. (I)*
[Editor's Note27]	*As it is assumed that the home IdMS is systematically used for user authentication, it is also assumed that a unique URI is systematically used as MC ID for user authentication. The systematic use of home IdMS create a dependency between railway companies, each user registration requiring the availability of the home infrastructure to be performed. However, this dependency could be considered of the same level as the current HLR dependency within GSM-R. A withdrawal of this dependency could probably make sense if and only if the HSS dependency is also withdrawn by systematically using a (e)SIM from the visited 5G transport network (full FRMCS independency for railway companies). (I)*
[Editor's Note28]	*It is assumed that a distinct MCX client is required to initiate the second session when a different service domain has to be used. (I)*

4.1.7. Handling of a PKI and KMS sessions

4.1.7.1. General information

4.1.7.1.1. The communications related to the PKI (Security Certificate Management) and KMS (ETCS safety key management) are not mission critical in nominal operational conditions. (I)

[Editor's Note29]	*Even if not considered as mission critical at application level, the use of MC service is foreseen for these communications.*

4.1.7.1.2. The sessions with the PKI, i.e., management of security certificates and download of needed certificate revocation lists are normally accomplished in advance to ATP (and ATO) connection setup. (I)

4.1.7.1.3. The sessions with the KMC, i.e., management of safety keys are accomplished in advance to ATP connection setup. (I)

4.1.7.1.4. The host-to-network addressing mode is used at MCX level for communications related to PKI and KMS, see [FRMCS SRS]. (I)

4.1.7.1.5. The PKI and KMS applications will use standard IP addressing over a MCDATA IPcon service session established between the On-Board MCX client and the Trackside FRMCS MCX client that will relay the data stream towards the IP network where is located the partner application entities. (M)

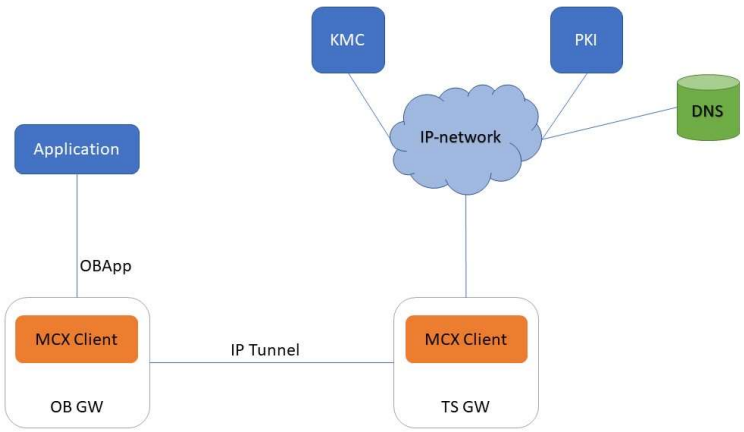

Figure 13: Addressing for PKI and KMS session

4.1.7.2. Session start

4.1.7.2.1. When required by the On-Board application, a session shall be initiated in accordance with the requirements specified in section 2.1.3. (M)

4.1.7.3. Session end

4.1.7.3.1. The session shall be ended in accordance with the requirements specified in section 2.1.4. (M)

4.2. Automatic train operation

4.2.1. Introduction

4.2.1.1.1. The present version of the document only covers the requirements for ATO based on the European Train Control System (ETCS). (I)

4.2.1.1.2. There are several types of data sessions related to the ATO application, (I)

a) between on-board entity and trackside entity, enabling the automatic train operation
b) between trackside entities, enabling connection with other ATO trackside entities, TMS etc.
c) management and verification of security certificates for end-to-end communication (PKI).

4.2.1.1.3. Type a) is specified below using the loose-coupled interface mode. (I)

4.2.1.1.4. Type b) is a permanently connected links in the fixed PDN and out of scope of this specification. (I)

4.2.1.1.5. Type c) is specified by section 4.2.5 and is using the loose-coupled interface mode in host-to-network addressing mode. (I)

4.2.2. ATO user registration

4.2.2.1.1. The ATO user (On-board or Trackside) shall be registered to FRMCS system in accordance with the requirements specified by section 2.1.2 and section 3.1.2.2 of this document. (M).

4.2.3. Use of FRMCS location services

[Editor's Note30]	*The use of location services in the framework of ATO application is FFS. (I)*

4.2.4. QoS and priority

4.2.4.1.1. The ATO application is in [FRMCS FRS] categorized as CRITICAL DATA, with priority below ATP. (I)

4.2.4.1.2. The QoS and priority shall be managed according to requirements specified within section 2.1.3. (M)

4.2.5. Handling of an ATO session

4.2.5.1.1. An ATO session shall be handled in the same way as the one specified in section 4.1.5 for an ATP session. (M)

4.2.6. Handling of ATO-TS responsibility handover

4.2.6.1.1. The responsibility handover for an ATO session shall be handled in the same way as the one specified in section 4.1.6 for an ATP session. (M)

4.2.7. Handling of a PKI (Security Certificate management) session

4.2.7.1.1. A PKI session for the ATO application shall be handled as specified in section 4.1.7 for a PKI session related to the ATP application. (M)

4.3. Railway emergency communication

4.3.1. Introduction

4.3.1.1.1. Railway Emergency communication is specified according to the requirements of the section 10.11 in [FRMCS FRS]. (M)

[Editor's Note31]	*In this FIS version, only a subset of the requirements specified in [FRMCS FRS] will be fulfilled. The level of fulfilment of the FRS Requirements will be indicated in [FIS-7971]. (I)*
[Editor's Note32]	*The level of fulfilment of the FRS Requirements will determined as soon as the REC implementation will be fully specified. This is FFS and will be covered by the next version of this document. (I)*

4.3.1.1.2. The REC application in gateway access mode shall utilize the TC mode as described in section 1.3 of this document. (M)

4.3.2. REC user registration and Role Management

4.3.2.1.1. A user shall register to FRMCS system in accordance with the requirements specified by section 3.1.2.3 of this document in order to perform REC. (M)

4.3.2.1.2. A REC user using the gateway access mode shall in addition comply to the requirements specified by section 2.2.2 of this document. (M)

[Editor's Note33]	*The current assumption is that the addressing for all RECs shall be based on the same addressing schemes as defined in section 4.4 of this document. (I)*

4.3.3. REC Types

4.3.3.1.1. In order to cover the different variants of REC specified within [FRMCS FRS], the following types of REC have to be defined in this document due to the fact they could correspond to different message flows: (I)

a) Standalone RECalert
b) Combined REC alert & REC voice: REC alert with an additional REC voice
c) Combined REC alert & REC data: REC alert with an additional REC data

[Editor's Note34]	*Combined REC alert & REC data (Type c)) is currently not specified in this version of the document and is FFS.*

[Editor's Note35]	*Handling of subsequent initiation of a REC voice or REC data after a REC alert has been initiated (i.e. after some time and not in the same procedure) is FFS.*

4.3.4. Generic REC principles

4.3.4.1.1. This section defines the generic requirements for REC which are denoted as generic REC principles. (I)

4.3.4.1.2. The REC principles specified in this section shall apply whatever is the REC Type. (M)

[Editor's Note36]	*The determination of the users to be included in a REC should preferably happen on the FRMCS Server (MCX Server) but this is FFS. For implementation option 1 (see chapter 7), the determination is client-based and that is one of the reasons why this is not the preferred option. (I)*

4.3.4.1.3. The process for determination of the REC participants shall take the following information into account: (M)

a) Current Location of mobile users
b) Current Role (Functional Alias) of users

4.3.4.1.4. The determination of the location of mobile users shall be based on the generic Location services and Location reporting described in section 3.2 . (M)

[Editor's Note37]	*The implementation option 1 doesn't require reporting of location information to FRMCS server. Nevertheless, this location reporting will anyway be required for any mobile users to achieve other requirements from [FRMCS FRS]. This is FFS. (I)*

4.3.4.1.5. In this document, the concept of "targeted area" defined in [FRMCS FRS] is completed by the concept of "addressed area" in order to achieve the technical implementation of the functional requirements as illustrated in the figure below. (I)

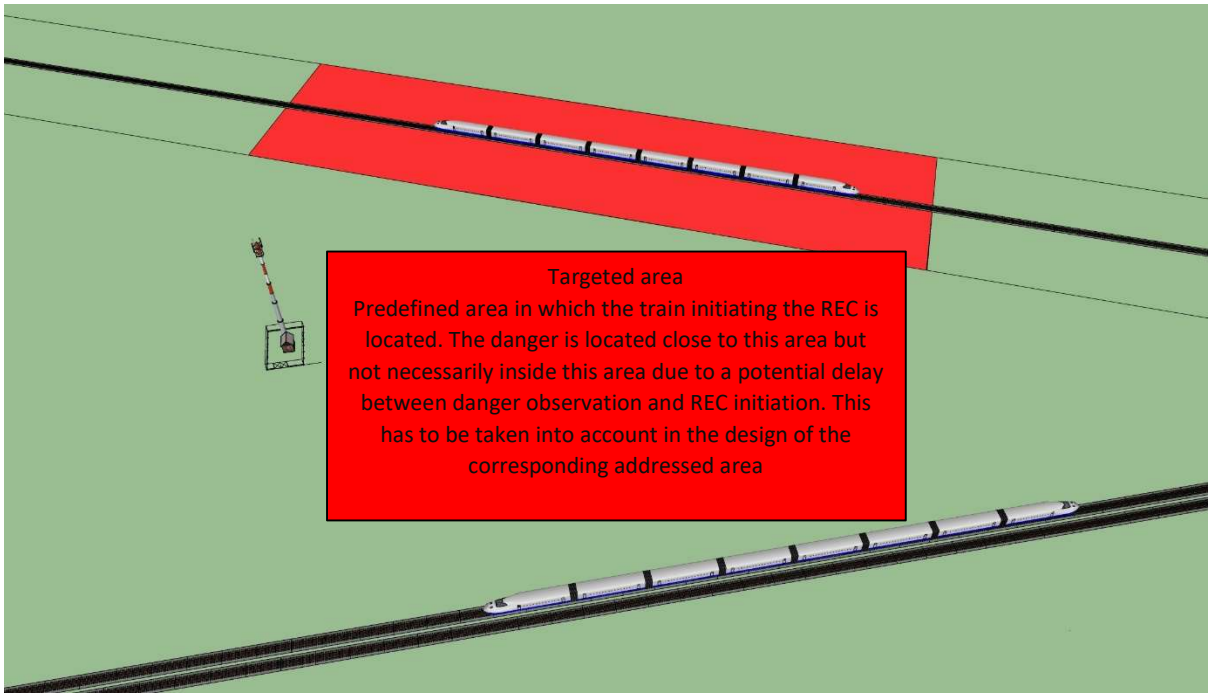

Figure 14:Selected targeted area upon REC initiation

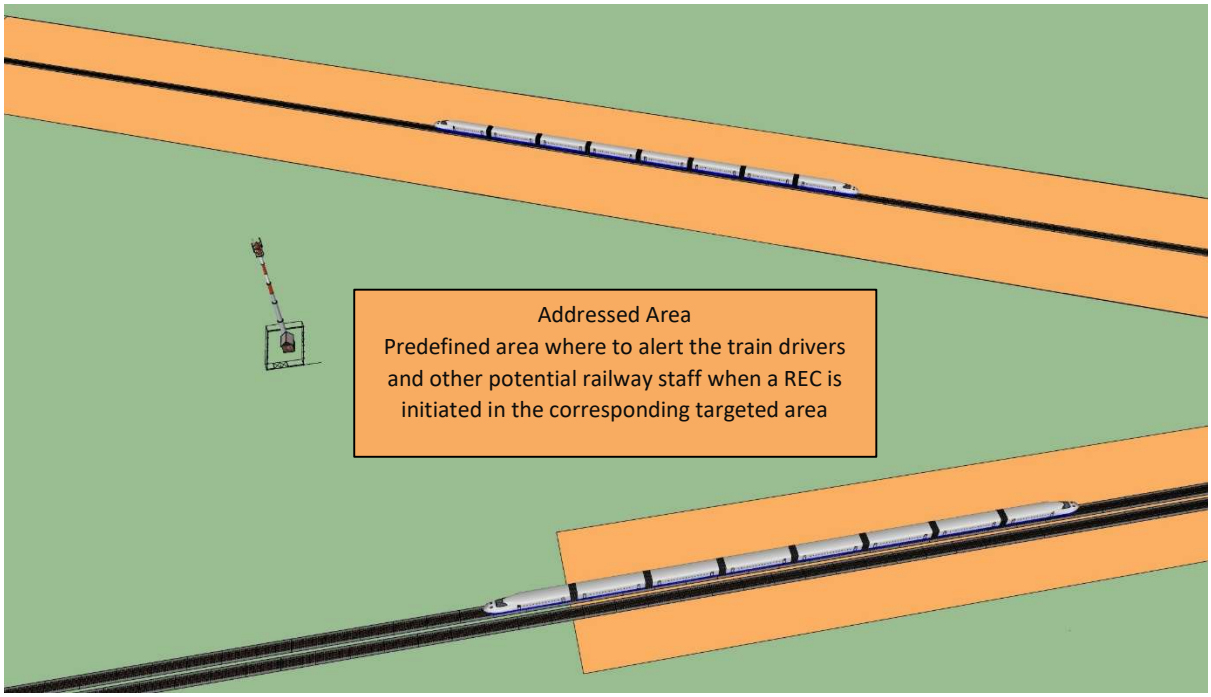

Figure 15:Addressed area corresponding to selected targeted area

4.3.4.1.6. The FRMCS system shall provide the ability to predefine the targeted and addressed area. (M)

4.3.4.1.7. The FRMCS system should provide the ability to dynamically define the targeted and addressed area based on predefined rules. (O)

[Editor's Note38]	*Implementation of the dynamic configuration of an addressed area based on predefined rules for the concerned track line(s) is FFS. (I)*

[Editor's Note39]	*Current proposed implementation is not taking into account the speed and direction in the REC participants determination process (only inclusion in a predefined area and registered role are taken into account). This is FFS. (I)*

4.3.4.1.8. The Location Area Definitions in current version of FIS shall be based on Polygon area definition as per [TS 24.483]. (M)

[Editor's Note40]	*Location Area definition based on Ellipsoid Arc maybe included in future versions of this document (FFS). (I)*
[Editor's Note41]	*Support of Railway specific Location Area definition or formats is FFS. (I)*
[Editor's Note42]	*The usage and the accuracy of location sources are FFS. (I)*

4.3.5. QoS and priority

4.3.5.1.1. The REC application is categorized as CRITICAL DATA for REC-alert and REC-data and CRITICAL VOICE for REC-voice according to [FRMCS FRS]. (I)

4.3.5.1.2. The MCX client associated with the REC application shall request the priority level based on the type of communication (emergency communication) as specified within [FRMCS SRS]. (M)

4.3.5.1.3. The MCX Server is responsible for the determination of the appropriate QoS Category and for the propagation to the transport layer based on the priority level requested from MCX client (see [FRMCS SRS] for details about QoS and priority). (I)

4.3.6. Generic REC flows

[Editor's Note43]	*This section describes generic REC flows. The detailed implementation method is currently under evaluation and will enhance and/or replace the generic REC flows in the FIS version 2.x.x. (I)*
[Editor's Note44]	*In "Annex A: REC Implementation Options" the identified implementation options for REC are described. For FIS V2.x.x a choice between the Options 2A, 2B (3GPP Release-17 based solutions) and Option 4 (3GPP Release-18 based solution) is FFS. (I)*

4.3.6.1.1. The generic REC flows as described below based on the principles defined in section 4.3.4 shall be respected. (M)

[Editor's Note45]	*The aim is to make the generic REC flows valid for all REC Types defined in section 4.3.3 of this document. However, upon final selection of the detailed REC flows in the FIS version 2.x.x, minor deviations from the generic REC flows could be required depending on the REC type used (e.g. REC alert). FFS. (I)*

4.3.6.2. Generic REC flow for setup

4.3.6.2.1. The generic REC flow for setup of a mobile user-initiated REC is shown in Figure 16. (I)

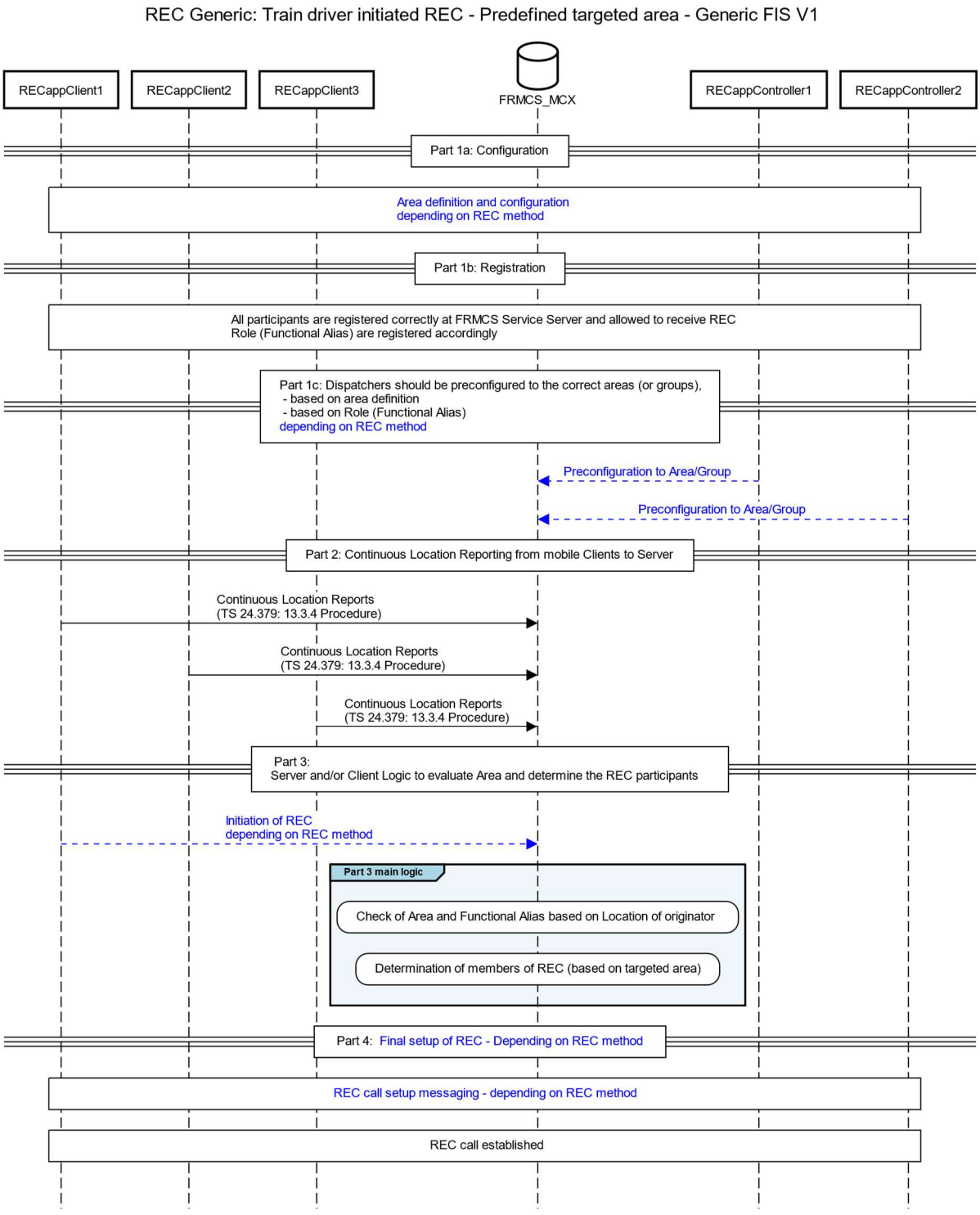

Figure 16: Generic REC flow for mobile originating REC.

Description:

Part 1a: Configuration and Prerequisites

- System is configured with Area definition
- All participants are correctly configured in the FRMCS Service Server (MCX Server)

Part 1b: Registration

- All participants are registered correctly at FRMCS Service Server and allowed to receive REC
- Controller is registered in as controller identity
- Roles (Functional Alias) have been registered accordingly by all participants

Part 1c: Dispatcher configuration

- Dispatchers should be preconfigured/registered to the correct areas (or groups),
  - based on area definition
  - based on Role (Functional Alias)
- depending on REC method

Part 2: Continuous Location Reporting from mobile Clients to Server

- All mobile clients shall continuously report their location as defined in the Section 4.3.4.
- Thus the FRMCS Service Server (MCX Server) is aware of current location of all mobile clients.

Part 3: Server and/or Client Logic to evaluate Area and determine the REC participants

- After initiation of the REC a logic shall
  - Shall check the area based on the location of the originator
  - Shall check the Functional Alias and associated permissions of the originator
  - Shall eventually determine the members of the REC (based on the above evaluations and the addressed area)

Part 4: Final setup of REC – depending on REC method

- Initiation of REC call setup signalling – depending on REC method

Finally the REC is established between all determined participants.

4.3.6.2.2. The generic REC flow for setup of a dispatcher initiated REC is depicted in Figure 17 which is identical to Figure 16 with difference that the controller is performing the initiation of REC. (I)

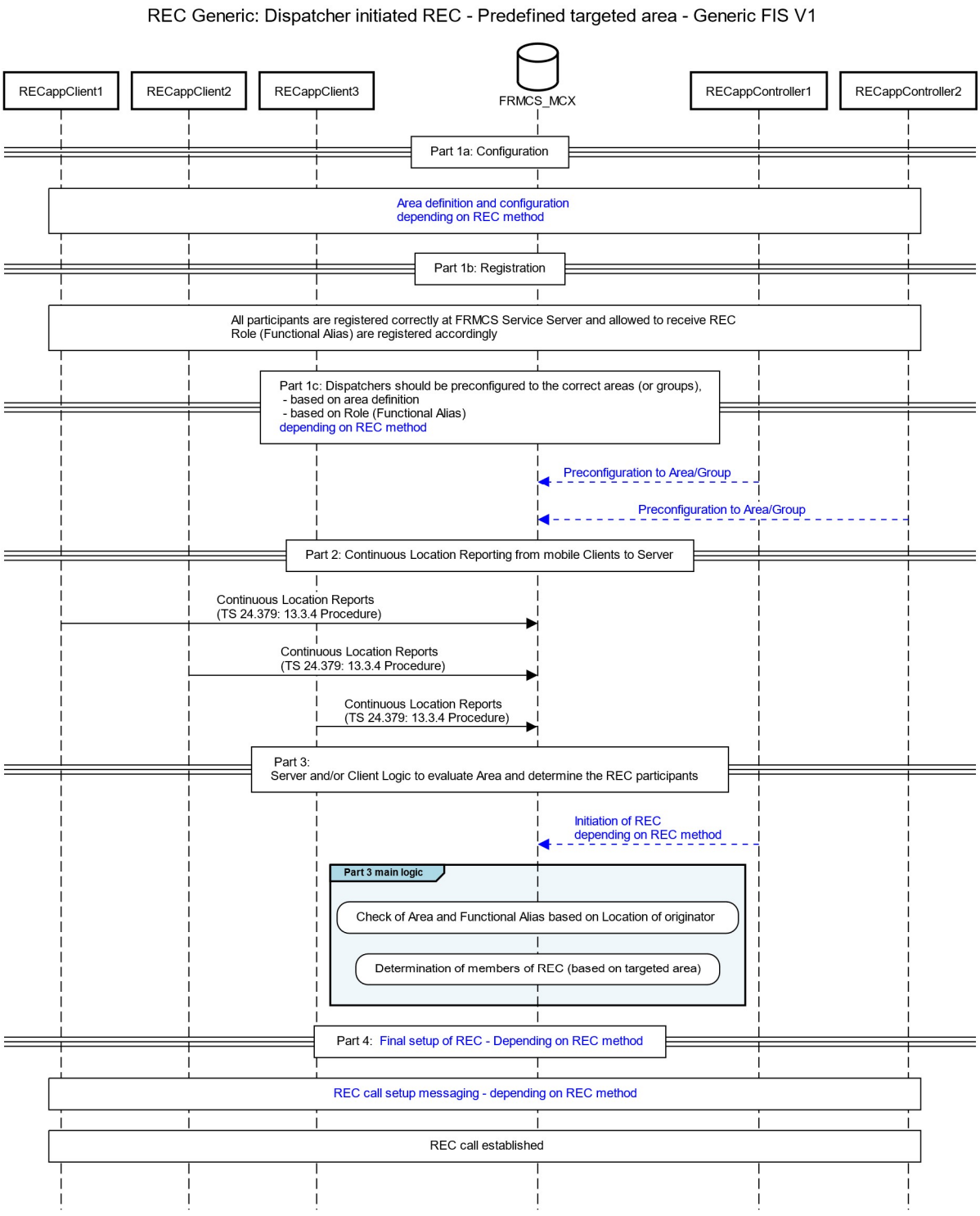

Figure 17: Generic REC flow for dispatcher originating REC.

4.3.6.3. Generic REC flow for entry or leaving addressed area

4.3.6.3.1. The generic REC flow for entry and leaving of a mobile user to an ongoing REC is shown in Figure 18. (I)

[Editor's Note46]	*This flow covers use cases for "Late Entry" in the sense of moving into the area but also when Mobiles are turned on or off inside the addressed area (tbc).*
[Editor's Note47]	*This communication flow assumes server-based evaluation method. In case of choosing a different method for FIS V2.x.x this flow might change.*

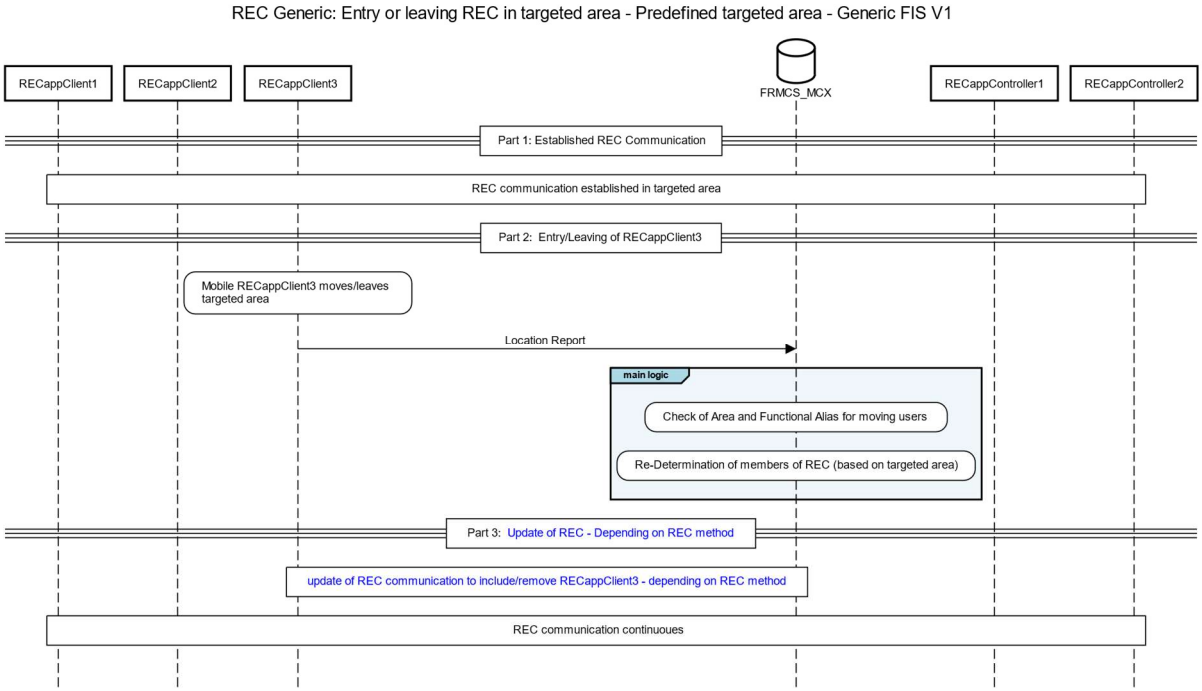

Figure 18: Generic REC flow for entering/leaving REC based on client movement.

Description:

Part 1: Established REC

- REC is established and ongoing in addressed area between participants (except ECappClient3)

Part 2: Entry/Leaving of RECappClient3

- Mobile RECappClient3 moves into/leaves addressed area
- The Mobile RECappClient3 reports the updated location to the FRMCS_MCX server
- The FRMCS_MCX Server
  - Shall check the area based on the location of the moving client
  - Shall check the Functional Alias and associated permissions of the moving client
  - Shall eventually re-determine the members of the REC (based on the above evaluations and the addressed area)

Part 3: Update of REC - Depending on REC method

- update of REC to include/release RECappClient3 – depending on REC method

Finally the REC continuous between all determined participants.

4.3.6.4. Generic REC-voice communication flow for floor request

4.3.6.4.1. The generic REC-voice communication flow for requesting floor by a specific user in an ongoing REC-voice communication is shown in Figure 19. (I)

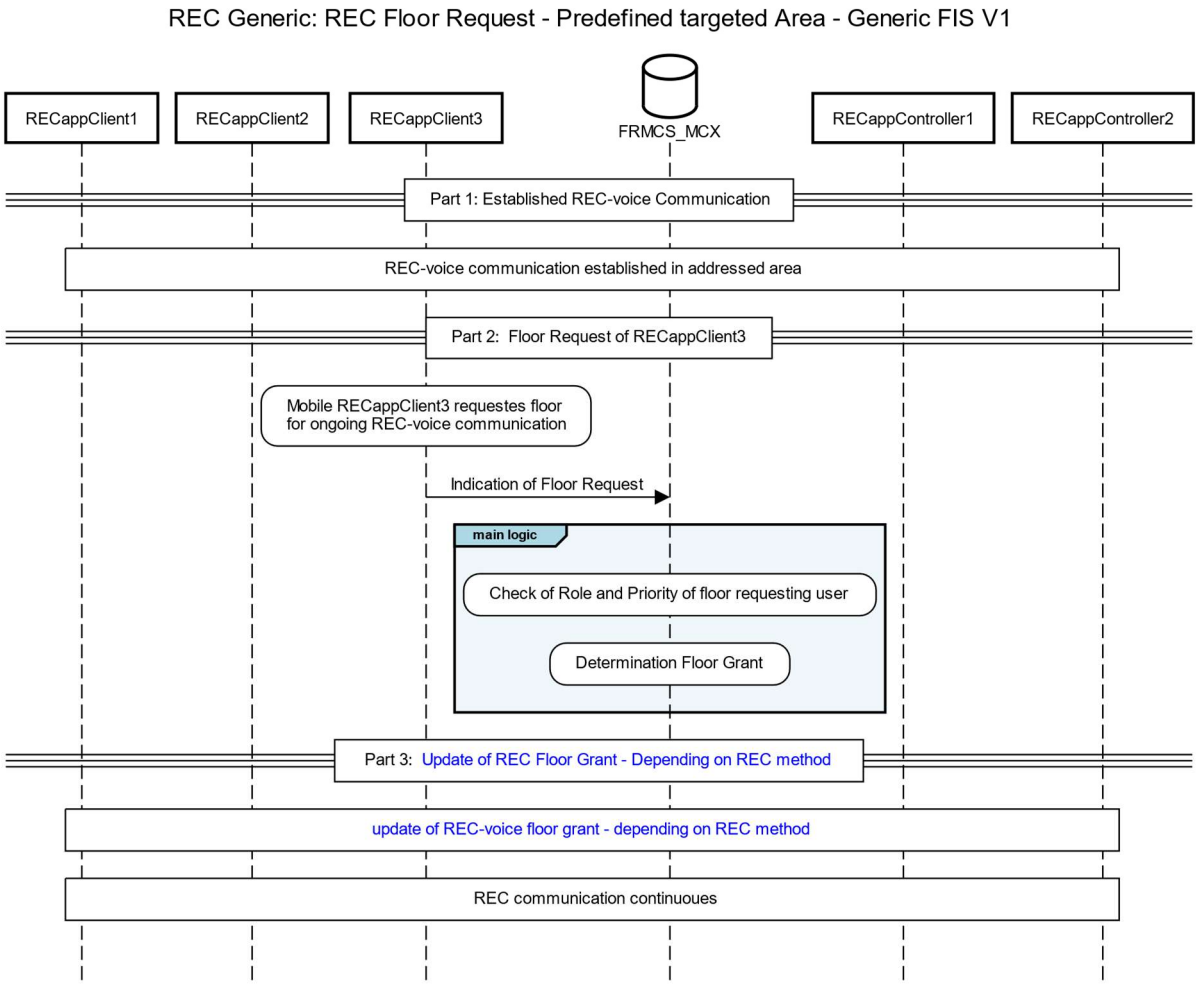

Figure 19: Generic REC-voice communication flow for floor request.

Description:

Part 1: Established REC-voice Communication

- REC is established and ongoing in addressed area between participants.

Part 2: Floor request of RECappClient3

- Mobile RECappClient3 requests floor for ongoing REC-voice communication
- The Mobile RECappClient3 reports the floor request to the FRMCS_MCX server
- The FRMCS_MCX Server
  - Shall check the Role (Functional Alias), Permission and Priority of floor requesting user
  - Shall eventually re-determine the floor granting REC (based on the above evaluations)

Part 3: Update of REC-voice floor grant - Depending on REC method

- update of REC-voice communication to change floor control – depending on REC method

Finally the REC continuous between all determined participants.

4.4. Voice communications

[Editor's Note48]	*This section will be specified in a next version of this document. It will cover the main use cases required for train operations (driver/controllers voice communications). (I)*

4.5. Train control and monitoring system

[Editor's Note49]	*The specification of the potential requirements specific to TCMS application is FFS. LC mode as defined in section 1.3 is envisaged for TCMS application. (I)*

5. Coordinating function for voice applications

[Editor's Note50]	*The specification of the potential requirements related to coordination function for VOICE applications is FFS. (I)*

6. FRMCS/GSM-R interworking

[Editor's Note51]	*The specification of the requirements related to interworking functions between FRMCS and GSM-R is FFS. (I)*

7. Annex A: REC Implementation Options

7.1. Summary and comparison of REC implementation Options

This Annex describes the current status of potential implementation options for REC with current or upcoming 3GPP MCX building blocks.

The following options have been discussed:

- Option 1: Client based approach using rule-based affiliation done by the client
- Option 2: Server based approach. Server sends message to the clients based on rules that trigger the clients to perform an affiliation to the emergency group
    - Option 2A: Client Aware solution - Originating client calls area-specific emergency group
    - Option 2B: Client Aware solution - Using emergency alert as REC trigger by originating client
- Option 3: User regroup method: Server determines based on group and area definition the clients that have to be included in the call. Then the originating client performs user regroup and initiates group call using the newly defined group. Affiliation of clients to the group is triggered by the server similarly to option 2.
- Option 4: Adhoc group method. Server based area definition and user determination (Target for 3GPP Rel-18)

The following view on the priority of the above described options shall be the base for further studies and first trial implementations:

- “Option 2A” and “Option 2B” are the current preferred solution for a 3GPP Rel17 based REC. This is considered as intermediate solution.
- “Option 4” is the subsequent preferred solution for a 3GPP Rel18 based REC.

A more detailed description of the preferred options 2A, 2B and 4 is provided in the subsequent sections.

A high level comparison is provide in the following table.

	Option 1	Option 2 Option 2A and Option 2B	Option 3	Option 4
Type	Client based approach based on rules based affiliation done by the client	Server based approach. Server sends message to the clients based on rules that trigger the clients to perform an affiliation **Option 2A:** using continuous affiliation/de-affiliation after client movements based on Areas and Roles **Option 2B:** server triggered explicit affiliation of clients based on Area and Roles subsequent to client initiating a generic emergency alert.	User regroup method: Server determines based group and area definition the clients that have to be included in the call). Then originating client performs user regroup and initiates group call using the newly defined group Client based affiliation	Adhoc group method Server based area definition and user determination
Pro	- Less load on MC server - Transparent for MC Server - Specification ready in 3GPP (including emergency alert)	- Little impact on client (functional and Less load on client): *Note: an implementation without impact on client was discarded during discussion of the options, as non-standards compliant that could cause interoperability issues.* - modification of areas (for later FIS Versions) can be done easily (as only affects MC server and can include more easily other location	- Relies on available user regroup procedure for group definition - Easy integration of external location sources on the server side. - Security aspects captured by existing procedures	- Clean definition of Targeted and addressed areas - Areas (addressed and targeted) only to be defined at server – thus also no need to define it in MCX XML structure (no MCX spec change in case of FIS changes required) - Matching current GSM-R operation mode very well (e.g. call type to all users in area)

	Option 1	Option 2 Option 2A and Option 2B	Option 3	Option 4
		sources and speed of devices.) - avoid different client implementation issues, easier recertification when server based. - More easily integration of external location sources on the server side.		- Easy integration of external location sources on the server side - A single emergency ad hoc group is called, e.g. country-wide emergency Group ID
Cons	- continuous calculation of own user and all groups on the client device – lot of data in the client - affiliation to be changed continuously (lightweight message only) - Issues with modification of areas (for later FIS Versions) - needs to be distributed for all users/profiles - Does not provide the necessary flexibility for selection of the participants in the REC call as using	- continuous calculation of all users and groups on the server, heavy calculation on continuous base on MC Server – scaling of server could be problematic – maybe easier for Variant 2B (evaluation only at REC call setup (tbc, effect on call setup time) - 2A: affiliation to be changed continuously (lightweight message only) - except Option 2B - Some additional enhancements to standard to be specified in FIS.	- complex and heavy messaging ("redefinition" of each group on location change of client required) (slowing down call setup) - Group update needs also to be distributed to the clients (slowing down call setup) - user regroup is defined for authorized user only - so client based only - potential change of standard required. - Difficult to handle late entry (Late entry to emergency group call not easily addressed)	- Release 18 only - Still do be defined Stage2/3 - Need support/acceptance from PS community in 3GPP - Server procedure needed for initiating an emergency Group call - (+ probably implicit or local affiliation performed by server) - Security aspects may need to be addressed, since the initiation of the call is not by the Client

	Option 1	Option 2 Option 2A and Option 2B	Option 3	Option 4
	configuration on client side. - Location source based on client information (what about central location source?) - Considering targeted/addressed area gets very cumbersome - Security info per area needs to be preconfigured at the client side, if security is required	*Note: No updates to Rel-17 are planned any more as release is frozen* - Option 2A: Still some client based logic on group selection for MO calls (determination of targeted/addressed area based on last affiliation) - Option 2A: - User/client is involved in deciding which group to call - Security info per area needs to be preconfigured at the client side, if security is required		
Required Standarization (3GPP and/or FIS) ***Note***: *No updates to Rel-17 are planned any more as release is frozen. Only*	- Area Definition/Configuration at server (targeted/addressed area) – maybe FIS V2 - Client logic to select correct group for origination -	- - Allow notification message (6.3.2.4.2 procedure which triggers 12.1.1.4 procedure in [TS 24.379]) also outside of emergency alert - Adding Note (or normative text) that the server may use the rules for affiliation of user	- Procedure to initiate determination of group members (Initiation at emergency setup, Server based member determination, response to authorized client) - Area Definition/Configuration at server (targeted/addressed area) (tbd if standardization is required in FIS)	- Adhoc Group call in general - Flexibility to have server based approach in Adhoc call compared to PS approach - Emergency Alert support for Adhoc groups - Area Definition/Configuration at server (targeted/addressed area)

	Option 1	Option 2 Option 2A and Option 2B	Option 3	Option 4
updates for Rel-18 based Option 4 are considered for future. Thus topics mentioned for Option 1, 2 and 3 will not be considered in standardization work anymore.		profile, or local configuration to capture the FA condition - Area Definition/Configuration at server (targeted/addressed area) - Option 2A: Client logic to select correct group for origination - Support for Generic Group ID -	-	(depending on choice), tbd in probably in FIS - Dynamic aspects (late entry, ..) to be defined - Target Release 18 -

Table 1: REC implementation options

7.2. REC Implementation Option 2A

REC Implementation Option 2A is a Server based approach. The MCX Server determines the affiliation of the clients by internal rules that trigger the clients to perform an affiliation to a specific group. **The step to affiliate the client is performed continuously as the mobiles are updating their location independent if a call setup is performed.**

The standard MCPTT emergency group call is used as base procedure.

Basic principles:

- **Operation:**
  - Clients sends continuous location reports to MC Server.
  - MC Server can determine client affiliation to Area specific group depending on the client locations
    - Client determination can use internal server rules which triggers the notification ([TS 24.379] Section 6.3.2.4.2 procedure which triggers [TS 24.379] Section 12.1.1.4 procedure) and subsequent trigger the client based affiliation procedure.
  - Upon emergency initiated by user, the client automatically selects the last known emergency group (see affiliation step 0 below) and requests a standard MCPTT emergency group call request.
- **Clients configuration**:
  - all clients initiate emergency-group calls to the currently-selected group

Basic call flow:

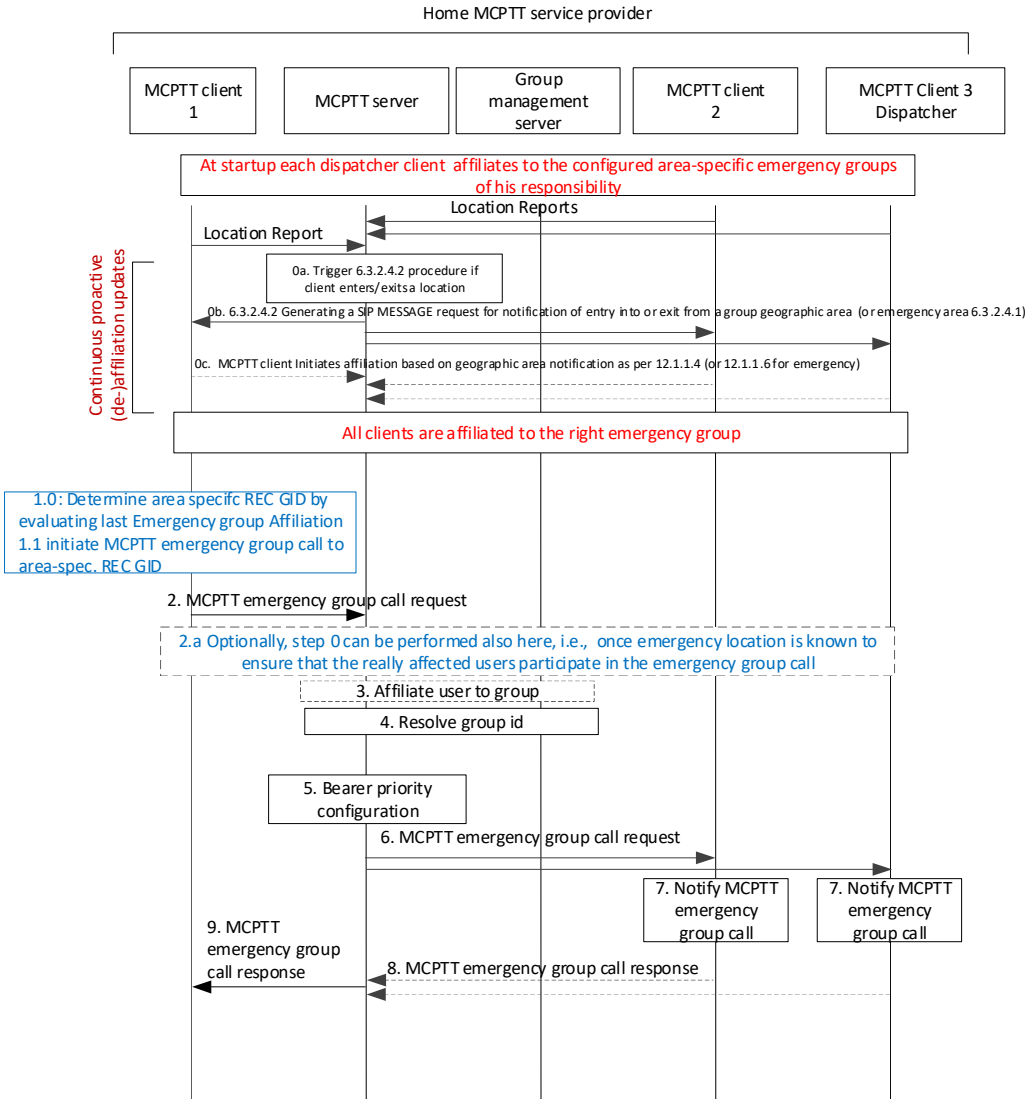

Figure 20:Basic call flow for REC option 2a

Description of the call flow:

- **Prerequisites:**
  - Area specific predefined emergency group definitions are required.
  - Dispatchers are managed with static affiliation to the configured area specific emergency groups of his responsibility

0. Continuous tracking of mobile clients based on location reporting
   Server triggers mobile clients to perform continuously group affiliation/de-affiliation based on internal criteria (FA, location etc.)
1. Upon emergency initiated by user, the client automatically selects the last known emergency group (see affiliation step 0)
2. *(as per standard procedure - no change) MCPTT emergency group call request*

2a: *Optionally Step 0 can be repeated here. Once the real emergency location is known, this step can be used to ensure that the really affected users participate in the emergency group call*
3. *(as per standard procedure - no change) – if required*
4. *(as per standard procedure - no change)*
5. *(as per standard procedure - no change)*
6. *(as per standard procedure - no change)*
7. *(as per standard procedure - no change)*
8. *(as per standard procedure - no change)*
9. *(as per standard procedure - no change)*

Implementation notes:

- Server based rules are not specified (Rel-17) (kind of “Rules based affiliation status change procedure” for the server with implicit affiliation), thus this needs to be defined separately or left implementation specific.
- Use the procedure from [TS 24.379] Section 6.3.2.4.2 also outside of emergency alert (i.e. not only is defined as per section in [TS 24.379]).
    - Extract from [TS 24.379]: : 6.3.2.4.2 Generating a SIP MESSAGE request for notification of entry into or exit from a group geographic area
        - The procedure is initiated by the participating MCPTT function when the participating MCPTT function determines that the MCPTT client has entered a pre-defined group geographic area or exited from a pre-defined group geographic area.
        - after notification the client based group affiliation is triggered
- Static Affiliation of Dispatchers are justified as we expect a dispatcher is always affiliated and no dynamic affiliation would be needed. This we can reuse client based affiliation solution which is already existing.
- Some signalling overhead especially for frequent movements/updates expected – but this is assumed to be affordable for pilot/trial implementations
- since the emergency has not happened yet at affiliation (Step0), the server cannot take into account any info related to the exact emergency, e.g. exact location of emergency or speed of train detecting the emergency. This can be enhanced by optional Step 2.a
- Step 0 constantly runs in the background for all areas
- Step 2a running for the emergency area during the call enables also Late-Entry Scenarios

7.3. REC Implementation Option 2B

REC Implementation Option 2B is a Server based approach. The MCX Server determines the affiliation of the clients by internal rules that trigger the clients to perform an affiliation to a specific group. **The step to affiliate the clients is performed just at call setup**.

The standard MCPTT emergency group call is used as base procedure.

Basic principles:

- **Operation:**
    - Clients sends continuous location reports to MC Server (tracking of clients).

- Step 1: Upon emergency initiated by user, the client generates an alert to a **generic emergency group**.
- Step 2: An emergency alert is sent which is just the trigger for server to affiliate the affected clients.
- Step 2.a: Perform step 0 for (de-)affiliation of addressed clients based on internal criteria (FA, location etc.) and emergency details
- Upon reception of the emergency alert response by originating client, the client automatically selects the area specific emergency group (as per last affiliation Step 2.a below) and requests a standard MCPTT emergency group call request.

- **Clients configuration**:
  - initiate emergency-group calls to the currently-selected group
  - triggering an emergency group communication after an emergency alert automatically (Railways solution 25 of TR 23.796)

Basic call flow:

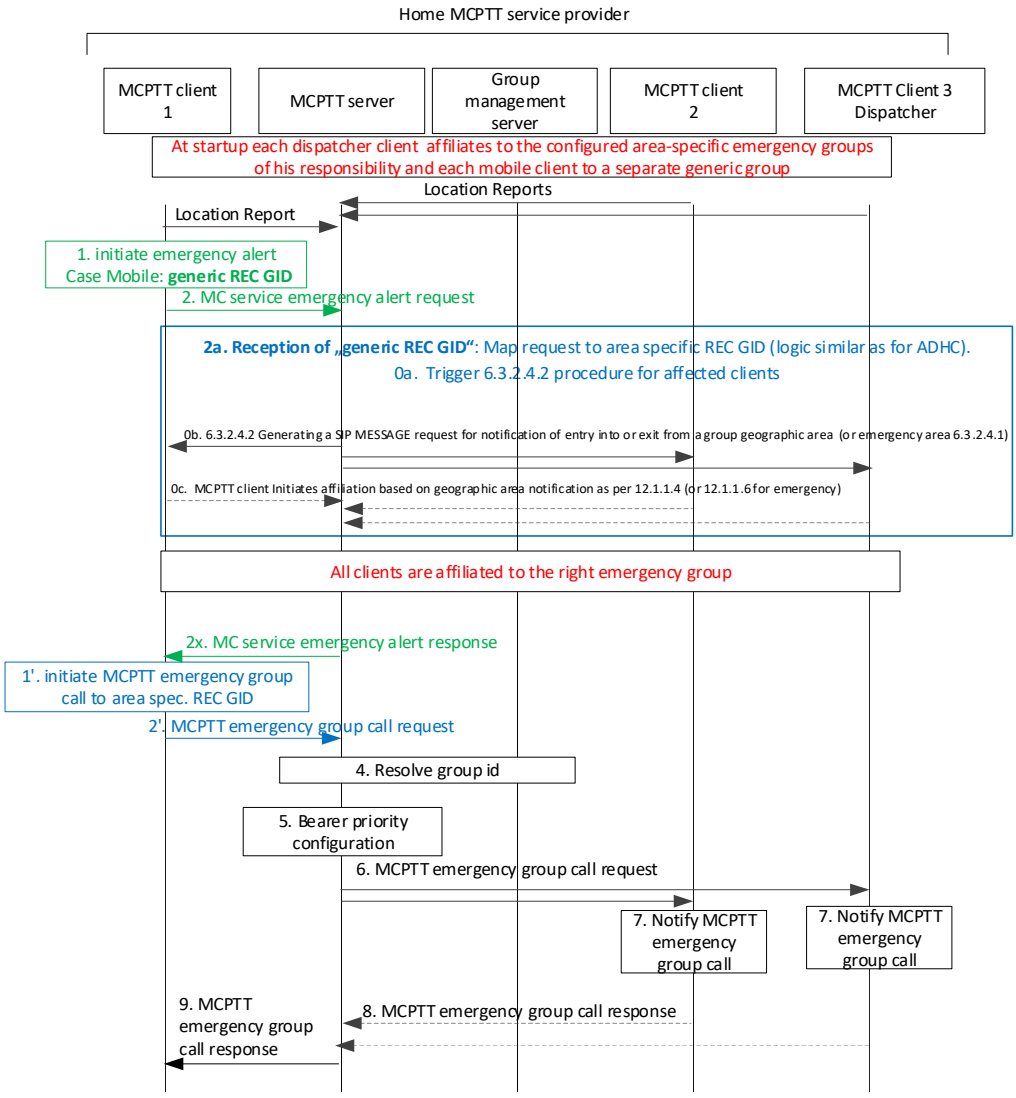

Figure 21:Basic call flow for REC option 2b

Description of the call flow:

- **Prerequisites:**
    - Area specific predefined emergency group definitions are required.
    - Dispatchers are managed with static affiliation to the configured area specific emergency groups of his responsibility

0. Continuous tracking of mobile clients based on location reporting
1. Upon emergency initiated by user, the client generates an alert to a generic emergency group
2. An emergency alert to a **generic REC GID** is sent which is just the trigger for server to affiliate the affected clients

2a. Perform step 0 for (de-)affiliation of addressed clients based on internal criteria (FA, location etc.) and emergency details.
After step 2a all clients are affiliated to the right emergency group

Note: All subsequent steps are identical to Option 2A – following standard MCPTT emergency group call

1' initiate MCTPP emergency group call to area specific REC group ID – currently selected group

2' MCPTT emergency group call request *(as per standard procedure - no change)*

4. (as per standard procedure - no change)

5. (as per standard procedure - no change)

6. (as per standard procedure - no change)

7. (as per standard procedure - no change)

8. (as per standard procedure - no change)

9. (as per standard procedure - no change)

Implementation notes:

- Server based rules are not specified (Rel-17) (kind of "Rules based affiliation status change procedure" for the server with implicit affiliation), thus this needs to be defined separately or left implementation specific.
- Use the procedure from [TS 24.379] Section 6.3.2.4.2 also upon reception of emergency alert to **generic REC GID** with specific treatment of the generic REC GID as trigger (i.e. not only is defined as per section in [TS 24.379]).
    - Extract from [TS 24.379]: : 6.3.2.4.2 Generating a SIP MESSAGE request for notification of entry into or exit from a group geographic area
        - The procedure is initiated by the participating MCPTT function when the participating MCPTT function determines that the MCPTT client has entered a pre-defined group geographic area or exited from a pre-defined group geographic area.
        - after notification the client based group affiliation is triggered
- Static Affiliation of Dispatchers are justified as we expect a dispatcher is always affiliated and no dynamic affiliation would be needed. This we can reuse client based affiliation solution which is already existing.
- Delay until group is established due to the extra step 2, this affects call setup time.
- Alert is always initiated to a generic group different from emergency group call
- Step 0 continues to run in the background but only for the emergency area and only during the call (enables Late Entry scenario)

7.3.1. REC Implementation Option 2B-Variation « Dispatcher centric»

A specific variation to Option 2B can be used to minimize the necessary client updates only to Dispatcher clients – and not on all clients.

The difference to Option 2B is that the Step 1' and Step 2' are performed only and always by the corresponding Dispatcher client for the currently addressed emergency area and not by the mobile originator of the emergency alert.

Basic call flow:

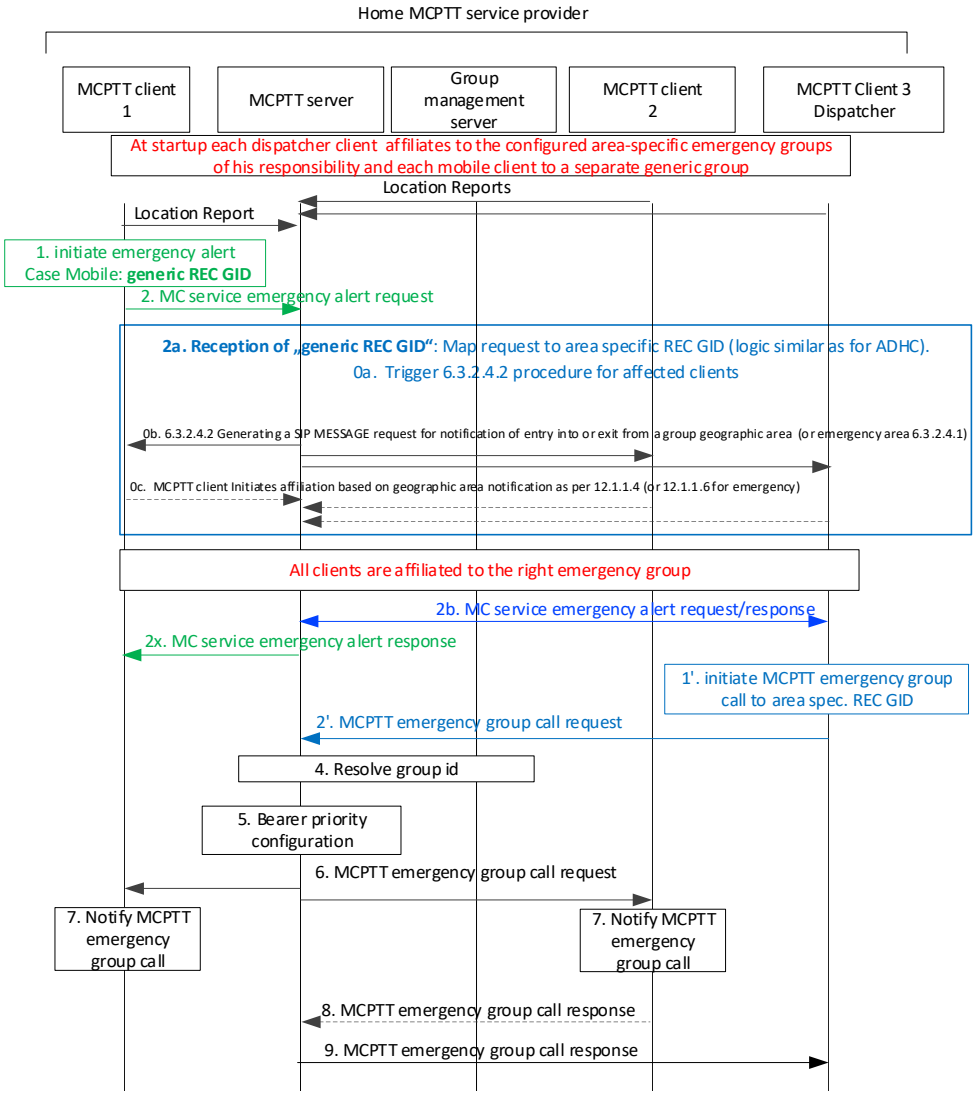

Figure 22:Basic call flow for REC option 2b-Variation "dispatcher centric"

It can be seen that Step 1' and Step 2' are initiated by "MCPTT Client 3 Dispatcher" although the mobile originator of the emergency alert was "MCPTT client 1".

Remarks:

- In Option 2B-Variation the Dispatcher needs to be configured to initiate the emergency group call. In this case, affiliation of the dispatcher also to the generic emergency group and Step 2b are needed
- Pro:
    - Not all clients need to be configured and updated so that they are able to perform Step 1' on the correct area specific emergency REC GID – only the Dispatcher clients need to have this capabilities
- Con:
    - The User perception of the originating client of the emergency alert is affected: Although the user initiates the emergency alert, the subsequent emergency group call will be always initiated by the corresponding dispatcher and the originator will perceive it as an incoming emergency call (Note: this can be potentially hidden to the user by client implementation).
    - There is a risk to rely on another MC client that the originator to achieve the setup of a REC. Even in the case where no dispatcher is available, the REC should be set up.

7.4. REC Implementation Option 4

The REC implementation Option 4 is based on MCX Adhoc group method: Server based area definition and user determination.

It is based on the Requirements for a Study Item for AdHoc Groups in MCX Specification for Release 18 (Ad hoc Group Communication support in Mission Critical Services, AHGC, WID SP-211058).

Excerpt of the Requirements [TS 22.280]:

- [R-6.15.5.2-001] The MCX Service shall provide a mechanism for an authorized MCX User to combine an ad hoc multiplicity of MCX Users into a MCX Service Ad hoc Group Communication. NOTE: Selection of the list of MCX Users can be manual, or automatic based on certain criteria. This is left for implementation.
- [R-6.15.5.2-012] The MCX Service shall provide a mechanism for the initiator to add or remove participants during an in progress MCX Service Ad hoc Group communication.

Basic principle:

- Define targeted areas and corresponding addressed areas on the controlling server.

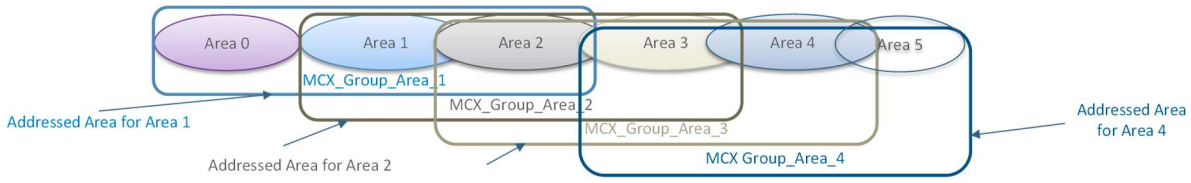

Figure 23: Assignment of MCX Group to REC addressed areas

- At REC origination:
    - The client sends a request to the MCPTT server to create an adhoc group communication
    - The Server determines all users in the addressed area based on the location of the originating user which determines the targeted area.
    - The MCPTT server invites all addressed users (thus completing the adhoc group communication)

Pro's (to be elaborated more in detail):

- Areas (addressed and targeted) only to be defined at server
- Straight forward call flow

Con's (to be elaborated more in detail):

- …

The next figure shows a simplified call flow

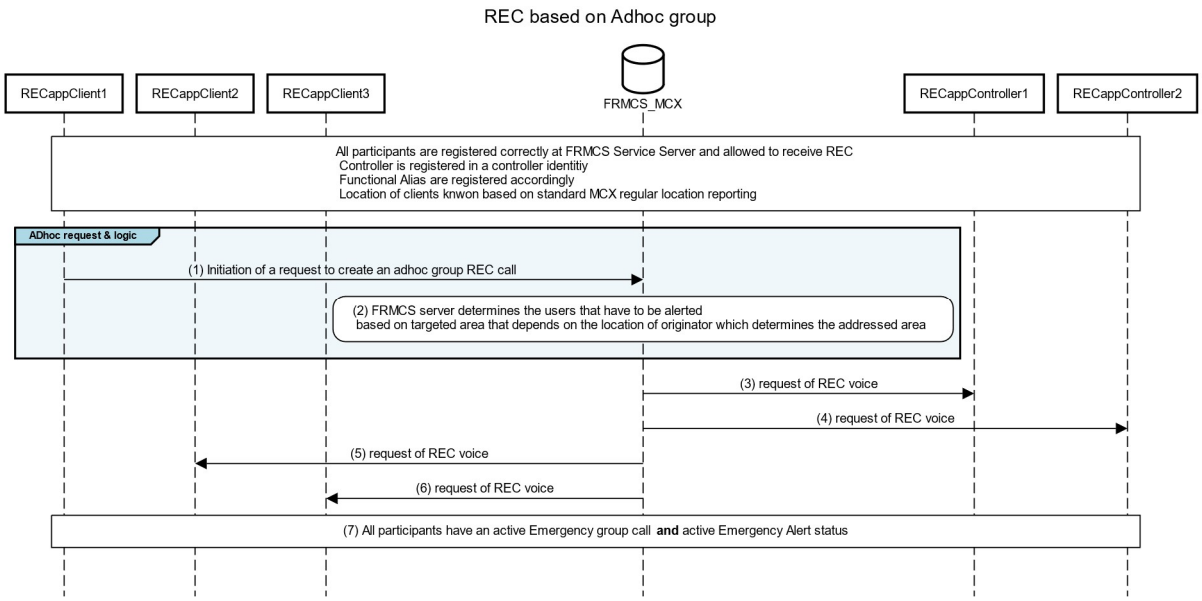

Figure 24:Simplified call flow for REC option 4

Open Items (to be completed):

- Location specific part not included explicitly in MiniWID but automatic selection based on criteria is allowed – location part thus can be added in FRMCS FIS, only server side relevant ➔ seems ok
- Add Emergency Alert support for Adhoc group requirements in SA6 ➔ 3GPP action
- Functional Alias support for Adhoc group requirements ➔ to be checked
- Check Late-Entry Functionality
    - Emergency alert ➔ to be checked
    - Emergency call ➔ to be checked
- Analyze Use Cases if they will work

8. Annex B: Interoperability requirements in EU

This annex is the placeholder for identifying the requirements relevant for interoperability in the European Union, i.e. the requirements, with respect to the authorisation in the EU according to the TSI, that are considered in the European Directives to be relevant for interoperability as fulfilling the essential requirements for the Control-Command and Signalling (CCS) subsystem related to safety and technical compatibility which must be met by the rail system, the subsystems, and the interoperability constituents, including interfaces according to the corresponding conditions set out in Directive (EU) 2016/797. It is mandatory that each railway subsystem in the EU meets these requirements on lines under the scope of the Directive and the CCS TSI to ensure technical compatibility between Member States and safe integration between train and track.

At this stage, the version of this specification is not considered complete for the purpose of tendering On-Board FRMCS equipment, and the identification of all requirements relevant for interoperability is for further study.

This annex is therefore only informative.