ETSI TR 103 459 V1.2.1 (2020-08)

Rail Telecommunications (RT);
Future Rail Mobile Communication System (FRMCS);
Study on system architecture

Reference
RTR/RT-0052

Keywords
architecture, FRMCS, railways

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

Contents

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 Report (TR) has been produced by ETSI Technical Committee Railway Telecommunications (RT).

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

Version x.y.z

where:

- x the first digit:
  - 0 presented to TC RT for information;
  - 1 presented to TC RT for approval; or
  - 2 greater indicates TC RT 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.

Modal verbs terminology

In the present document "**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.

Executive summary

Since the first studies on the successor to GSM-R have been launched by UIC in 2012, the railway community has been considering how to meet railway requirements with a future proof and flexible radio communication system.

The rail needs are defined in the User Requirements Specification (URS) [i.1] and the Telecom Onboard Architecture (TOBA) Requirements [i.2] delivered by the UIC Project Future Railway Mobile Communications System (FRMCS). From the UIC requirements, requirements relevant to 3GPP have been captured in 3GPP TR 22.889 [i.3]. Altogether, the stated requirements are the basis for the development of the GSM-R successor.

The present document is a study on FRMCS system architecture, which initially describes a potential logical FRMCS architecture that is suitable to meet the rail requirements according to the requirement documents cited before, and the key reference points that are to be specified. As one input to the design, it provides an analysis of specific challenges such as security, migration, positioning, etc., and derives their implications on the FRMCS architecture. The present document also describes several deployment scenarios (for instance related to setups with multiple transport networks operated by different entities), which are also relevant to the design of the FRMCS system architecture, as this should support all deployment scenarios that are currently envisioned. Beyond the description of the logical FRMCS architecture, the present document then elaborates on possible technical realizations of the FRMCS architecture through building blocks from 3GPP and from other standards bodies. Special emphasis is here put on consideration for the support of multiple onboard/handheld radios and/or multiple trackside transport domains, and the support of border-crossing scenarios. Finally, the present document provides a functional gap analysis and identifies risks, before listing topics for further study.

Introduction

The Technical Committee Rail Telecommunications (TC RT) is the "home" for those telecommunication aspects of rail transportation which are not part of the specification of the current mobile communication technologies themselves. TC RT is in particular responsible for the development and maintenance of GSM-R standards.

GSM-R has been a great success not only in Europe, where more than 100 000 km of railway tracks are daily operated through GSM-R, but also worldwide, and this number will double within the next years due to the on-going installations of this technology all over the world.

As the needs of the railways are constantly evolving, in particular in the context of the digitalisation of rail operation that is pursued in many countries, and considering the upcoming obsolescence of GSM-R technology, UIC launched in 2012 the first studies for a successor to GSM-R, pertinently named Future Railway Mobile Communication System (FRMCS). The UIC project then concretely delivered the new User Requirements Specifications (URS) [i.1] focusing mainly on rail communication needs - as a basis for the development of the GSM-R successor.

The present document is a study on the FRMCS system architecture, which defines a logical FRMCS architecture and likely deployment scenarios, and which elaborates in detail on possible technical realizations of the FRMCS system. The result of this study is expected to provide the basis for the subsequently following normative work on FRMCS in ETSI.

1 Scope

The present document is a technical report, in line with the scope and field of application of its related Work Item. In particular, it covers:

- Definition of key terms and a high-level description of the FRMCS architecture, as agreed among UIC and ETSI (see clauses 3 and 4, respectively).
- An analysis of the architectural implications of various requirements on the FRMCS system captured in UIC TOBA and 3GPP TR 22.889 [i.3], and of aspects such as identification and addressing, security, positioning and migration (see clause 5).
- A description of the logical architecture of the FRMCS system, including a description of the main logical entities and key reference points among these (see clause 6).
- A derivation of key deployment and border-crossing scenarios that the FRMCS architecture should support (see clause 7).
- An investigation of possible technical realizations of the FRMCS system, based on the usage of building blocks from 3GPP and other standards bodies (see clause 8).
- A gap analysis and identification of risks related to the FRMCS standardization, for instance due to its dependency on timelines of different standards bodies (see clause 9).

Finally, the present document identifies the next steps to ensure the complete definition of the FRMCS system.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user with regard to a particular subject area.

[i.1] UIC FRMCS URS v5.0: "User Requirements Specification".

[i.2] UIC FRMCS TOBA-7510 (V1.0.0) (April 2020): "FRMCS Telecom On-Board System - Functional Requirements Specification".

[i.3] 3GPP TR 22.889 (V17.2.0) (January 2020): "Study on Future Railway Mobile Communication System (FRMCS)".

[i.4] 3GPP TS 21.905 (V16.0.0) (June 2019): "Vocabulary for 3GPP Specifications".

[i.5] 3GPP TS 23.501 (V16.4.0) (March 2020): "System architecture for the 5G System (5GS) (Release 16)".

[i.6] 3GPP TS 24.501 (V16.4.1) (April 2020): "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (Release 16)".

[i.7] 3GPP TS 22.280 (V17.2.0) (December 2019): "Mission Critical Services Common Requirements (MCCoRe); Stage 1".

[i.8] 3GPP TR 28.801 (V15.1.0) (January 2018): "Telecommunication management; Study on management and orchestration of network slicing for next generation network".

[i.9] 3GPP TS 23.228 (V16.4.0) (March 2020): "IP Multimedia Subsystem (IMS); Stage 2".

[i.10] 3GPP TS 23.003 (V16.2.0) (March 2020): "Numbering, addressing and identification".

[i.11] 3GPP TS 23.280 (V17.2.0) (March 2020): "Common functional architecture to support mission critical services; Stage 2".

[i.12] UIC FRMCS TOBA-7540 (V1.0.0) (April 2020): "FRMCS Telecom On-Board System - Architecture Migration Scenarios".

[i.13] 3GPP TR 23.796 (V16.0.0) (March 2019): "Study on application architecture for the Future Railway Mobile Communication System (FRMCS) Phase 2".

[i.14] 3GPP TS 27.007 (V16.4.0) (March 2020): "AT command set for User Equipment (UE)".

[i.15] ETSI TS 123 002 (V15.0.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Network architecture (3GPP TS 23.002 version 15.0.0 Release 15)".

[i.16] 3GPP TS 24.193 (V1.2.0) (May 2020): "5G System; Access Traffic Steering, Switching and Splitting (ATSSS); Stage 3".

[i.17] IETF RFC 8743 (March 2020): "Multi-Access Management Services (MAMS)".

[i.18] 3GPP TR 23.783 (V0.10.0) (June 2020): "Study on Mission Critical (MC) services support over the 5G System (5GS)".

[i.19] IETF RFC 7542 (May 2015): "The Network Access Identifier".

[i.20] IETF RFC 1035 (November 1987): "Doman names - implementation and specification".

[i.21] IETF RFC 1123 (October 1989): "Requirements for Internet Hosts -- Application and Support".

[i.22] IETF RFC 3966 (December 2004): "The tel URI for Telephone Numbers".

[i.23] IETF RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[i.24] IEEE 802.11™: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.25] ETSI TS 123 271: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Functional stage 2 description of Location Services (LCS) (3GPP TS 23.271)".

[i.26] ETSI TS 123 282: "LTE; Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2 (3GPP TS 23.282)".

[i.27] TIA-603-D: "Land Mobile FM or PM Communications Equipment Measurement and Performance Standards".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

communication services: services enabling the exchange of information between two or more service users

complementary services: ancillary services, e.g. providing and/or utilizing the location of the service user, supporting communication services and the railway application stratum

FRMCS Mobile Application Client: client that enables authorization of an application to the FRMCS Mobile Gateway

FRMCS Mobile Gateway: gateway that provides access to the FRMCS Transport Stratum for FRMCS Users through FRMCS Service Client(s)

FRMCS Service Client: client that enables the use of the Communication Services and/or Complementary Services for the railway applications

FRMCS System: telecommunication system conforming to FRMCS specifications, consisting of Transport Stratum and Service Stratum

FRMCS User: human or machine making use of Communication Services and/or Complementary Services

FRMCS User Identity: unique identity associated with a single or multiple FRMCS User and can be complemented by alternative addressing schemes

legacy conversion: function that provides conversion towards legacy interfaces (e.g. V.24 serial interface)

NOTE: The Legacy Conversion provides encapsulation/de-capsulation for control and user plane data as well as the necessary conversion of the physical interfaces between legacy GSM-R UE and FRMCS.

mobile radio: 3GPP User Equipment or non-3GPP equivalent, which supports selected 3GPP and/or non-3GPP access (e.g. 4G, 5G, Wi-Fi, satellite)

on-board transport system: system that provides on-train only transport services and enables the interaction with the FRMCS Gateway and the FRMCS Service Stratum where applicable

proxy: person or entity that is acting or being used in the place of someone or something else

railway application stratum: railway-specific functionalities using services offered by the service stratum

reference point: conceptual point applicable for interaction between functional services that enables authorized functions, e.g. in the network, to access their services

service domain: implementation of (parts of) the Service Stratum which belongs to and/or is operated by a unique organization

service stratum: communication services and complementary services

train communication network: sub-system of the on-board transport system that aggregates various train backbones

transport domain: implementation of (parts of) the transport stratum which belongs to and/or is operated by a unique organization

transport stratum: set of access and corresponding core functions applicable for the FRMCS system

User Equipment (UE): equipment according to 3GPP terminology (see 3GPP TS 21.905 [i.4]) that allows access to 3GPP transport services

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
4G	Fourth Generation Mobile Networks
5G	Fifth Generation Mobile Networks
5GS	5G System
AF	Application Function
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
APN	Access Point Name
ARP	Allocation and Retention Priority
AS	Access Stratum
ATO	Automatic Train Operation
ATSSS	Access Traffic Steering, Switching & Splitting
ATSSS-LL	Access Traffic Steering, Switching & Splitting - Low Layer
CAPIF	Common API Framework
CCM	Client Connection Manager
C-MADP	Client Multi-Path Data Proxy
CP	Control Plane
CS	Circuit-switched
CT	Call Type
CTCS	Chinese Train Control System
EAP	Extensible Authentication Procedure
eDECOR	enhancements of DEdicated CORe networks
eNB	evolved NodeB
EPC	Enhanced Packet Core
EPS	Enhanced Packet System
ETCS	European Train Control System
EUG	ERTMS Users' Group
E-UTRA(N)	Evolved Universal Terrestrial Radio Access (Network)
E-UTRAN	Enhanced UMTS Terrestrial Radio Access Network
FC	Functional Code
FFS	For Future Study
FRMCS	Future Rail Mobile Communications System
FSSI	FRMCS Service Session Interface
FTS	Fixed Terminal Subsystem
GNSS	Global Navigation Satellite System
GRUU	Globally Routable User-agent URI
GSM-R	Global System for Mobile communication for Railways applications
GW	Gateway
HW	Hardware
IC	International Code
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public identity
IMS	Internet Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
IoT	Internet of Things
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IWF	InterWorking Function
KASME	Key Access Security Management Entries
LAA	Licensed-Assisted Access

LAN	Local Area Network
LBS	Location Based Service
LDS	Location Dependent Service
LTE	Long Term Evolution
LTE-U	Long Term Evolution-Unlicensed
LWA	LTE-WLAN Aggregation
MAC	Media Access Control
MAMS	Multi Access Management Services
MC	Mission Critical
MCData	Mission Critical Data
MCPTT	Mission Critical Push To Talk
MCVideo	Mission Critical Video
MCX	Mission Critical Services
MOCN	Multi Operator Core Network
MPTCP	Multi-Path Transmission Control Protocol
MSISDN	Mobile Subscriber ISDN Number
NAI	Network Access Identifier
NAS	Non-Access Stratum
NCM	Network Connection Manager
N-MADP	Network Multi Access Data Proxy
NR	New Radio
OB_{APP}	Onboard Application Interface
OB_{RAD}	Onboard Radio Interface
OSI	Open Systems Interconnection
PCF	Policy Control Function
PDU	Packet Data Unit
PLMN	Public Land Mobile Network
PLMN-ID	Public Land Mobile Network Identification
PS	Packet-Switched
PSTN	Public Switch Telephone Network
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RBC	Radio Block Centre
RFC	Request For Comments
RG	Residential Gateway
RRC	Radio Resource Control
RTT	Round-Trip Time
SBA	Service Based Architecture
SDAP	Service Data Adaptation Protocol
SDF	Service Data Flow
SDS	Short Data Service
SEPP	Security Edge Protection Proxy
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMF	Session Management Function
SRS	System Requirement Specification
SS7	Signalling System No 7
SST	Slice/Service Type
SW	Software
TCP	Transmission Control Protocol
TCRT	Technical Committee Rail Telecommunications
TETRA	Terrestrial Trunked Radio
TS_{FS}	Trackside FRMCS Service Interface
UE	User Equipment
UIC	Union Internationale des Chemins de fer (English: International Rail Union)
UIN	User Identification Number
UN	User Number
UP	User Plane
UPF	User Plane Function

URI	Uniform Resource Identifier
URLLC	Ultra-Reliable Low-Latency Communications
URS	User Requirements Specification
URSP	User Equipment Route Selection Policy
W-AGF	Wireline Access Gateway Function
WiFi™	Wireless Fidelity
WLAN	Wireless Local Area Network

3.4 Notion of logical architecture, technical realization and physical implementation

In the remainder of the present document, the FRMCS architecture is described in different forms, with a general differentiation between:

- **Logical architecture:** Describes the FRMCS system in the form of logical function blocks and reference points in between. The logical architecture is purposely kept solution-agnostic. Clauses 6 and 7 in the present document describe the FRMCS system from a logical architecture perspective.
- **Technical realization:** Describes one or multiple possibilities to realize the FRMCS system by using building blocks from 3GPP or other bodies. In the present document, clause 8 delves into technical realization options for the FRMCS system, with the aim to identify any possible technology gaps and ensure that the reference points in the logical architecture are defined in a meaningful way.
- **Physical implementation:** Describes how (parts of) the FRMCS system could be mapped to physical entities or products from a vendor. Since physical implementations are not relevant for standardization, they are only used for illustration purposes in the present document, for instance in clause 8.4 in the context of onboard architecture.

These forms of architecture description are also illustrated in figure 3-1.

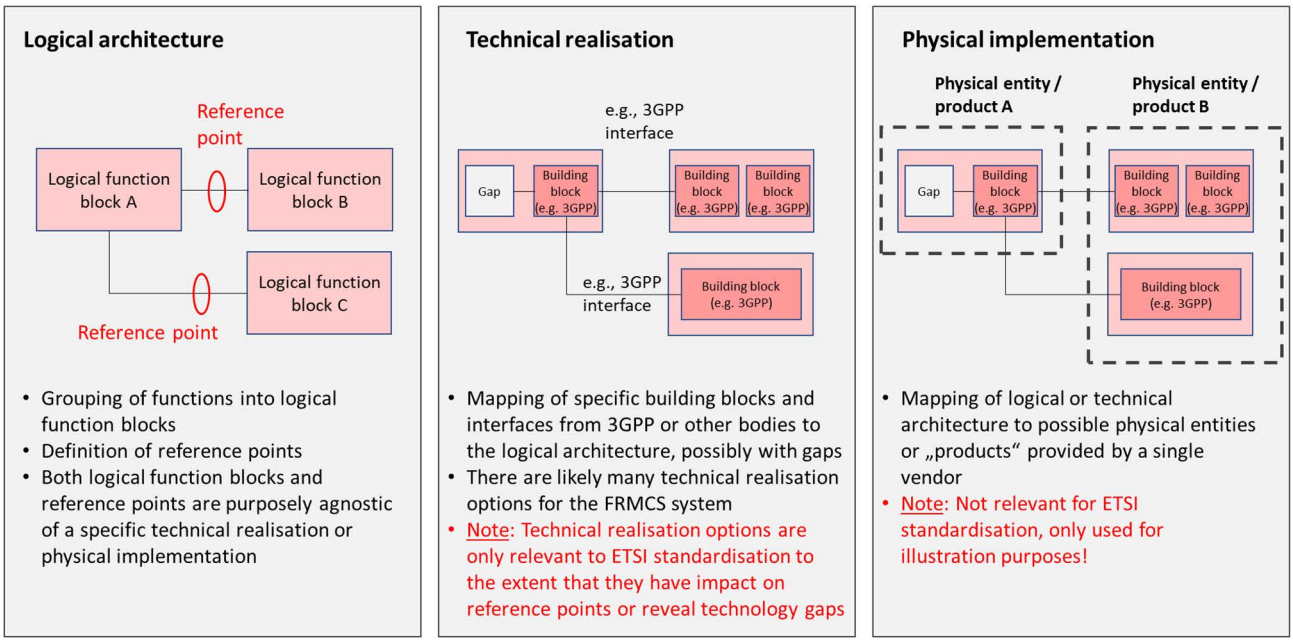

Figure 3-1: Notion of logical architecture, technical realization and physical implementation

4 High level description

One key objective behind the design of FRMCS is a clear separation between the so-called Railway Application Stratum, Service Stratum, and Transport Stratum, as illustrated in figure 4-1. The following definition applies:

- The **Railway Application Stratum** provides railway-specific functionalities using services offered by the Service Stratum.
- The **Service Stratum** comprises Communication services and Complementary Services:
  - **Communication Services** are services enabling the exchange of information between two or more service users.
  - **Complementary Services** are ancillary services, e.g. providing and/or utilizing the location of the service user, supporting Communication Services and the Railway Application Stratum.
- The **Transport Stratum** comprises the set of access and corresponding core functions applicable for the FRMCS system.

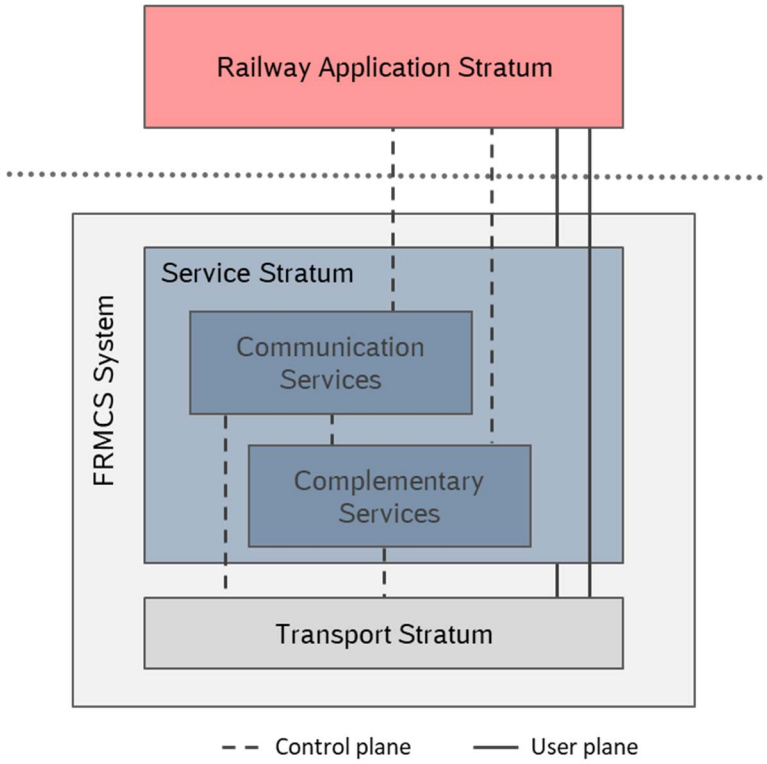

Figure 4-1: High-level FRMCS architecture overview

It is commonly assumed that:

- Applications in the Railway Application Stratum should use Communication Services to guarantee interoperable service behaviour and the deterministic and controlled use of the Transport Stratum. Once a service user, e.g. an application, has been authenticated and authorized itself to the Communication Service instances, the application should be able to obtain control about the services, and the system should allow a direct user plane connection for this application between Application Stratum and Transport Stratum if possible.
- Communication Services may use Complementary Services (and vice versa). In the Service Stratum, the control plane may contain user plane information content, e.g. MCData service SDS, embedded in the signalling content.

Which functions of the Service Stratum are covered by the Communication Services and Complementary Services is further elaborated in clause 6.2.

5 Analysis of architectural implications of key aspects to be covered by FRMCS

5.1 General

Before introducing the FRMCS logical architecture, clause 5 elaborates on requirements from UIC TOBA-7510 [i.2] and 3GPP TR 22.889 [i.3] which have explicit implications on the FRMCS architecture. In dedicated clauses, further elaboration on the functional and architectural implications of aspects such as addressing, migration, security, etc., is provided.

5.2 Analysis of architectural requirements from UIC TOBA

Table 5-1 lists requirements from UIC TOBA-7510 [i.2] with implications on the FRMCS architecture. **Note that the listed requirements are a snapshot from [i.2] and may change over time. They are only listed here for the purpose of a preliminary analysis.**

Table 5-1: Requirements from UIC TOBA-7510 [i.2] with FRMCS architecture impact

Number in UIC FRMCS TOBA-7510 [i.2]	Quoted requirement	Comment
R1 (clause 7.2.2.1)	"*The FRMCS On-Board System shall have the capability to simultaneously control multiple FRMCS Radio Modules.*"	Solutions for the support of multiple UEs/Mobile Radios are compared in clause 8.3 and assessed w.r.t. this requirement.
R2 (clause 7.4.2.1)	"*The FRMCS On-Board System shall have the capability to share FRMCS Radio Modules among different communication services (e.g. multiple applications using the same FRMCS Radio Module).*"	Solutions for the support of multiple UEs/Mobile Radios are compared in clause 8.3 and assessed w.r.t. this requirement.
R3 (clause 7.2.2.2)	"*The FRMCS On-Board System shall detect the non-availability/availability of transport capabilities provided by the FRMCS Radio Modules.*"	This translates into: • requirements on the FRMCS Mobile Gateway, see clause 6.2; • requirements on reference point OB_{RAD}, see clause 6.3.
R4 (clause 7.3.2.5)	"*The FRMCS On-Board System shall provide a mechanism to allow reestablishment of transport services using a different FRMCS Radio Module in case of a failure of the FRMCS Radio Module in use or upon detection of a persistent service outage of the FRMCS Radio Module in use.*"	Solutions for the support of multiple UEs/Mobile Radios are compared in clause 8.3 and assessed w.r.t. this requirement.
R5 (clause 7.5.2.1)	"*The FRMCS onboard system shall provide transport and communication service exposure, such as providing information about the network (e.g. PLMN ID) to which the FRMCS Radio Modules are registered.*"	This translates into requirements on both reference points OB_{APP} and OB_{RAD}, see clause 6.3.
R6 (clause 7.5.2.2)	"*The FRMCS On-Board System shall request a FRMCS Radio Module to select a certain network if requested by an application.*"	This translates into requirements on both reference points OB_{APP} and OB_{RAD}, see clause 6.3.
R7 (clause 7.5.2.3)	"*The FRMCS onboard system shall be able to process instructions to change the transport domain or service domain.*"	This translates into requirements on reference point OB_{APP}, see clause 6.3.
R8 (clause 7.5.2.4)	"*The FRMCS On-Board System shall establish a communication service using the transport services of a specific network if requested by an application.*"	This translates into requirements on both reference points OB_{APP} and OB_{RAD}, see clause 6.3.
R9 (clause 7.3.2.3)	"*The FRMCS On-Board System shall be able to establish multiple communication service sessions for the same application using the transport services from a single FRMCS Radio Module or different FRMCS Radio Modules.*"	This is captured in the design of the FRMCS Clients and FRMCS Mobile Gateway, see clause 6.2.

Number in UIC FRMCS TOBA-7510 [i.2]	Quoted requirement	Comment
R10 (clause 7.2.2.5)	"*The FRMCS On-Board System shall provide a mechanism to reallocate a communication session to a preferred transport service when it becomes available.*"	Solutions for the support of multiple UEs/Mobile Radios are compared in clause 8.3 and assessed w.r.t. this requirement.
R11 (clause 7.1.2.5)	"*Based on the QoS Profile, the FRMCS on-board system shall be able to determine:* *The need for using multiple transport services (increased reliability);* *The need for bandwidth aggregation;* *The suitable transport services/FRMCS Radio Modules;* *The preferred transport service/FRMCS Radio Module;* *The Initial FRMCS Radio Module;* *Which transport service to offload in case of capacity limitations.*"	This translates into requirements on the FRMCS Mobile Gateway, see clause 6.2.
R12 (clause 7.2.2.6)	"*The FRMCS On-Board system shall provide a mechanism to reallocate transport services to other FRMCS Radio Modules in order to optimise the overall FRMCS on-board system capacity. The transfer may also be triggered from trackside.*"	This translates into requirements on the FRMCS Mobile Gateway, see clause 6.2. Further, solutions for the support of multiple UEs/Mobile Radios are compared in clause 8.3 and assessed w.r.t. this requirement.
R13 (clause 7.3.2.4)	"*The FRMCS On-Board System shall be capable to aggregate the data received from multiple service or transport sessions and to split data to be sent across multiple service or transport sessions.*"	This translates into requirements on the FRMCS Mobile Gateway, see clause 6.2. Further, solutions for the support of multiple UEs/Mobile Radios are compared in clause 8.3 and assessed w.r.t. this requirement.

5.3 Analysis of architectural requirements from 3GPP TR 22.889

Table 5-2 to Table 5-7 list requirements from 3GPP TR 22.889 [i.3] with likely implications on the FRMCS architecture. **Note that the listed requirements are a snapshot from [i.3] and may change over time. They are only listed here for the purpose of a preliminary analysis of their possible implications on the FRMCS architecture.**

Table 5-2: Requirements from 3GPP TR 22.889 [i.3] related to overall FRMCS system architecture

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.9-004]	"*The FRMCS transport system including 3GPP and non-3GPP access shall be agnostic to Railway Applications.*"	This is inherent in the design of the FRMCS system based on separate application, service and transport stratums, see clause 4.
[R-12.9-005]	"*New access technology shall not require changes for the pre-existing application layer to be able to make use of this new access technology.* *NOTE: Changes are required if the application layer wants to make use of the new capabilities of a new access technology.*"	This is inherent in the design of the FRMCS system based on separate application, service and transport stratums, see clause 4.

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.9-008]	"*The FRMCS System shall be able to make use of one or more of the followings:* *3GPP radio access (i.e. 4G and/or 5G) through railway-dedicated licensed spectrum* *3GPP radio access (i.e. 4G and/or 5G) provided by public providers* *3GPP radio access (e.g. LTE-U) through unlicensed spectrum* *Non-3GPP radio access (e.g. IEEE 802.11 [i.24] based and/or satellite based)* *Wireline access* *NOTE 1: GSM-R, TETRA, and P25 are not considered as a radio access technology of FRMCS.* *NOTE 2: Not all of the radio access technologies may support all of the FRMCS requirements.*"	The FRMCS system as described in clause 4 and beyond in principle supports the usage of the listed access technologies.
[R-12.9-012]	"*Session continuity between 3GPP access and non-3GPP access shall not require FRMCS Users intervention.*"	The FRMCS architecture as captured in the present document explicitly allows for the concurrent usage and switching between 3GPP and non-3GPP access without FRMCS User intervention, as for instance elaborated in clause 8.3. Whether this completely fulfils the quoted notion of "session continuity" is to be clarified.
[R-12.22-002]	"*The FRMCS System shall provide a mechanism that minimizes the risk of single point of failure.*"	The FRMCS architecture captured in the present document explicitly facilitates the avoidance of single points of failure (e.g. through the usage of multiple onboard and/or trackside radios, core networks, etc., as for instance elaborated in clause 8.3).

Table 5-3: Requirements from 3GPP TR 22.889 [i.3] related to usage of multiple UEs and/or access domains

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.9-001]	"*The FRMCS System shall be able to manage 3GPP access systems and non-3GPP access systems (terrestrial and non-terrestrial) simultaneously.*"	The overall FRMCS architecture as description in clause 4 is explicitly designed to support 3GPP and non-3GPP access systems. The simultaneous handling of multiple access systems is elaborated in clause 8.3.
[R-12.9-002]	"*If provided by the FRMCS Equipment, the FRMCS Application on the FRMCS Equipment shall be able to make use of 3GPP and non-3GPP access systems simultaneously.*"	This relates to the capability of the FRMCS system to make use of multiple (3GPP and non-3GPP) access systems, which is elaborated in clause 8.3.
[R-12.9-003]	"*The FRMCS User shall not experience service interruptions in the usage of applications due to a change of an access system.*"	This relates to the capability of the FRMCS system to handle multiple UEs and/or access domains, see clause 8.3.
[R-12.9-009]	"*The FRMCS System shall consider the availability of radio bearer services at the position of the FRMCS User to allow communication.*"	This relates to the capability of the FRMCS system to handle multiple UEs and/or access domains, see clause 8.3.
[R-12.9-010]	"*The FRMCS System shall select appropriate radio bearer service with consideration of the FRMCS applications configurable preconditions (e.g. ranking of the available bearer services).*"	This relates to the capability of the FRMCS system to handle multiple UEs and/or access domains, see clause 8.3.

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.10.2-034]	"*The FRMCS System shall take into account the service attributes to allow selection of the available bearer services.*"	This relates to the capability of the FRMCS system to handle multiple UEs and/or access domains, see clause 8.3.
[R-12.22-001]	"*The FRMCS System shall be able to provide a mechanism to allow redundancy of transmission paths making use of multiple spectrum blocks.*"	This relates to the capability of the FRMCS system to handle multiple UEs and/or access domains, see clause 8.3.

Table 5-4: Requirements from 3GPP TR 22.889 [i.3] related to QoS management

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.10.2-008]	"*The FRMCS System shall detect and process the various user data traffic characteristics, latency and session reliability requirements. These requirements are summarized in table 12.10-2.*"	It is expected that only an FRMCS system based on 5G transport can in principle meet the quoted requirements (see 3GPP TS 23.501 [i.5] and 3GPP TS 24.501 [i.6]).
[R-12.10.2-011]	"*The FRMCS System shall be able to request service attributes (latency, reliability, guaranteed bitrate/ non-guaranteed bitrate and priority) from the underlying 3GPP transport system and if appropriate also from non-3GPP transport systems.*"	This requirement is fulfilled by a 5G system and also (with a different granularity of service attributes) by a 4G system. In this context, ATSSS is a potential building block to also meet this requirement for non-3GPP transport.
[R-12.10.2-014]	"*The FRMCS System shall be able to assess whether the communication service attributes received from the transport system are sufficient to support the communication service fully or in a restricted way and report this information to the FRMCS application."*	The 5GS supports mechanisms for E2E QoS monitoring including 3GPP- and non-3GPP accesses. The FRMCS System should include a real time E2E QoS monitoring to request QoS parameters, events, logging information etc. from the 5GS.
[R-12.10.2-035]	"*The FRMCS System shall be able to assign multiple individual FRMCS User communications having individual QoS profile to a single IP address.*"	An FRMCS system based on a 5GS supports this requirement. 4GS does not support this requirement.
[R-12.10.2-036]	"*The FRMCS System shall provide a mechanism to derive the communication characteristics of an application and map those on a data flow with a predefined QoS profile.*"	An FRMCS system based on a 5GS supports this requirement. 4GS does not support this requirement.
[R-12.16.2-008]	"*The FRMCS System shall select the bearer characteristics based on exchanged signalling information.*" NOTE: This requirement relates to interworking with external networks.	**For other MCX systems:** No specific requirement is defined in stage 1 technical specifications. **For LMR/PMR (e.g. TETRA, P25 and TIA-603-D [i.27]):** No specific requirement is defined in stage 1 technical specifications. **For PLMN and PSTN:** Based on 3GPP TS 22.280 [i.7], the MCX Service system will enable interworking with PLMN and PSTN telephony services. 3GPP Stage2/3 activity is still ongoing to define features to be supported by the Interworking Function (IWF). Specification of the IWF will be defined by ETSI later on. In conclusion, this requirement is not fully supported yet.

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.19.2.5-001]	"*The FRMCS System shall be able to support the segregation of transport data for different application categories.*"	An FRMCS system based on a 5GS (explicitly involving a 5G core) is expected to support this requirement, potentially through the usage of network slicing [i.8]. Note that the topic is for further investigation in 3GPP Rel. 17 and potentially beyond.
[R-12.19.2.5-002]	"*The FRMCS System shall support dedicated QoS handling for segregation of transport data.*"	An FRMCS system based on a 5GS (explicitly involving a 5G core) is expected to support this requirement, potentially through the usage of network slicing [i.8]. Note that the topic is for further investigation in 3GPP Rel. 17 and potentially beyond.

Table 5-5: Requirements from 3GPP TR 22.889 [i.3] related to interfaces and reference points

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.9-006]	"*The transport layer shall allow using IP as a generic interface.*"	This relates to design of reference point OB_{RAD}, see clause 6.3.
[R-12.9-011]	"*The FRMCS System shall provide indication to FRMCS application on which bearer service is being used.*"	This relates to design of reference point OB_{APP}, see clause 6.3.

Table 5-6: Requirements from 3GPP TR 22.889 [i.3] related to realm boundaries and border-crossing scenarios

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.21.2-001]	"*The FRMCS System shall provide the technical means to allow communication services between FRMCS Users that are belonging to different administrative realms of the FRMCS System i.e. Home FRMCS Network and Visited (FRMCS) Network.*"	Solutions for border-crossing scenarios are elaborated in clause 7.6.
[R-12.21.2-002]	"*The FRMCS System shall provide communication services to FRMCS Users visiting another administrative realm i.e. Visited (FRMCS) Network.*"	Solutions for border-crossing scenarios are elaborated in clause 7.6.
[R-12.21.2-003]	"*The FRMCS System shall support a mechanism for an administrator to determine if a FRMCS User is able to use communication services in the Visited (FRMCS) Network.*"	Solutions for border-crossing scenarios are elaborated in clause 7.6.
[R-12.21.2-004]	"*The FRMCS System shall be able to provide service continuity when relocating between FRMCS Network without the FRMCS User noticing the change.*"	Solutions for border-crossing scenarios are elaborated in clause 7.6.
[R-12.21.2-005]	"*The FRMCS system shall be able to provide the same Quality of Service for the use of FRMCS Applications regardless of whether the FRMCS User is using the Home FRMCS Network or Visited (FRMCS) Network.*"	Solutions for border-crossing scenarios are elaborated in clause 7.6.
[R-12.21.3-001]	"*The FRMCS System shall be able to establish communication services based on FRMCS Functional Identity(ies) between FRMCS Users or FRMCS Equipment associated with different FRMCS Networks.*"	Solutions for border-crossing scenarios are elaborated in clause 7.6.
[R-12.21.3-002]	"*The FRMCS System shall be able to establish a communication services based on FRMCS Functional Identity(ies) associated with different FRMCS Networks.*"	Solutions for border-crossing scenarios are elaborated in clause 7.6.

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.21.3-003]	"*The FRMCS System shall provide the necessary means for a FRMCS User or FRMCS Equipment to register and deregister FRMCS Functional Identity(ies) with the Home FRMCS Network and/or with the Visited (FRMCS) network.*"	Solutions for border-crossing scenarios are elaborated in clause 7.6.
[R-12.21.3-004]	"*When the FRMCS User or FRMCS Equipment is relocating between networks, the FRMCS System shall provide a mechanism to perform necessary registration/deregistration of one or multiple FRMCS Functional Identity(ies) with the Visited (FRMCS) Network operator and inform the Home FRMCS Network.*"	Solutions for border-crossing scenarios are elaborated in clause 7.6.

Table 5-7: Other requirements from 3GPP TR 22.889 [i.3] with possible FRMCS architecture implications

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-9.3.2-007]	"*At the time of initialisation the FRMCS-system shall be able to determine the FRMCS Equipment Type.*"	It is expected that rail-specific solutions should be introduced to meet this requirement (as this is outside scope of 3GPP), but this requires further study.
[R-12.16.2-009]	"*The FRMCS System shall select the appropriate interconnection type, e.g. CS or PS based on the destination address of the target user.*"	As captured in clause 5.7, the FRMCS system will not support circuit-switched (CS) connectivity.
[R-12.20.6-002]	"*The service capabilities of an FRMCS Equipment shall be attributable individually to multiple FRMCS Users.*"	No direct relation to FRMCS architecture, is covered inherently in 3GPP TS 22.280 [i.7], see [R-5.15-002 and [R-5.15-003].
[R-12.20.6-003]	"*When an FRMCS Equipment is simultaneously used by multiple FRMCS Users, the communication for each of the FRMCS Users shall receive its required priority and QoS (latency and reliability) within the FRMCS System.*"	No direct relation to FRMCS architecture, is covered inherently in 3GPP TS 22.280 [i.7], see [R-5.15-002 and [R-5.15-003].
[R-12.20.6-004]	"*When an FRMCS Equipment is simultaneously used by multiple FRMCS Users, each of the FRMCS Users shall be individually addressable.*"	No direct relation to FRMCS architecture, is covered inherently in 3GPP TS 22.280 [i.7], see [R-5.15-002 and [R-5.15-003].

5.4 Identification and addressing

5.4.1 General

Clause 5.4 addresses the necessary measures to separate the identification dedicated to the application, transport and communication strata as part of the FRMCS System. If needed, applications such as ETCS may use their own identification methodology which could differ from application to application.

The following assumptions are considered in the identity context:

- Identification and addressing is based on the usage of identities.
- Identities in each of the strata have to be unique.
- From a security point of view, and supported through these means, every user in a system should be identifiable and should be able to authenticate itself.

Identities are required for applications, communication services, transport services and their respective users based on the requirement [R-12.15.2-001] in 3GPP TR 22.889 [i.3]. There are application user identities (e.g. ETCS RBC ID), communication services user identities (e.g. MCPTT ID, MCVideo ID, MCData ID) or transport service user identities (e.g. MAC address).

In general identities used in different strata are independent among themselves and are only used in the respective stratum. Such an approach enables independent exchangeabilities and evolutions in the FRMCS System.

5.4.2 Design assumptions

The following clauses refer to the requirements according to 3GPP TR 22.889 [i.3], clause 12.

With the decoupling of the applications from the communication services and these from the transport system, the usual compact GSM-R user identification approach will no longer be able to withstand this. This is also to be understood in the context of the Mobile/FTS convergence when FRMCS users do not use 3GPP UEs. But future rail vehicle equipment demands more flexibility for the operation of applications that are not necessarily coupled with 3GPP UEs.

It is a requirement that FRMCS users and their assigned services are uniquely identifiable while using communication services, but this service identification has nothing in common with the 3GPP transport system credentials.

Based on this unique identification the general authorization to communicate (point-to-point communication, group communication), authorization to use certain basic services (voice, video, data), authorization to use certain applications based on the basic services will be performed.

In addition to the unique (user) identification within the communication service(s), depending on the application, the users may use specific identifications. As an example, the ETCS application is mentioned here. Vehicle identification and Radio Block Controller (RBC) recognition scheme is regionally applicable but uses individual country and supplier identifications. Accordingly, user IDs within the application are supplementary to the communication service user identification. The use of service identities within the application needs to be avoided (e.g. RBC ISDN number used in the application). Otherwise it will cause again dependencies.

What is left for the transport? In general, the transport manages the access to the medium. For example, the MAC address (LAN environment) or IMEI and the IMSI (3GPP environment) is used to distinguish between cascaded and non-cascaded access to the medium.

Typical for non-cascaded access is the 3GPP-capable handheld design with a single access type.

Typically for a cascaded access to the medium will be the future vehicle equipment, where local access to the local medium on the vehicle takes place, e.g. LAN that uses in the second instance the 3GPP medium between the vehicle and the terrestrial network.

Accordingly, different transport systems have different identifiers. For instance, LAN uses the unique MAC address for the device used, while the 3GPP access uses the IMSI to authorize access to the 3GPP (transport) system. The IMEI as such is only used to identify the equipment type by its serial number.

IP addresses as layer 3 addressing element within the OSI layer model are mainly used to be able to transport data from its sender to the intended recipient. They do not have a user addressing function, since they can no longer be unambiguously assigned to the addressee or sender when using IP proxy functions or IP traversal setups.

Conclusion: With the decoupling of the application from the communication services and these from the transport system, this requires a consistent decoupling of the necessary identification features. Accordingly, the transport system, the communication services and, if applicable, the application have unique identification features with regard to device, service and user. For operational purposes, in addition to mandatory service addressing, e.g. MSISDN or MC Service ID, an alternative user addressing schemes, e.g. based on a functional alias can be used, but this should always be used according to uniqueness principles with the mandatory service identification.

5.4.3 Identification and addressing schemes

5.4.3.1 General

To be able to independently follow the evolution of the transport systems and the communication services, it needs to be ensured that user´s application identification (if available) is independent of the communication service identification which itself is independent of the identifications of the transport systems (including those of devices). Accordingly, this also provides no link or dependencies of the identification features or addressing elements between transport and services, as also shown in figure 5-1. If an application uses specific addressing elements, the service user can be uniquely identified inside the application.

Service identities are used to differentiate between multiple service types, i.e. voice, video, and data.

This allows flexible operation of the services by different providers, e.g. a voice service is hosted by the rail infrastructure manager, while the data service is hosted and operated by an external care provider.

Alternative addressing schemes, e.g. functional alias, are complementary to the service identification features and have therefore no standalone characteristics.

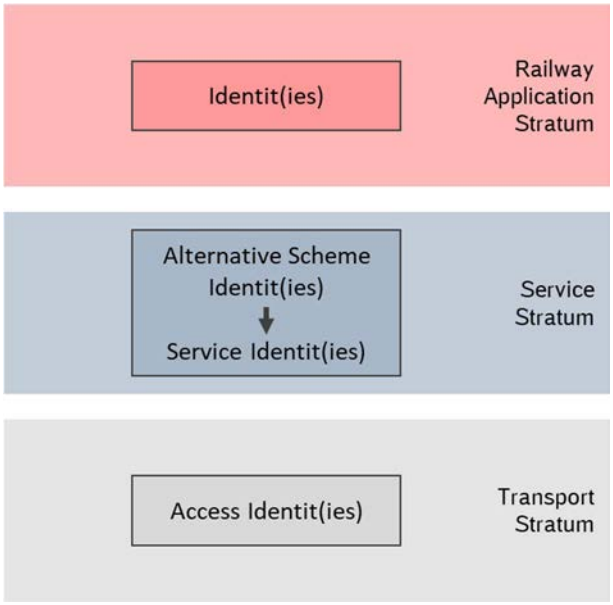

Figure 5-1: Identification in FRMCS

For uniqueness reasons, transport, communication service and, if available, application identities, belong to the corresponding standalone administrative realm. The duplication of the identities within the same administrative realm needs to be prohibited. Application identities, service identities and their corresponding alternative identities can be used with transport systems belonging to different transport administrative realms, e.g. during relocation among transport systems. The serving transport system may resolve the administrative home transport system to retrieve the applicable transport credential. The same applies when relocating among service domains. The serving service domain may restrict the use of services and their corresponding identities compared to the home service domain. Accordingly, service identities may be obtained from the new serving service domain.

For data hosts, servers or simple video cameras that are neither aware about service domain credentials nor service domain identities, the service domain provides the necessary means to identify the data host and the related exchange of information.

5.4.3.2 Identification and addressing in the application stratum

This is left to each individual application and is not further elaborated in the present document.

5.4.3.3 Identification and addressing in the service stratum

5.4.3.3.1 Introduction and definitions

Based on FRMCS basic system architecture assumptions, the service user is to be addressed within the Service Stratum independently of the transport stratum. Hence, considering the applicable 3GPP technical specifications, the service user addressing may result from the fact that the Service Stratum will possibly consist of IMS and the MCX service system. The user addressing requirements contained therein form the basis for the FRMCS User addressing. It should be pointed out once again that IMS and the corresponding service addressing scheme can be used independent of the underlying transport system.

For the use of IMS 3GPP TS 23.228 [i.9] applies, which accesses the general user addressing and identifications of 3GPP TS 23.003 [i.10]. Accordingly, the following main definitions for user addressing within the IMS may also apply in the FRMCS System:

- **Home Network Domain** consists of one or more labels and is in the form of an Internet domain name, e.g. operator.com, according to IETF RFC 1035 [i.20] and IETF RFC 1123 [i.21].
- **Network Address Indicator** (NAI) IETF RFC 7542 [i.19] is the user identity submitted by the user or its corresponding client during network access authentication. In roaming, the purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request.
- **Private User Identity**, in the context of IMS referred to as IMPI, is used for the user in a form of username@realm for a representation of the IMSI to be contained within the Network Address Identifier for the private identity specified in clause 2.1 of IETF RFC 7542 [i.19]. It is a unique global identity defined by the Home Network Operator.
- **Public User Identity**, in the context of IMS referred to as IMPU, is used by any user for requesting communication to another user. The Public User Identity takes the form of either a SIP URI (see IETF RFC 3261 [i.23] form "sip:username@domain") or a Tel URI (see IETF RFC 3966 [i.22] form "tel:+<CC><NDC><SN>" E.164 number format).

5.4.3.3.2 Relationship between identities in the IMS

The user profile in the home administrative realm is responsible for the assignment between the Private User Identities and the corresponding Public User Identities. The service profile contains all service relevant configuration applicable for Public User Identity. One service profile can be attached to multiple Public User Identities that corresponds to the same Public User Identity, as also shown in figure 5-2.

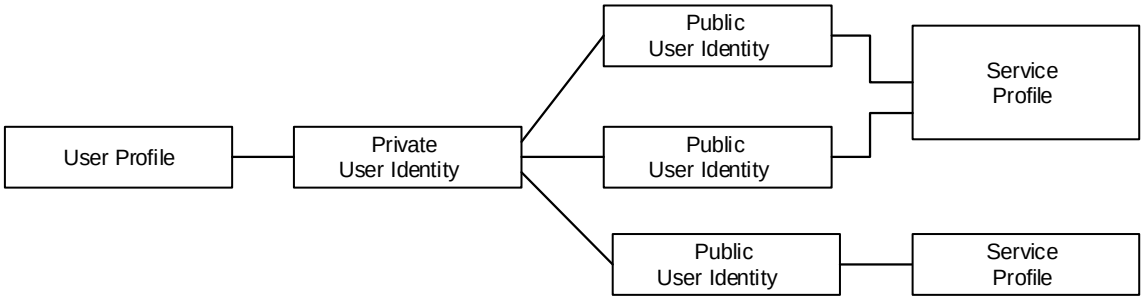

Figure 5-2: Association between user profile and user identities (3GPP TS 23.228 [i.9])

A Public User Identity may have one or more Globally Routable User-agent URIs (GRUUs) which consist of two types:

- Permanent GRUU (P GRUU); and
- Temporary (T-GRUU).

Both types of GRUU can only be associated with the Public User Identity and are generated and assigned to the corresponding UE during registration as pair of one P-GRUU and one T GRUU.

The relations between Public User Identity, GRUU and UE are illustrated in figure 5-3. Here, the following cases are considered:

- A UE is associated with multiple Public User Identities, a dedicated GRUU set is associated with each.
- Different UEs can register with the same Public User Identity, a different GRUU set is associated with each.

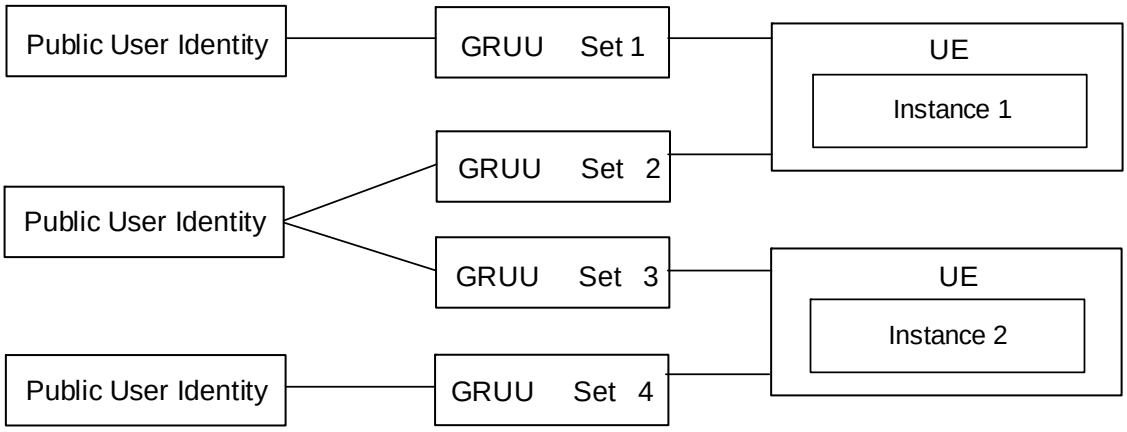

Figure 5-3: Association of Public User Identities, GRUU sets and UEs (3GPP TS 23.228 [i.9])

5.4.3.3.3 Basic MC service identities

The MC service system (3GPP TS 23.280 [i.11]) distinguishes between the application plane and SIP signalling control plane. The application plane encompasses all the additional functions, e.g. management or configuration management necessary for mission critical communication purposes. The following Mission Critical identities exist and apply:

- **Mission Critical (user) Identity (MC ID)** uniquely identifies the MC service user to the identity management server which is linked to a set of credentials (e.g. biometrics, secureID, username/password) that may not necessarily be tied to a single mission critical service. The MC ID and the MC service ID may be the same.
- **MC Service (user) Identity (MC Service ID)** is a globally unique identifier within the MC service that represents the MC service user. An MC service ID may also identify one or more MC service user profiles for the user at the application layer (see also figure 5-4).

There are attributes associated with the MC service ID configured in the MC service that relate to the human user of the MC service. This information identifies the MC service user, by name or role, the user organization, and the MC service user's service subscription to one or more MC services (i.e. MCPTT, MCVideo and MCData). The MC service ID has the form of an URI.

5.4.3.3.4 Alternative MC service identities

An **MC service - functional alias** provides a complementary, role-based user identification scheme which can be used by MC service users for operational purposes in the form of meaningful elements such as the function, the order number or vehicle identifications that can be used within any form of MC service communication. For reasons of illustration, a related requirement on the format of functional addressing in 3GPP TR 22.889 [i.3] is quoted in table 5-8. A functional alias takes a form of a URI and is complementary to the MC Service ID.

Each functional alias is subject to the uniqueness principle within an organization and can be shared simultaneously by several MC service users.

Table 5-8: Requirement related to functional addressing in 3GPP TR 22.889 [i.3]

Number in 3GPP TS 23.228 [i.3]	Quoted requirement
[R-9.3.9-002]	"*The FRMCS System shall support functional addressing format consisting of:* *IC+CT+UN* *IC International code is used to route calls to the appropriate GSM-R network* *CT Call Type prefix defines how to interpret the User Number (UN) as train function number, engine function number, group calls, etc.* *UN User Number is of variable length and depends on the information i.e. train function number etc. Within the UN a Functional Code (FC) is associated and provides the information of the person or equipment on a particular train, or a particular team within a given area. Therefore, the UN consists of User Identification Number (UIN) i.e. train number etc. and the Functional Code (FC) resulting into: UN= UIN+FC.* *A functional address only consists of numeric characters.*"

5.4.3.3.5 Relationship identities

In the MC service system. the SIP signalling control plane depends upon the use of both a Private User Identity and one or more Public User Identities.

The Private User Identity is used to find corresponding credentials for authentication and fulfils the same functions as the IMPI defined in 3GPP TS 23.228 [i.9]. The Public User Identity is the identifier to enable signalling messages to be routed through the SIP system. The Public User Identity fulfils the same functions as the IMPU defined in 3GPP TS 23.228 [i.9].

The SIP core may generate public GRUUs and temporary GRUUs in order to uniquely identify MC service UEs when a user logging on from multiple devices or multiple users sharing the same UE as described in clause 5.4.3.3.2.

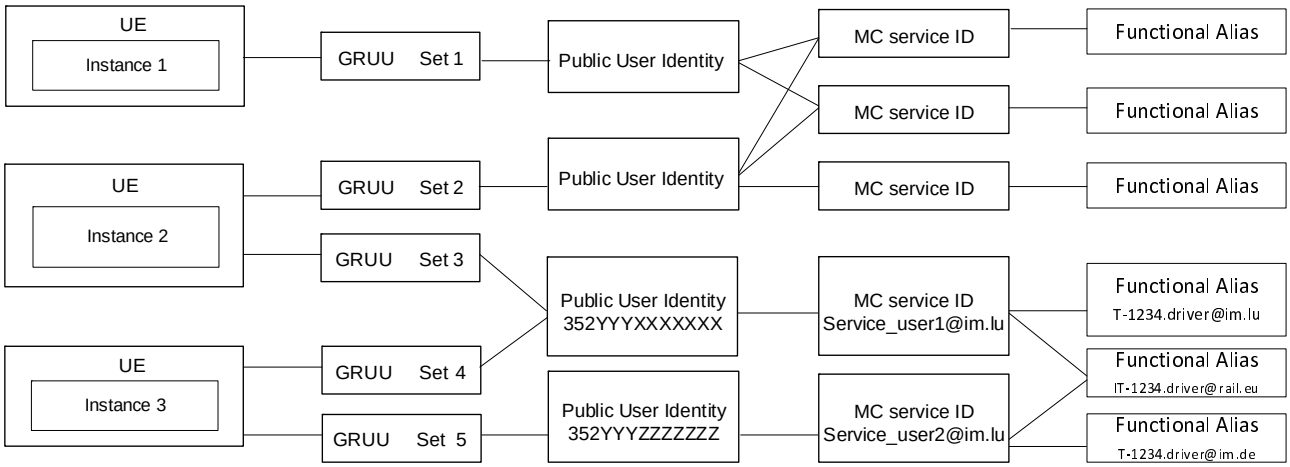

Figure 5-4: Relationship identities

The following relationships exist between the MC service ID(s) and the Public User Identity(ies), as also depicted in figure 5-4:

- an MC Service ID may be mapped to one or more Public User Identities;
- an MC Service ID may be mapped to one or more public GRUUs.

The following relationships exist between the MC service ID(s) and functional alias(es):

- an MC service ID may be associated with to one or more functional alias at the time; and
- a functional alias may be associated with one or more MC Service ID's at the time (e.g. sharing of one functional alias by multiple MC service users at the time).

In the lower part of figure 5-4 it can be seen that a functional alias (IT-1234.driver@rail.eu) can be used by two MC Service IDs at the same time, although other functional aliases can also be used at the same time. These MC Service IDs use different Public User Identities, which are then integrated into different GRUU sets. The example of the Public User Identity 352YYYXXXXXXX shows that this user can be reached via both UE instance 1 and UE instance 2.

5.4.3.4 Identification and addressing in the transport stratum

Identification and addressing in the transport stratum is defined in 3GPP TS 23.501 [i.5].

5.4.4 Implications on the FRMCS system architecture

So far, no major implications from identification and addressing needs on the FRMCS System architecture as such (i.e. in terms of reference points, etc.) have been identified. However, the need for a clear separation of identities and addressing schemes in application, service and transport stratum, as introduced in clause 5.4.1, and various definitions introduced in clause 5.4.3 are reflected throughout the remainder of the present document.

5.5 System Security

5.5.1 Introduction and requirements

System security should provide or support the required features and functions to:

- ensure all users are identified and authenticated;
- protect the service and transport stratum against unauthorized access;
- defend the service and transport stratum from external threats and risks;
- mitigate any implications from malicious attacks;
- report any intrusion or malicious behaviour of, e.g. users or FRMCS System internal functions;

with the aim to protect the Service and Transport Stratum. For reference, related requirements from 3GPP TR 22.889 [i.3] are quoted and shortly commented in table 5-9.

The key attributes of a secured system, which are referred to in the remainder of clause 5.5, are typically listed as

- data integrity;
- data confidentiality;
- information privacy;
- non-repudiation (traceability) of data origin;
- availability.

Table 5-9: Security-related requirements from 3GPP TR 22.889 [i.3]

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.15.2-001]	"*The FRMCS System security framework shall enable the use of unique identities.*"	Covered in identification context in clause 5.4.
[R-12.15.2-002]	"*The FRMCS System security framework shall allow the grouping of identities.*"	Covered in identification context in clause 5.4.
[R-12.15.2-003]	"*The FRMCS System security framework shall provide mechanisms to authenticate a unique identity.*"	Covered in identification context in clause 5.4.
[R-12.15.2-004]	"*The FRMCS System security framework shall provide authentication mechanisms required for the secured interaction between FRMCS network functions.*"	Covered in clause 5.5, likely a matter of implementation.
[R-12.15.2-005]	"*The FRMCS System security framework shall provide mechanisms to authorise communications and the use of applications.*"	Covered in clause 5.5.
[R-12.15.2-006]	"*The FRMCS System security framework shall provide a management of identities, passwords and keys required for the protection of FRMCS User communication, the interaction between FRMCS network functions as well as subscribers and service-related data.*"	Covered in clause 5.5. Protection of "interaction between FRMCS network functions" likely implementation matter.
[R-12.15.2-007]	"*The FRMCS System security framework shall be able to block the use of any FRMCS Equipment when it is detected as being stolen or lost.*"	To be discussed, likely implementation matter.
[R-12.15.2-008]	"*The FRMCS System security framework shall be able to unblock the use any recovered stolen or lost FRMCS Equipment.*"	To be discussed, likely partly a matter of implementation.
[R-12.15.2-009]	"*The FRMCS System security framework shall protect the services provided by the FRMCS System; bearer flexible access including 3GPP as well as non-3GPP access; interaction between the FRMCS end user devices and FRMCS network; interaction between FRMCS network functions; stored data within the FRMCS System; interworking between a FRMCS System and another FRMCS System; Interworking between a FRMCS System and a legacy system.*"	Touched in clause 5.5, though to be studied in detail.

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-12.15.2-010]	"*The FRMCS System security framework shall prevent software-based attacks which have an impact on any of the following security attributes: data confidentiality; information privacy; data integrity; non-repudiation of data; FRMCS System availability.*"	Touched in clause 5.5, though to be studied in detail.
[R-12.15.2-011]	"*The FRMCS System security framework shall be able to detect software-based attacks which have an impact on any of the following security attributes: data confidentiality; information privacy; data integrity; non-repudiation of data transfer; FRMCS System availability.*"	Touched in clause 5.5, though to be studied in detail, likely a matter of implementation.
[R-12.15.2-012]	"*The FRMCS System security framework shall be able to react on detected software-based attacks which have an impact on any of the following security attributes: data confidentiality; information privacy; data integrity; non-repudiation of data transfer; FRMCS System availability.*"	Touched in clause 5.5, though to be studied in detail, likely a matter of implementation.
[R-12.15.2-013]	"*The FRMCS System security framework shall provide procedures and mechanisms for management of FRMCS System security.*"	To be discussed, likely implementation matter.
[R-12.15.2-014]	"*The FRMCS System security framework shall be able to track users' actions such as usage of communication services, management operations, configuration changes, etc.*"	To be discussed, likely implementation matter.
[R-12.15.2-015]	"*The FRMCS System security framework shall be able to store security related data for post-analysis, e.g. forensic.*"	To be discussed, likely implementation matter.

5.5.2 Expected security layers in the FRMCS system

Before delving into the details of the required security functions in the FRMCS system, it is important to stress that there will be independent security layers in the different strata of the FRMCS system, as shown in figure 5-5:

- In the Railway Application Stratum (depending on the exact application), there are security mechanisms (for instance used in the context of application safety), which are independent of the FRMCS System and not covered in the present document.
- In the Service Stratum:
  - there will be security mechanisms between the FRMCS Mobile Application Client representing an onboard/handheld application (see clause 6.2) and the FRMCS Mobile Gateway to ensure that only authenticated and authorized onboard/handheld applications may access the FRMCS System;
  - there will be security mechanisms on service level between FRMCS Service Clients (see clause 6.2), and between FRMCS Service Clients and the FRMCS Server assuring authentication, data integrity, data confidentiality and data privacy.
- In the Transport Stratum, there will be security mechanisms (e.g. from 3GPP security architecture for 3GPP-based transport domains) that are independent of the Railway Application Stratum and Service Stratum.

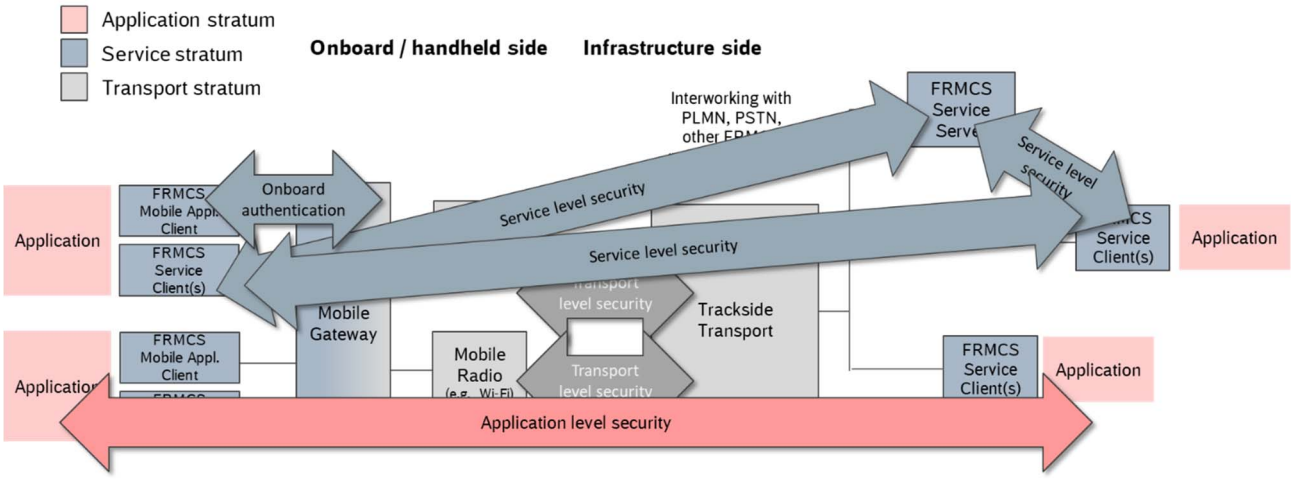

Figure 5-5: Expected security layers in the different strata of the FRMCS system

5.5.3 Required security functions

Required security functions in the user-, control- and management plane in Service and Transport Stratum for on- and off-network communication can be grouped as:

- **Identification and Authentication** (e.g. at the beginning of a data transmission or for an access to the communication or transport stratum), with needed functions:
  - Identity management.
  - Certification management.
- **Authorization** (e.g. at the beginning of a data transmission or for an access to the communication or transport stratum), with needed functions:
  - Identity management.
  - Certification management.
  - Role management.
  - Protocol data management (e.g. time stamps or location stamps).
- **Key and password management**, with needed functions:
  - Generation, transmission, revocation and deletion of keys and passwords.
  - Certification management.
  - Encryption.
  - Data integrity check.
  - Context check (time, sequence of events, location, mobility, etc.).
- **Secured data transmission**, with needed functions:
  - Encryption.
  - Data integrity check.

Table 5-10 now elaborates on how the aforementioned security functions should be covered in the Transport and Service strata. Note that the expected security protection outlined in the table refers to the Transport and Service strata of a single FRMCS System and those of interconnected FRMCS Systems. In the latter case, the respective interworking between the systems has to be protected as well, e.g. by SEPP.

As shown in the table, each access system of the FRMCS Transport Stratum is expected to provide identification, authentication and authorization for the user that gains transport services. For this, each access system may provide individual key management approaches, but the FRMCS system is expected to provide means for a consolidation of those.

Table 5-10: Expected security protection in Transport Stratum and Service Stratum

Security Attributes	Transport Stratum	Service Stratum
Integrity	Matter of implementation	Protection of any kind of data (e.g. positioning information, user data). Needed functionalities: • Integrity check – Key management – Identity management.
Confidentiality	Matter of implementation	Protection of any kind of data (e.g. positioning information, user data). Needed functionalities: • Encryption – Key management: ▪ Identity management.
Privacy	Protection of subscriber identities' integrity and confidentiality	Protection of subscriber identities' integrity and confidentiality.
Non-Repudiation	Matter of implementation	Traceability of data origin: Needed functionalities: • Authentication: – Identity management. – Certification management.
Availability	Protection of Transport Stratum's availability Needed functionalities: • (Radio)-access protection: – Identification and authentication: ▪ Identity management. ▪ Key management. • Internal security functions (e.g. in the control and management/configuration plane of the Transport Stratum) are matters of implementation. • Security functions in the Transport Stratum at interfaces to/from external systems/network are matters of implementation.	Protection of Service Stratum's availability. Needed functionalities: • Access protection: – Identification. – Authentication. – Authorization: ▪ Identity management. ▪ Role management. • Internal security functions (e.g. in the control and management/configuration plane of the Service Stratum) are matters of implementation. • Security functions in the Service Stratum at interfaces to/from external systems are matters of implementation.

5.5.4 Required interfacing with external systems

For the secured operation of the FRMCS system the following interfacing with external systems are needed:

- **Interfacing with an external Fraud Protection system**, with needed functions:
  - Disabling functionality from a FRMCS System component from normal operation if is reported/recognized as stolen or lost (e.g. based on time, location, mobility, etc.).
  - Re-enabling a FRMCS System component to normal operation if is reported/recognized as recovered.
- **Interfacing with an external system for the detection of threats and attacks**, with needed functions:
  - Anomaly detection (e.g. time, sequence of events, location, mobility, etc.).
  - Correlation of events (e.g. time, sequence, location, mobility, etc.).
  - System's performance and functionality monitoring.
  - System's (e.g. data base) integrity check.
  - Log-file processing.
  - Communication matrix.
  - Honey-pot.

  - SIEM (Security information and event management).

- **Interfacing with an external system necessary for the reaction on threats and attacks**, with needed functions:
  - Traffic and event monitoring.
  - Reporting.
  - Short-term, midterm and long-term reactions.
- **Interfacing which enables forensic analysis**, with needed functions:
  - Traffic and event monitoring.
  - Reporting.
  - Detection on threats and attacks.
  - Fraud protection.

5.5.5 Implications on the FRMCS system architecture

The aforementioned security needs have implications on the design of various reference points in the FRMCS system, for instance the expected OB_{AUTH} reference point between FRMCS Onboard Application Clients and the FRMCS Mobile Gateway, and the expected interworking among multiple FRMCS systems and with external systems, as covered in clause 6.3.

5.6 Positioning

5.6.1 Definitions

The following definitions are essential in the field of position determination to consistently describe the setting.

Positioning is a functionality captures the current physical location, speed and optionally the direction vector. A distinction is made between absolute and relative positioning.

An **absolute position** corresponds to the geographical position at the time determining the position.

The **relative position** corresponds to a position in relation to a particular reference point, e.g. conductor on a train relative to the heading of the train.

A **position-fix** corresponds to a position determination which may require one or more position determinations that results in a final absolute position specification of the corresponding device. A distinction is made according to initial position-fix and consecutive position-fixes.

An **initial position-fix** only encompasses the initial determination of the position of the corresponding device, e.g. after power up.

Consecutive position-fixes are referred to as those that occur after the initial position fix.

Positioning sources are referred to as actively providing positioning information of the affected device. This also encompasses possible external positioning sources. In the course of the document, the simultaneous use of different positioning sources is used as hybrid-positioning.

Hybrid positioning uses more than one positioning source at the same time. This method can affect positioning accuracy and the resulting confidence statement on the actual position.

Positioning accuracy describes the deviation of the current position-fix to the real geographical position.

The **reference information** for a position source determines the deviation between the detected position and the actual position of the user, which can be used for correction purposes in the position determination.

Location Estimate (ETSI TS 123 271 [i.25]) geographic location of a user expressed in latitude and longitude data, the velocity and direction.

Location guide information, e.g. track maps, encompassing external additional information that can be used to increase positioning accuracy.

Location Based Service (ETSI TS 123 271 [i.25]) utilizes the available location information of the user.

Location Dependent Service (ETSI TS 123 271 [i.25]) is available (pull type) or is activated (push type) when the user arrives to a certain area. The push type activation will be confirmed by the user.

Location Independent Service (ETSI TS 123 271 [i.25]) can be activated anywhere in the network coverage and requires a subscription in advance (pull type).

Location Retrieval Function (ETSI TS 123 271 [i.25]) is the functional entity that handles the retrieval of location information for the corresponding user including, where required, interim location information, initial location information and updated location information.

5.6.2 General

Clause 5.6 is concerned with the user's localization and its necessary function(s). User localization forms one of the cross-section functions within the Service Stratum and may obtain positioning information on the one hand from the Transport Stratum and/or through further available positioning sources, as also shown in figure 5-6. Hybrid positioning can improve the accuracy of the positioning information and the resulting location estimate at the respective current measurement time.

For reference, requirements related to positioning in 3GPP TR 22.889 [i.3] are quoted and commented in Table 5-11.

Table 5-11: Positioning-related requirements in 3GPP TR 22.889 [i.3]

Number in 3GPP TR 22.889 [i.3]	Quoted requirement	Comment
[R-9.4.2-005]	"*The FRMCS System shall be able to handle additional location information from other external sources.*"	Captured in the architecture considerations in clause 5.6.
[R-12.7-001]	"*The FRMCS System shall provide the alternative means than GNSS to obtain the position of the FRMCS Equipment.*"	The architecture considered in clause 5.6 is in capable to use multiple information sources for precise localization.
[R-12.7-002]	"*The positioning information shall provide an accuracy of [TBD] whilst the UE is travelling at a maximum of 500 km/h.*"	Rather a performance related requirement, likely no implication on architecture.

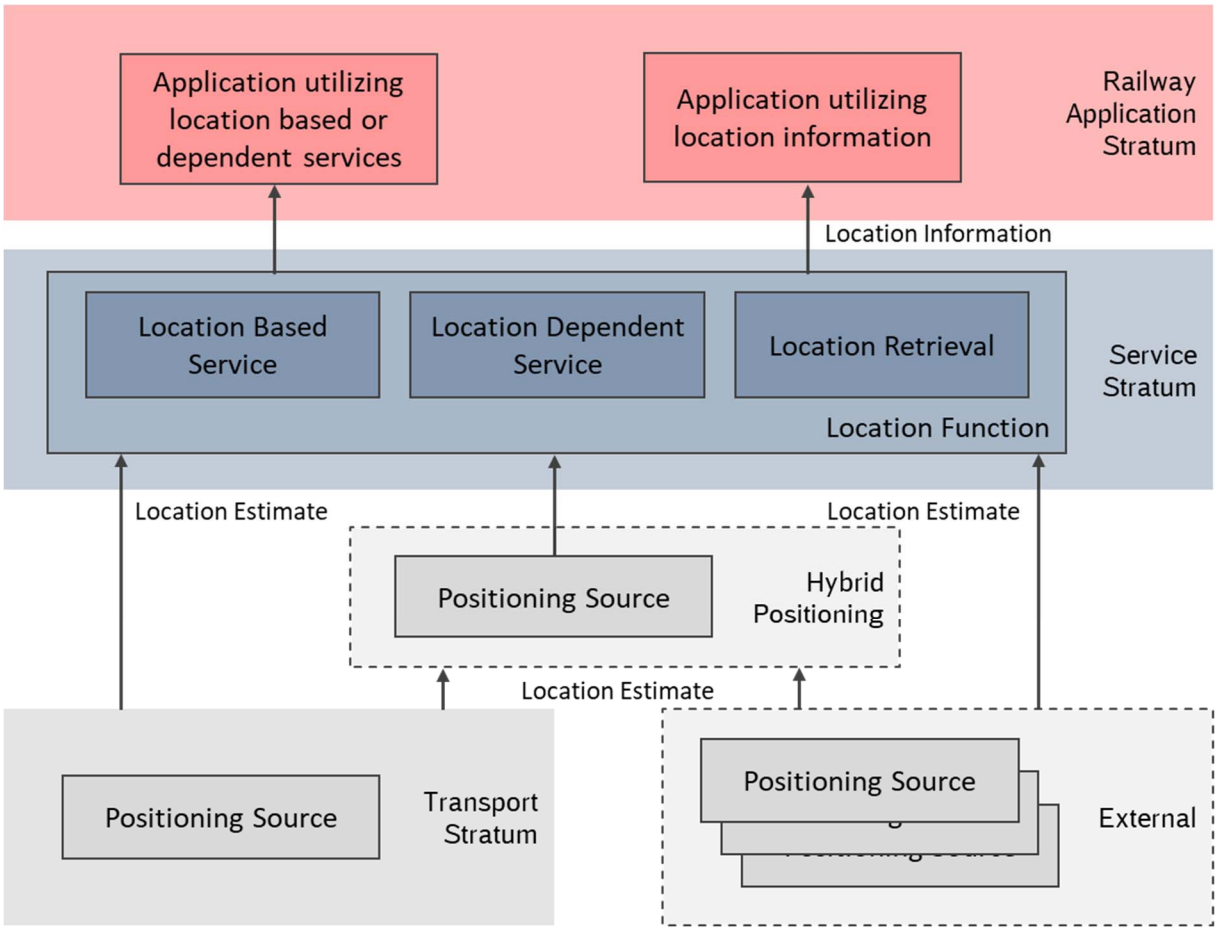

Figure 5-6: Possible forms of obtaining and utilizing location information

The intended use for location estimates is manifold. For instance, some rail applications require inclusion of the current location to allow access to communication, e.g. affiliation to group. Within the location function, which is located in the service stratum, the function subblocks LBS, LDS and the location retrieval are made available accordingly.

5.6.3 Position processing categories

The localization of a user consists of one or more positioning information either available in a central (core) localization management function and/or local (decentralized) on the corresponding device/UE. Hence, the approach differentiates between three categories:

Assisted positioning in which the UE/device provides position measurements for computation on the ground to the corresponding entity on the ground/network.

Device based positioning in which the UE/device performs both position measurements and computation of a location estimate.

Standalone positioning methods in which the UE/device performs position measurements and location computation.

5.6.4 For further study

The following items are for further study:

- Necessary security precautionary measures to prevent knowledgeable changes of a user position information.
- If necessary, protocol developments to enable hybrid positioning.
- Integrity of positioning information.

5.7 Migration from GSM-R to FRMCS

5.7.1 Introduction

In clause 5.7, the implications of the migration from GSM-R to FRMCS (on onboard/handheld and trackside) and those of the expected migration of railway applications (e.g. ETCS onboard unit, RBC) on the FRMCS System architecture are analysed.

5.7.2 Onboard migration

In the UIC Telecom Onboard Architecture (TOBA) group, possible onboard coexistence constellations among GSM-R and FRMCS have been analysed [i.12], in particular considering the interworking with existing installations such as ETCS and cab radio and their expected evolution. For the example of ETCS, the considered migration variants are depicted in figure 5-7, derived from TOBA-7540 [i.12].

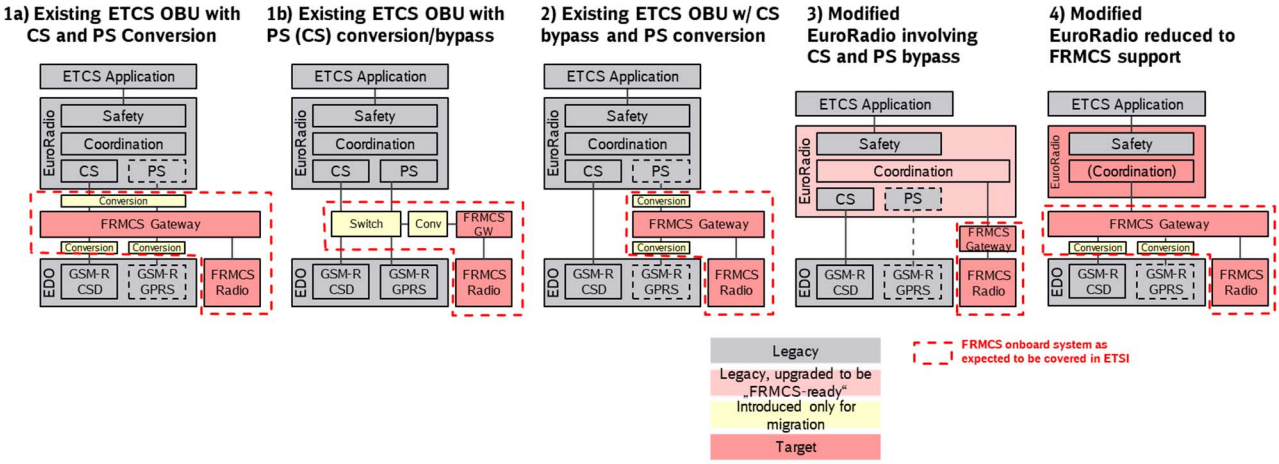

Figure 5-7: Possible onboard technology coexistences of legacy and evolved ETCS and communication functionality (UIC FRMCS TOBA-7540 [i.12])

At the time that this technical report is concluded, it appears that various bodies have converged toward TOBA migration variant 3. This is also inline with assumptions in ETSI that:

- Key FRMCS reference points (e.g. that between the applications and the FRMCS Mobile Gateway and that between the FRMCS Mobile Gateway and radio modules) and the functionality within the FRMCS System architecture should not contain any GSM-R-related functionality.
- Any conversion between GSM-R to FRMCS or vice versa should be minimized and placed in separated blocks that can be "discarded" after co-existence between GSM-R and FRMCS.

At this point the following conclusions can be drawn:

1) The future onboard system in the FRMCS context should not consider GSM-R technology.
2) The FRMCS onboard system should provide necessary conversion for legacy functionalities if necessary.

Both aspects are indicated through the red contours in figure 5-7.

5.7.3 ETCS transport modes

ETCS EuroRadio in the context with GSM-R controls and steers the selection, establishment and recovery of the GSM-R bearer. This strong interaction cannot be continued because the ETCS application will share a UE with multiple other applications simultaneously. Hence the EuroRadio protocol needs to be dismantled from such interaction. Today, an RBC consists of an actual RBC function and the transport like ISDN or IP based.

With FRMCS, the circuit switched based transport will discontinue and therefore the RBC function could be also virtualized and the infrastructure (HW and SW of the operating system, transport and assuming the Internet Protocol as common service) can be considered as a given service (infrastructure as a service). With this in mind, it can be assumed that an RBC in the future remains as a function, hence there is no dependency on the underlying transport.

Current RBC implementations using circuit switched transport will discontinue latest after GSM-R - FRMCS co-existence (no requirement in 3GPP TR 22.889 [i.3]). Also, the FRMCS service stratum will not provide adaptation for a circuit switched approach. This is indicated in figure 5-8, where it can be seen that connectivity for ETCS using an FRMCS Service and Transport Stratum has to be packet-switched.

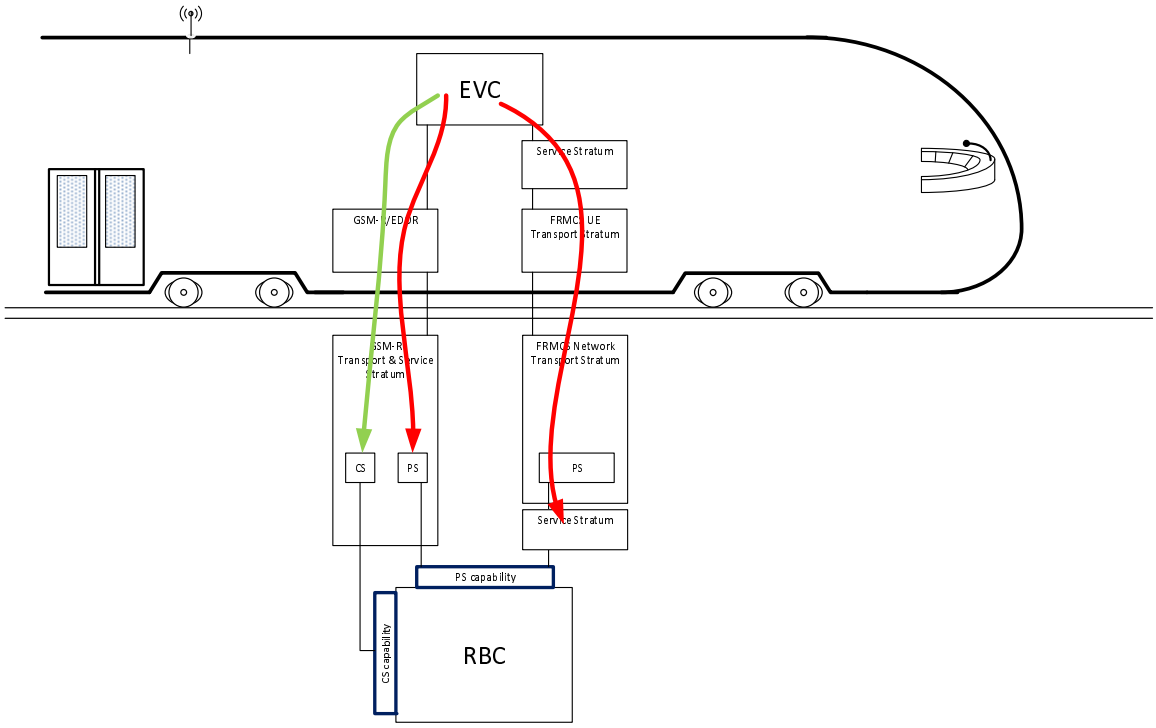

Figure 5-8: ETCS Transport Modes

Please note that a similar approach as shown in figure 5-8 can be used for CTCS due to the fact, that CTCS-3 is equivalent to the European ETCS Level-2.

5.7.4 GSM-R/FRMCS communication service migration at deployment boundaries

At the deployment boundaries of FRMCS system and GSM-R system, service migration should be ensured, to the extent required in 3GPP TR 22.889 [i.3].

The FRMCS (on-board) system should as far as possible be developed independently of GSM-R. Thus, in this context, the service migration functionality should be part of the Application Stratum and not part of the FRMCS Service Stratum, as also depicted in figure 5-9.

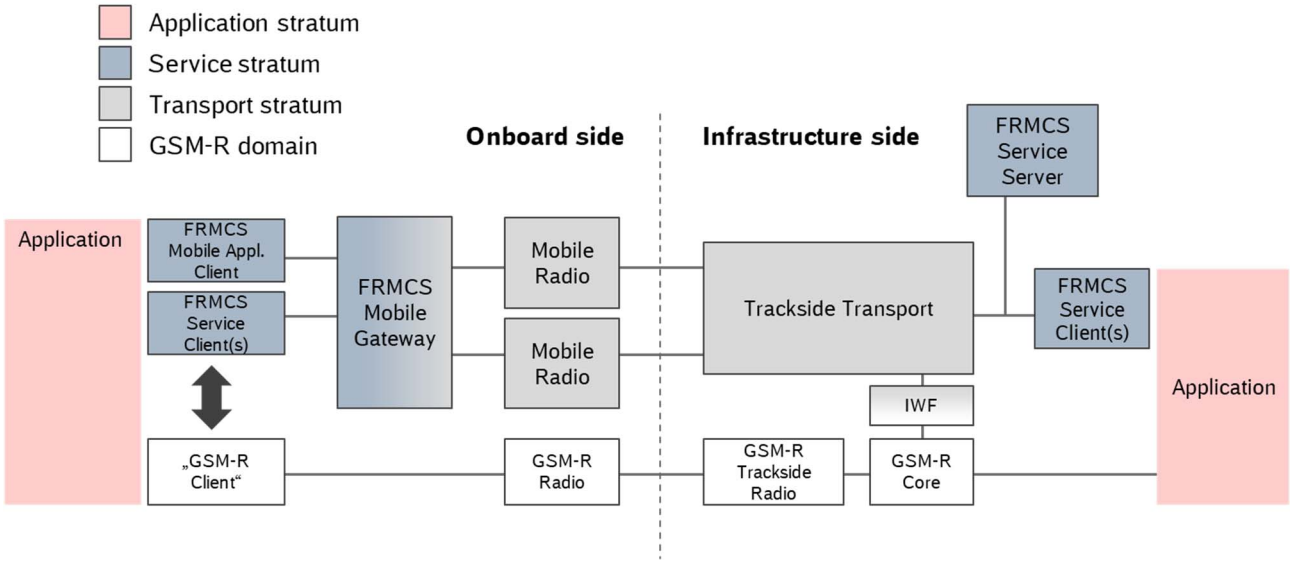

Figure 5-9: Service migration between FRMCS and GSM-R controlled by the Application Stratum

5.7.5 Implications on the FRMCS system architecture

In summary, the identified implications on the FRMCS System architecture are:

- GSM-R system is excluded from the FRMCS System.
- The FRMCS onboard system should provide necessary protocol conversion to interface legacy equipment (depending on the outcome of the migration considerations in EUG and UIC FRMCS TOBA).
- The FRMCS trackside system need not be able to interface to legacy circuit- or packet-switched RBCs.
- Service migration between FRMCS and GSM-R should be controlled by the Application Stratum.

6 FRMCS logical architecture

6.1 System boundaries and high-level logical architecture

The FRMCS system boundaries and high-level logical architecture are depicted in figure 6-1.

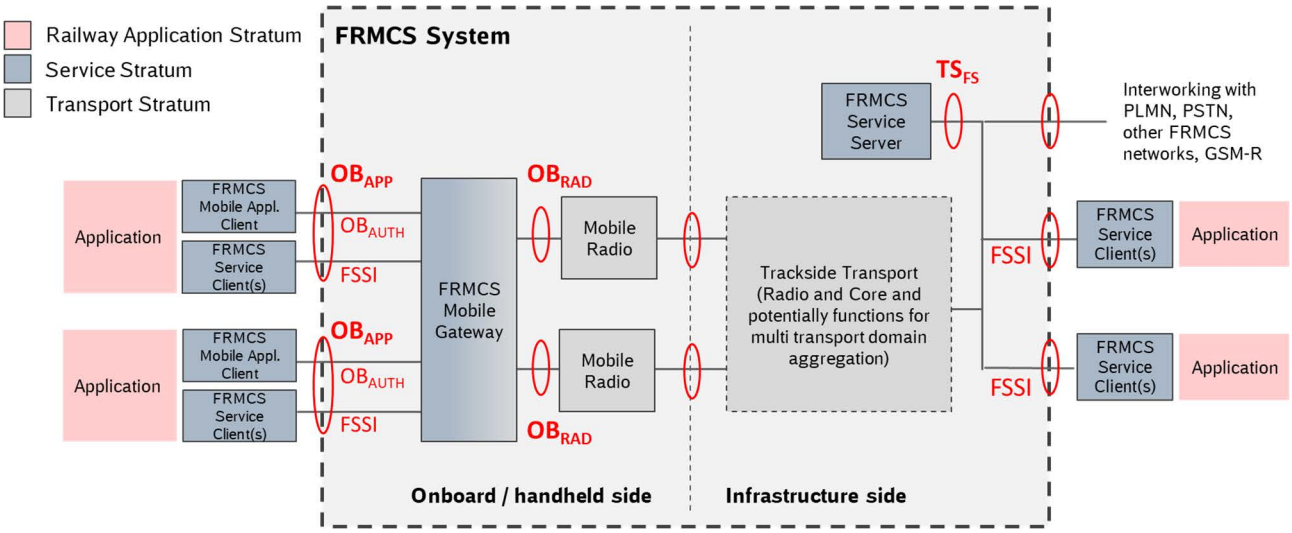

Figure 6-1: FRMCS system boundaries and high-level logical architecture

Through the color-coding, figure 6-1 indicates which of the entities relate to the Railway Application Stratum, Service Stratum and Transport Stratum, as introduced in clause 4. The different entities depicted in the figure are explained in clause 6.2.

It should be noted that the left side of the FRMCS System in the figure (labelled as "onboard/handheld side") depicts the common logical architecture for both onboard systems and handheld devices. Naturally, a handheld device may contain a reduced number of Railway Applications and Mobile Radio entities, but it is expected to follow the same logical architecture as an onboard FRMCS system. An example of a possible physical implementation of the FRMCS architecture for a handheld device is given in clause 8.4.

In figure 6-1, the trackside radio and core entities, plus potential additional functions required for the aggregation of multiple trackside transport domains, are all consolidated into one abstract block "Trackside Transport", as its exact composition of trackside radio elements and core elements depends on the exact deployment scenario and technical realization of the system, as detailed in clause 7 and clause 8, respectively.

The entity "Mobile Radio" as shown in the figure and used throughout the TR may support multiple radio access technologies (e.g. 3GPP or non-3GPP or both), but corresponds to a single User Equipment.

NOTE: Whether some information should be made available to the FRMCS Mobile Gateway on the existence of the radio technologies supported by one Mobile Radio is FFS.

A common understanding is that in cases where multiple transport domains are available (e.g. multiple Mobile Radios and/or multiple Trackside Transport domains), the decision of which transport domain to use for which Railway Application should be handled by the trackside infrastructure to the extent that is possible. The FRMCS Mobile Gateway covers mainly Service Stratum (likely OSI layers 5 and above) aspects and necessary exposure of applicable functions related to entities redundancy, mapping of applications to the applicable the transport domain etc. Transport Stratum related functionalities in the FRMCS Mobile Gateway should be minimized, to follow the transport evolution without impacting the onboard/handheld communication system.

It should be noted that the FRMCS Mobile Application Client and FRMCS Service Clients may be physically co-implemented with the FRMCS Mobile Gateway, as further elaborated in clause 8.4.

6.2 Description of main logical entities

6.2.1 FRMCS Mobile Application Client and FRMCS Service Client

6.2.1.1 Introduction

It is expected that each Railway Application contains or is otherwise represented through one instance of an FRMCS Application Client, which logically interfaces to the FRMCS Mobile Gateway (through a reference point coined as OB_{AUTH}). This application client enables authorization to the FRMCS Mobile Gateway (as first mandatory step to use the FRMCS System). In addition, there is one instance of an FRMCS Service Client for each tuple of FRMCS User, application and service type (e.g. critical data, critical voice, critical video), which logically interfaces to the FRMCS Server on the trackside (coined as reference point FSSI - *FRMCS Service Session Interface*).

The stated clients and mentioned reference points are illustrated for an example application setup in figure 6-2: Here, it is assumed that one FRMCS User (e.g. a human) utilizes two applications in parallel, e.g. an emergency call application and a messaging application. It is further assumed that the onboard system has two Mobile Radio units, i.e. two UEs. In this case, both applications would contain an instance of an FRMCS Mobile Application Client that authorizes the application to the FRMCS Mobile Gateway In addition, the emergency call application (assuming this needs critical data and critical voice) contains one instance of an FRMCS Service Client for the tuple of {FRMCS User, application and service type "critical data"}, and one instance for the tuple of {FRMCS User, application and service type "critical voice"}. The messaging application has an instance of FRMCS Service Client related to this user, application and service type "critical data").

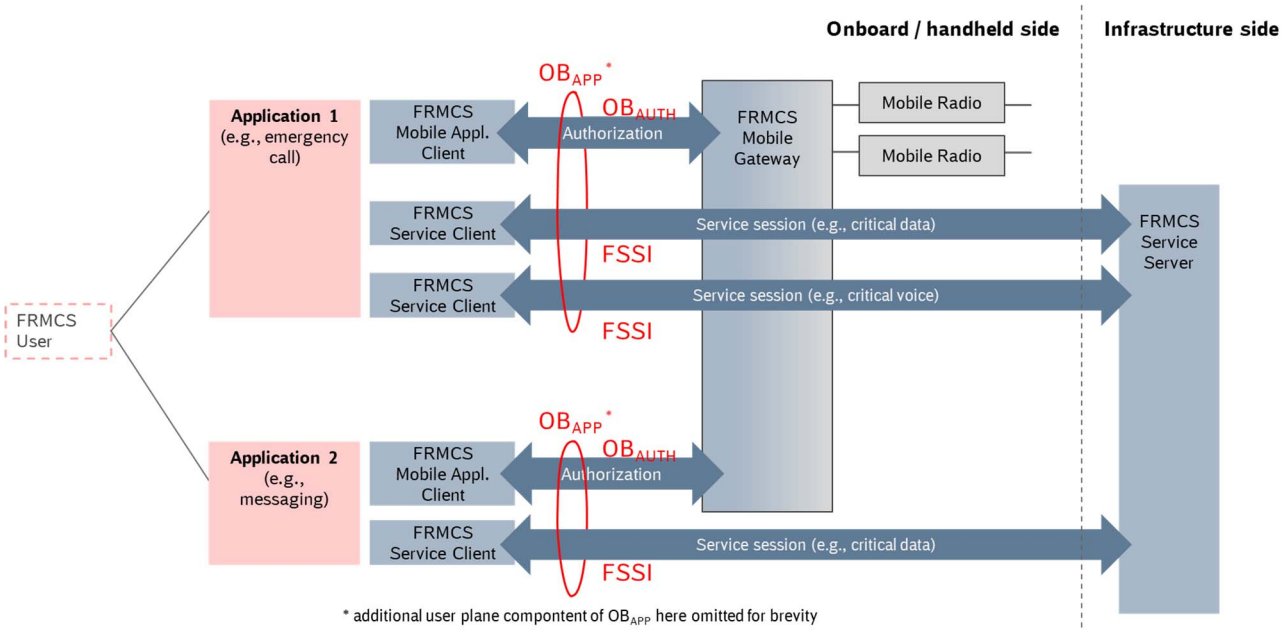

Figure 6-2: Illustration of FRMCS Mobile Application and Service Clients for a specific application example

NOTE: The mapping of an FRMCS User (e.g. a human) to an FRMCS ID in the FRMCS System will be addressed in the normative FRMCS work.

It should be noted that:

- The service sessions established between FRMCS Service Clients and the FRMCS Service Server are transparent to the FRMCS Mobile Gateway.
- The FRMCS Mobile Gateway, however, takes decisions on how to route the user plane, i.e. how to map PDU sessions to different Mobile Radio units, if these are available. This routing of PDU sessions is transparent to the FRMCS Service Clients and to the FRMCS Mobile Application Clients.
- As detailed further in clause 6.3, it is expected that the FSSI reference point will be realized through standard MC protocols (e.g. Gm and GC1 interfaces as specified in 3GPP), while reference point OB_{AUTH} may have to be rail specific.

It is expected that the clients cover the functionality described in the following clauses.

6.2.1.2 FRMCS Mobile Application Client

It is expected that the FRMCS Mobile Application Client covers at least the following functions:

- Establishes connection to FRMCS Mobile Gateway to authenticate the represented application to the gateway.
- Upon successful authentication, it is able to receive information from the FRMCS Mobile Gateway on the FRMCS Service Server(s) that should be used for this application.
- Based on this information it initiates or otherwise triggers FRMCS Service Client(s) to start setting up (or re-establishing) service sessions to right FRMCS Service Server(s).
- Upon termination/power down of an application, it triggers the FRMCS Service Client(s) to terminate their respective service sessions and deregisters the represented application from the FRMCS Mobile Gateway.

6.2.1.3 FRMCS Service Client

An FRMCS Service Client should provide at least the following **mandatory** functionalities:

- Enables service-level registration and de-registration (incl. authentication and authorization) within the service stratum, i.e. towards the FRMCS Server.
- Enables service-level session establishment/termination, e.g. with the FRMCS Server.
- Functionality related to role-based identification (e.g. functional aliasing in 3GPP).
- It informs the application whenever the FRMCS system cannot provide the connectivity expected by the application.

Depending on the needs of the associated application, an FRMCS Service Client provides at least the following **conditionally mandatory** functionality:

- Any functionality related to, e.g. location provision, group communication related services, communication recording, etc.

6.2.2 FRMCS Mobile Gateway

The FRMCS Mobile Gateway is assumed to provide at least the following functions:

General functions:

- Provides mechanisms to authorize applications (represented through FRMCS Mobile Application Clients) located in the application stratum.
- Monitors the operation of Mobile Radio unit(s) and takes actions if these are down or service is otherwise interrupted.
- May provide connectivity among onboard/handheld applications (note that this point is FFS).
- May provide O&M functionality (it is FFS whether this is to be specified by ETSI).

Functions specifically related to the handling of multiple Mobile Radio units:

- Provides mechanisms to determine a default Mobile Radio unit for a specific application (and possibly for a specific target functional alias) in cases where this cannot be done from trackside - FFS.
- Provides mechanisms for transport resource management in case multiple Mobile Radio units are used and where this cannot be done from trackside. For instance (see details in clause 8.3.2):
  - If a Multi-Access Management Services (MAMS) approach is used, the FRMCS Mobile Gateway covers Client Multi-Path Data Proxy (C-MADP) and Client Connection Manager (CCM) functionality.
  - If an emulated Access Traffic Steering, Switching & Splitting (ATSSS) approach is used, the FRMCS Mobile Gateway covers the functionality of an MPTCP client and ATSSS low-layer functionality (ATSSS-LL).

Functions specifically related to border-crossing scenarios:

- Anticipates border crossing and informs registered FRMCS Mobile Application Clients about new FRMCS Service Server to be used (aka service exposure function).

6.2.3 Mobile Radio

A Mobile Radio unit covers the functionality of a UE according to 3GPP definitions, though it may provide 3GPP and/or non-3GPP access (see definitions of "UE" and "Mobile Radio" in clause 3.1).

6.2.4 Trackside Transport

The Trackside Transport unit covers 3GPP radio and core network functionality as defined in 3GPP TS 23.501 [i.5]. A variety of implementations is possible, for instance to address the different deployment scenarios described in clause 7, with detailed solutions for instance elaborated in clause 8.3.

In case a trackside deployment has to support the usage of multiple Mobile Radio units on train side and/or integrate multiple Trackside Transport domains, the Trackside Transport also has to cover the following functionality (see clause 8.3 for details):

- If an (emulated) Access Traffic Steering, Switching & Splitting (ATSSS) approach is used, the Trackside Transport has to also cover MPTCP proxy functionality.
- If a Multi-Access Management Services (MAMS) is approached, the Trackside Transport also has to cover Network Multi Access Data Proxy (N-MADP) and Network Connection Manager (NCM) functionality.

6.2.5 FRMCS Service Server

For the FRMCS Service Server as part of the service stratum following applies:

- Provides the endpoint of service level sessions with FRMCS Service Clients.
- Provides transmission reception control, user profiles, location management, autorization, etc.
- Provides interworking to legacy systems, i.e. GSM-R, and interconnection between service domains.

6.3 Key reference points to be specified

6.3.1 OB_{APP}

OB_{APP} is the reference point between an onboard or handheld application and the FRMCS Mobile Gateway. It is composed of the reference points described in the following.

OB_{AUTH}

The OB_{AUTH} reference point allows FRMCS Mobile Application Clients (representing Railway Applications) to authenticate themselves to an FRMCS Mobile Gateway. In response to this authentication, and whenever this is needed in, e.g. the context of border crossing, an FRMCS Mobile Gateway also uses this reference point to inform FRMCS Mobile application Clients about the FRMCS Service Server to be used for service sessions.

FSSI

The FRMCS Service Session Interface (FSSI) is expected to correspond to the 3GPP Gm and GC1 protocols over SIP. More precisely, it is expected to cover at least the following set of functions [i.13]:

- Common functions:
  - Registration and Service Authorization (prior using any MCX services a MC service client has to perform the registration step. During registration the MC service server creates a binding between IMS public identity and the MC service identity. This is applicable for MCPTT, MCDATA, and MCVideo).
  - Configuration Management (allows subscription to and retrieval of UE, Profile, Service and Group configuration documents).
  - Affiliation/Deaffiliation (procedure used by an MC service client to indicate interest in one or more MC service groups).
  - Policing (procedure used to setup and modify unicast MC dedicated bearers).
  - Location (Location management for MC service user is provided by the location management client to the location management server. The location information reporting triggers are based on the location reporting configuration).

- Functional alias Management (Activation, Deactivation, Interrogation, Takeover and management of both Originating and Terminating side).
- Security (Key management, encryption, etc.).

- MCPTT functions:
  - Private call, Call involving functional alias, Driver to Controller call).
  - Group call.
  - Voice handling.
  - Pre-emption.
- MCDATA functions:
  - IP connectivity (provides a means to exchange of IP Data between MCData clients).
- MCVIDEO functions:
  - Video Pull.

6.3.2 OB_{RAD}

OB_{RAD} is the reference point between the FRMCS Mobile Gateway and Mobile Radio Units.

It is expected to reflect the standard user plane interface between a 3GPP UE and an application.

NOTE: Whether other interfaces to non-3GPP UEs may be supported is FFS during the normative FRMCS work.

For the FRMCS Mobile Gateway to be able to monitor the behaviour of a Mobile Radio, it is further expected that the reference point may convey radio status information such as unsolicited result codes according to 3GPP TS 27.007 [i.14].

6.3.3 TS_{FS}

TS_{FS} is the reference point between the Trackside Radio and Core and the FRMCS Service Server.

It is expected to correspond to the 3GPP N5 and N6 interfaces.

7 FRMCS deployment and border crossing scenarios

7.1 General

The basic FRMCS system architecture is expected to support the deployment and border crossing scenarios detailed in the following clauses. The following assumptions apply:

- Multiple independent transport domains are assumed to be 3GPP technologies (i.e. 4G, 5G) or non-3GPP technologies (e.g. Wi-Fi, satellite), following requirement R-12.9-008 in 3GPP TR 22.889 [i.3].
- The FRMCS system architecture applies in principle to any number of transport domains used.

7.2 Scenario 1a: Multiple trackside access domains with a common core network

In this scenario, depicted in figure 7-1, the following is assumed:

- Multiple trackside access domains are aggregated in one transport domain operated by the same entity (e.g. a railway infrastructure manager).
- A common service domain and application domain is used.

For this scenario, the following applies for the transport stratum:

- A common core is used for the multiple access domains; transport management (incl. priority handling) is handled by a common core.

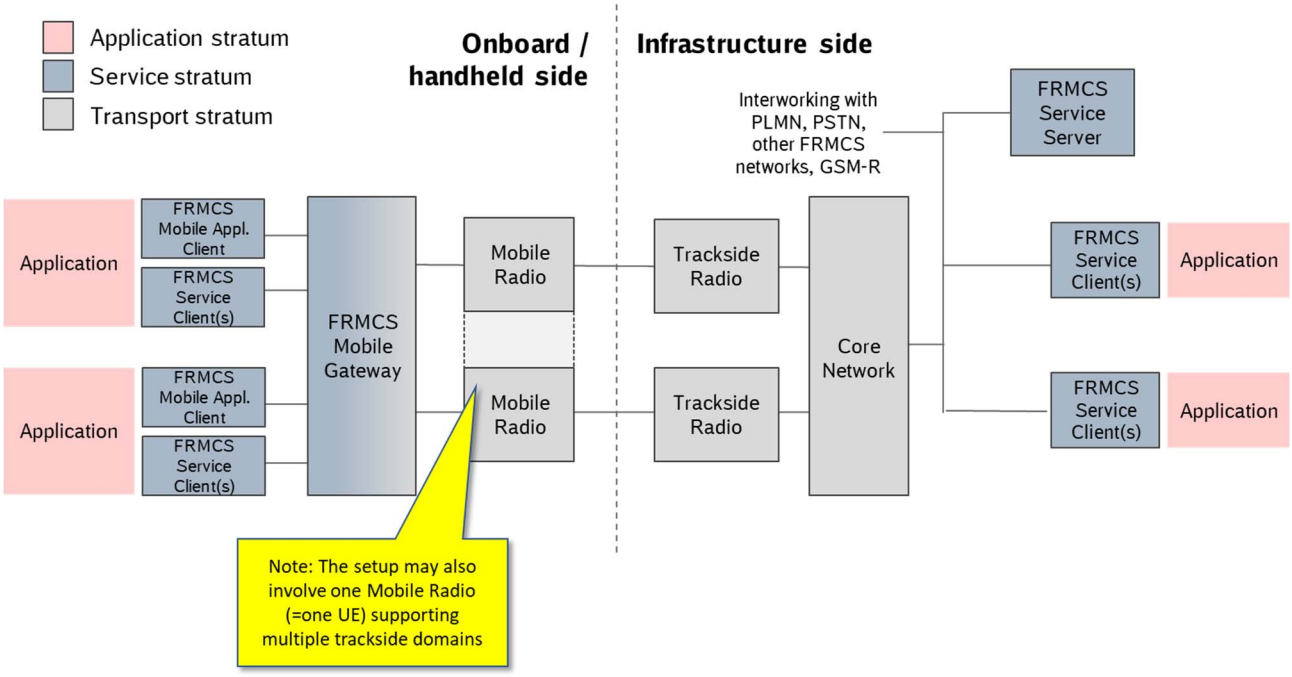

Figure 7-1: Deployment scenario 1a

7.3 Scenario 1b: Multiple trackside access domains under a common core network (infrastructure sharing)

This scenario, depicted in figure 7-2, is based on the following assumptions:

- Multiple access domains aggregated in one transport domain are operated by different entities (e.g. operated by a railway infrastructure manager and others, e.g. Public Mobile Network Operator.
- A setup with multiple core networks (comparable to a multi-operator core network or MOCN approach) is assumed where the radio access of the "other" entity is linked to both, the core of the "other" entity and the core of the rail infrastructure manager.
- A common service domain and application domain is used.

In this scenario the following applies for the transport stratum:

- There are two independent core entities, operated by the railway infrastructure manager and by "other" entity, respectively. While the infrastructure manager operated core network would be a 3GPP core network, the one operated by the "other" entity need not necessarily be a 3GPP core network.

NOTE: The core network operated by the "other" entity would in this case not be considered part of the FRMCS System.

- Same as in scenario 1a, transport domain management (incl. priority) is handled by the core network operated by the railway infrastructure manager.

It should be noted that the depicted deployment could also be operated in various other ways, e.g. the common core network aggregating the two access domains could also be operated by the "other" entity, or the exact split between what is operated by whom could be different. These are, however, seen as different implementation and operation variants which do not have any impact on the FRMCS system architecture.

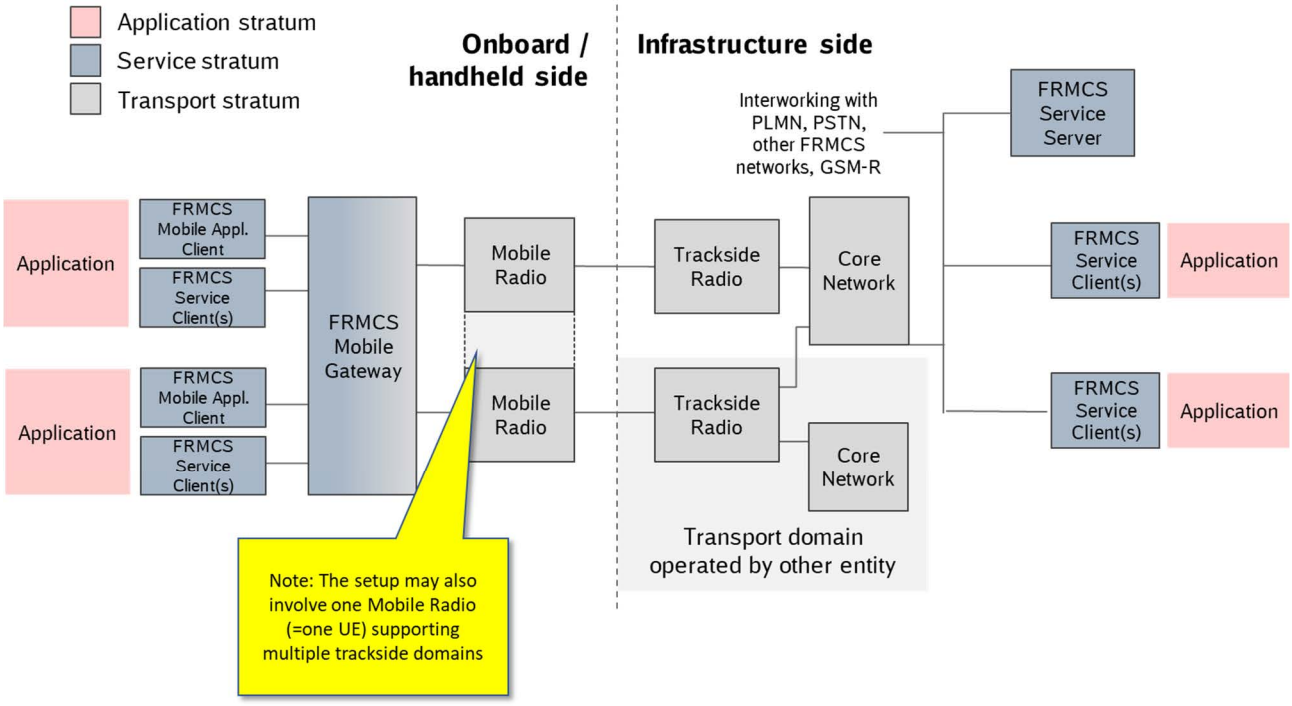

Figure 7-2: Deployment scenario 1b

The particular numbering of the scenarios 1a and 1b is chosen, because the two scenarios are equivalent in terms of the interfaces from the transport domain to the Service Stratum.

7.4 Scenario 2: Interconnected Trackside Transport domains with separate core networks

This scenario, depicted in figure 7-3, covers the following case:

- One Trackside Transport domain, e.g. operated by a railway infrastructure manager, is complemented by a transport domain operated by others.
- The core entities of the two Trackside Transport domains are interconnected.

NOTE: It is FFS how the initial session setup is handled (e.g. whether the FRMCS Mobile Gateway would have to take the initial decision which transport to use). It is further FFS whether both core networks would need a connection to the FRMCS Service Server, see also related discussion in the previous clauses.

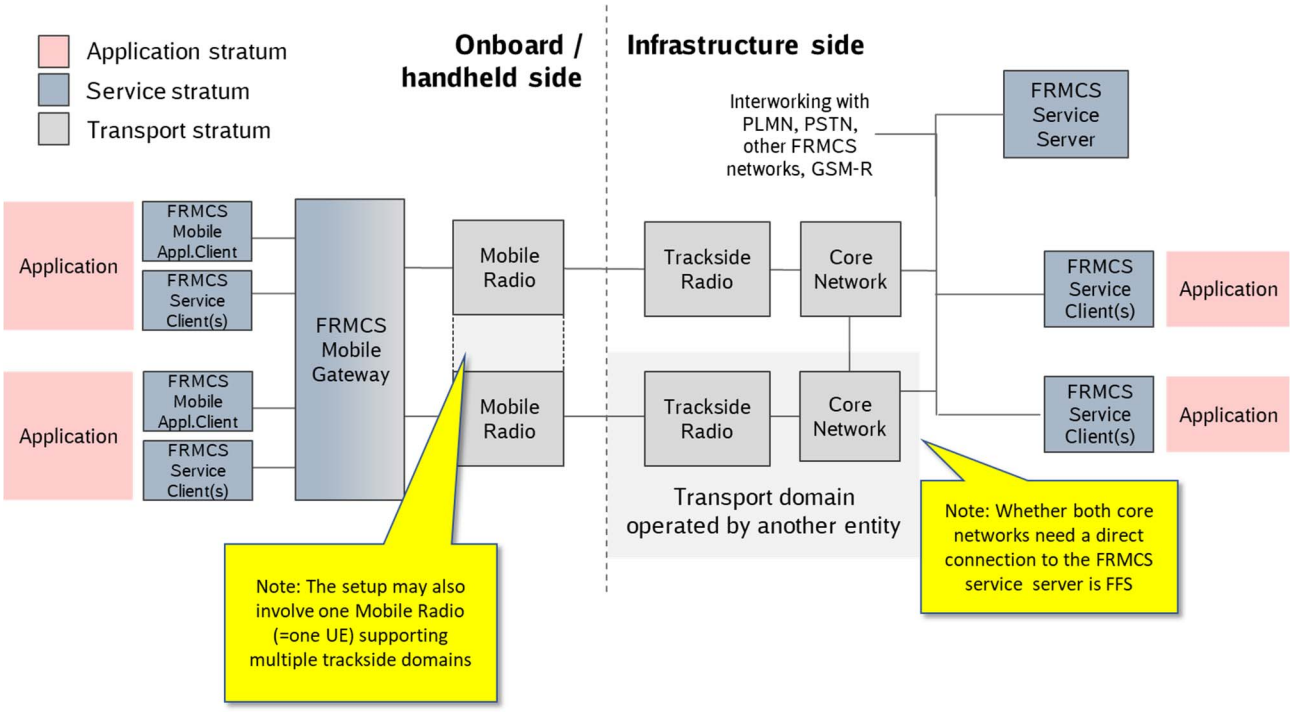

Figure 7-3: Deployment scenario 2

7.5 Scenario 3: Isolated transport and service domains

This scenario, depicted in figure 7-4, covers the following setup:

- One transport domain, e.g. operated by a railway infrastructure manager, is complemented by a transport domain operated by others.
- The service domains are isolated, and no service domain interconnection/interworking is present.
- The application domains are isolated and provided also by others (e.g. for applications that strictly always use the complementary transport domain). The rationale for this could be that a particular application, for instance related to asset management, is by default always handled over the same transport and application domain provided by another party.

For this scenario, the following applies:

- Permanent mapping between onboard/handheld applications service domain and the corresponding transport domain.

It should be noted that the two FRMCS Mobile Gateway instances may still be implemented in the same physical entity.

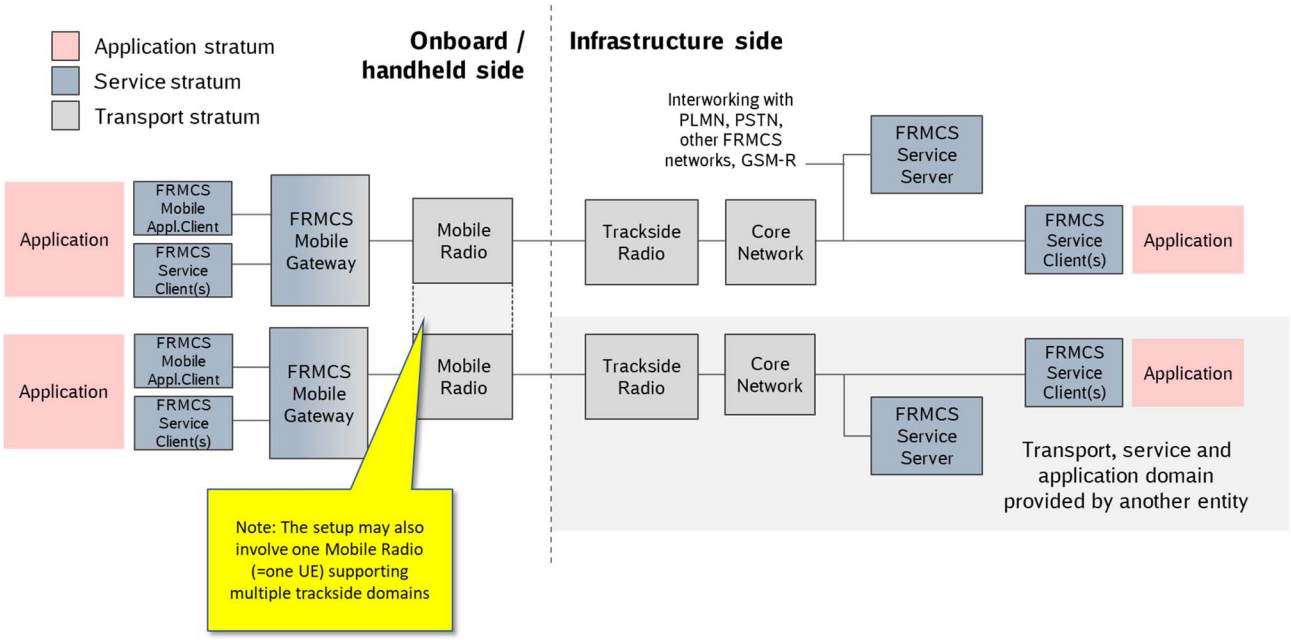

Figure 7-4: Deployment scenario 3

7.6 Scenario 4: Border-crossing scenarios

7.6.1 General

The following scenarios 4a-4c all refer to border crossing scenarios (referring to national borders or boundaries between regions within a country). As illustrated in figure 7-5, the difference among the scenarios is that:

- In scenario 4a, there are different application, service and transport domains on both sides of the border.
- In scenario 4b, there is a common application domain across the border, but service and transport domains are different.
- In scenario 4c, only the transport domains are different on both sides of the border, while the application and service domains are the same.

Other scenarios that would be thinkable (e.g. common service stratum across the border but different application domains) are omitted here, as the technical solutions to address these would either be straightforward or the same as for the scenarios defined here. It should also be noted that the deployment scenario applicable to a train crossing a border may obviously be application-specific, i.e. for some Railway Application the application and/or service domain may change, while for another Railway Application it may not.

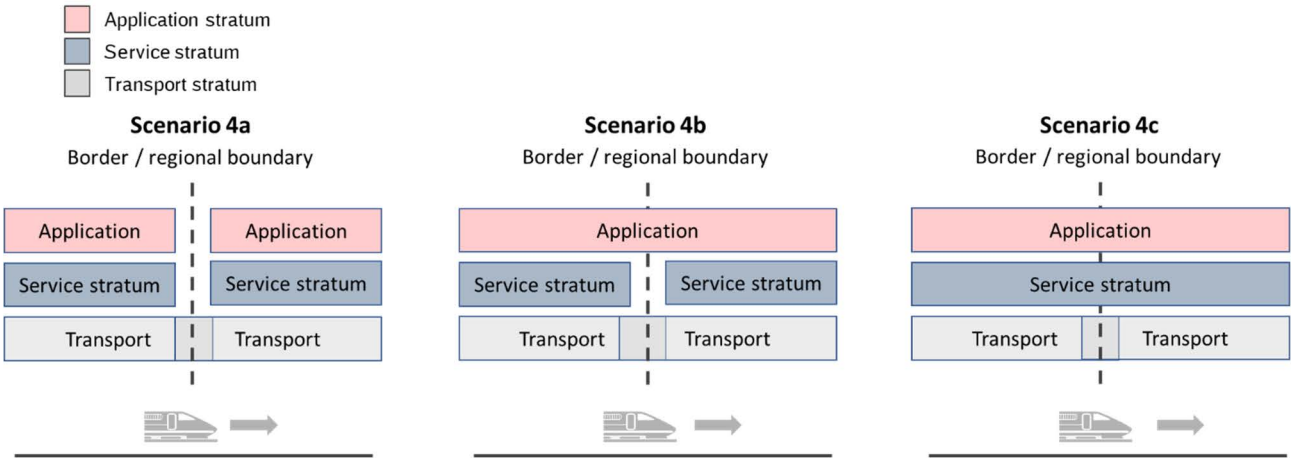

Figure 7-5: Illustration of the considered border-crossing scenarios

7.6.2 Scenario 4a: Border-crossing scenario (isolated application domains)

This scenario, as depicted in figure 7-6, addresses the following setup:

- Transport domain, service domain and application domain are operated by different entities (e.g. railway infrastructure managers).
- Interconnections between the transport domains and the corresponding service domains are in place (though it is FFS to which extent these are needed).

NOTE: This scenario excludes the interworking with legacy systems, i.e. GSM-R.

- Service domain and the application domain (server, e.g. ETCS trackside) are isolated under current assumptions.

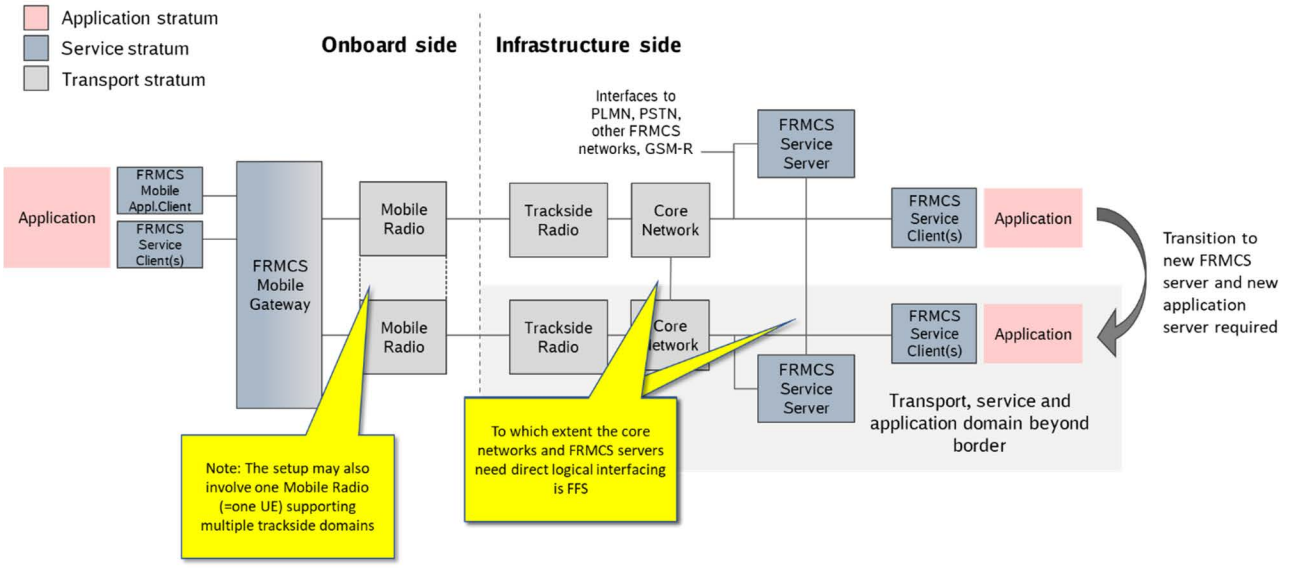

Figure 7-6: Deployment/border crossing scenario 4a

For this scenario, the following premises apply:

- Application-level "handover", service-level "handover" and transport-level "handover" should be decoupled.
- At least for critical applications always the FRMCS Service Server of the visited country should be used (for QoS management purposes) - it is FFS whether this should be mandated for all applications.

- Dual registration is supported from an architectural perspective (e.g. for make-before-break purposes), but it is FFS whether and in which cases this should be used.

It is expected that:

- Application-level "handover" is triggered in the Application Stratum. For instance, an ETCS onboard application may be triggered by balise or instructed by the RBC to connect to a new RBC. In this case, the FRMCS Mobile Application Client representing the onboard application should trigger all related FRMCS Service Clients to reestablish connections to the functional identity of the new RBC.

- Service-level "handover" is triggered by the FRMCS Mobile Gateway, which has mechanisms to anticipate an upcoming border crossing (for instance, it may infer from the detection of a particular PLMN ID by one of the onboard UEs that the train is approaching a border). In this case, the FRMCS Mobile Gateway informs all registered FRMCS Mobile Application Clients that a new FRMCS Service Server should be used.

Naturally, the trigger on application-level and that by the FRMCS Mobile Gateway may happen in any chronological order, hence both orders have to be considered. In figure 7-7, the case is shown where the FRMCS Mobile Gateway first anticipates the upcoming border crossing. In this case, it may be an option to skip step 2, i.e. if the FRMCS Mobile Gateway is informed that a new FRMCS Service Server is to be used, it may wait until the application-level trigger occurs before it then triggers the FRMCS Service Clients to setup service sessions with the new (foreign) FRMCS Service Server and to the new application target, hence ensure that application and service transition happen at the same time.

It should be noted that the procedure shown in figure 7-7 is just to be seen as an example; details on this and similar procedures are expected to be captured in the UIC FRMCS SRS.

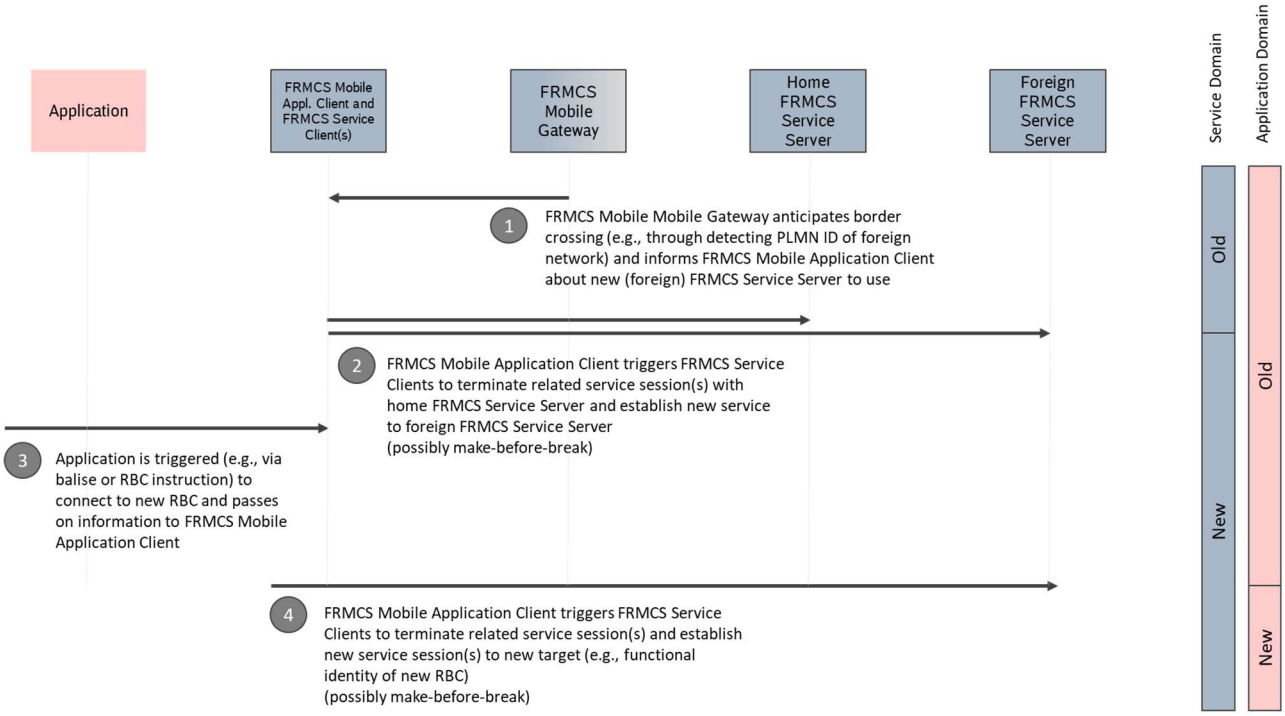

Figure 7-7: Application and service transition at border when trigger from FRMCS Mobile Gateway occurs first

Figure 7-8 now shows the case where the application-level trigger occurs first. In this case, it is likely inevitable that there is a period where the onboard application is already connected to the new application target (e.g. new RBC), but still using the home FRMCS Service Server.

Again it should be noted that the procedure shown in figure 7-8 is just to be seen as an example; details on this and similar procedures are expected to be captured in the UIC FRMCS SRS.

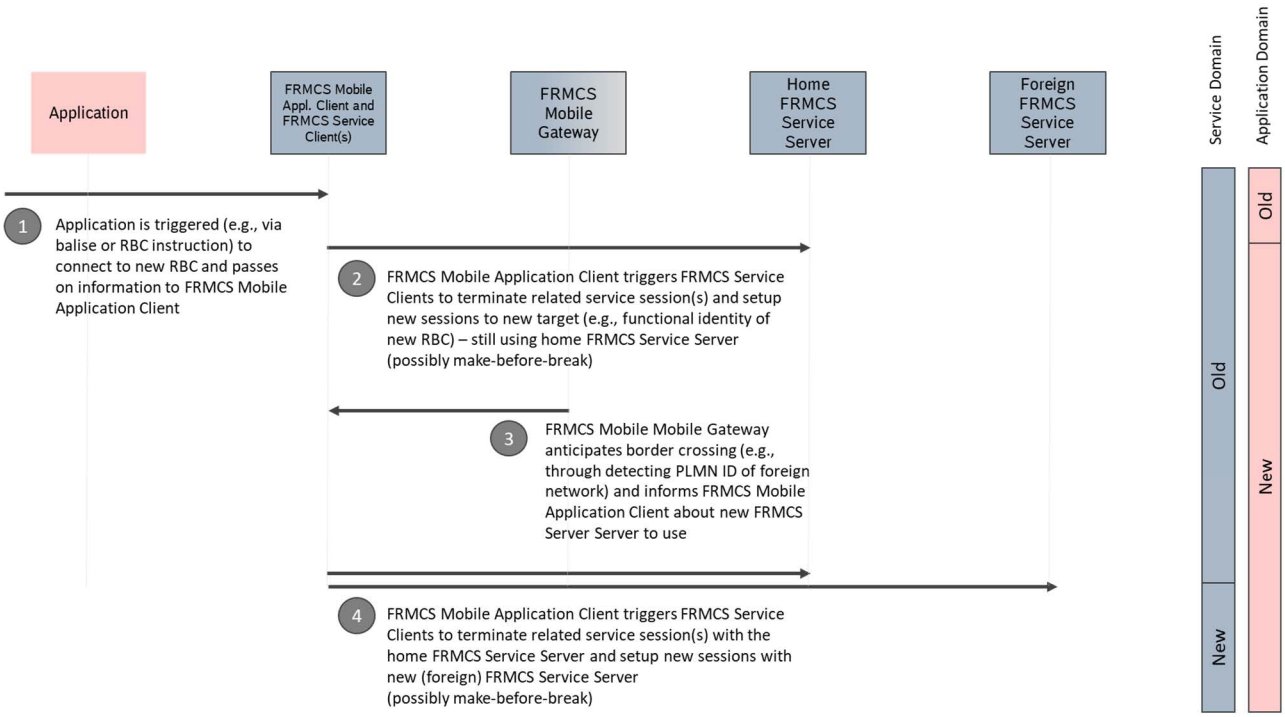

Figure 7-8: Application and service transition at border when trigger from application occurs first

As stated before and clear from the previous figures, it is expected that the transport domain transition is largely independent of the application-level and service-level transition steps and in particular transparent to the Application Stratum. However, some constraints may of course apply (e.g. a certain service session may only use a certain transport network). It is here assumed that the FRMCS Mobile Gateway knows which service sessions can be mapped to which transport network.

It should be noted that a change of application server could also be made transparent to the onboard application by letting this establish service session(s) to a group of functional entities (in the ETCS case, this could be a group of RBCs). In this case, the complexity of the application transition is to some extent moved into the Service and Transport Stratum. This option is FFS.

7.6.3 Scenario 4b: Border-crossing scenario (shared application domain)

This scenario, as depicted in figure 7-9, addresses the following border crossing situation:

- Transport domains and service domain are operated by different entities (e.g. railway infrastructure managers), but the application domain for a specific application stays the same.
- Interconnection between transport domains and the corresponding service domains are in place.

NOTE: This scenario excludes the interworking with legacy systems, i.e. GSM-R.

- The application domain is shared (e.g. ETCS trackside).

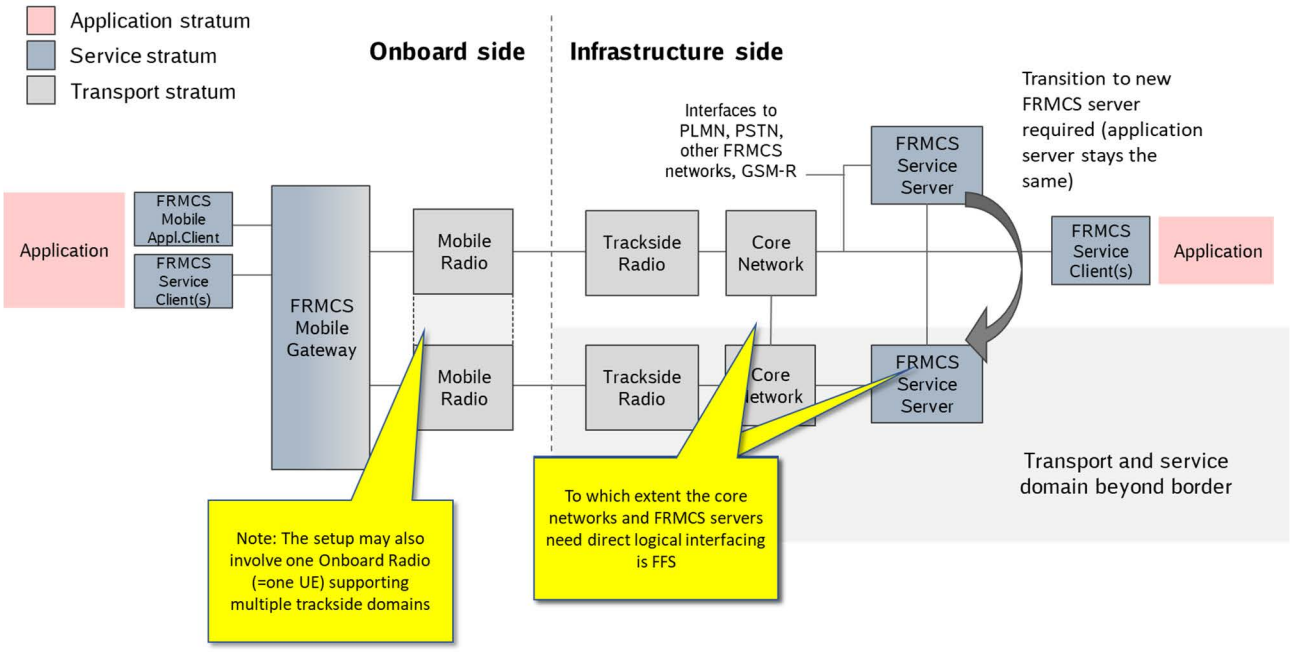

Figure 7-9: Deployment/border crossing scenario 4b

This border crossing scenario can essentially be addressed through a subset of the mechanisms described for the previous scenario. More precisely, it is assumed that the FRMCS Mobile is able to anticipate a border crossing scenario and informs the registered FRMCS Mobile Application Clients accordingly that a new FRMCS Service Server is to be used. These then trigger related FRMCS Service Client(s) to terminate ongoing service sessions and establish service sessions to the new (foreign) FRMCS Service Server, possibly in a make-before-break fashion. Again, it is expected that the transport-level transition is handled largely independent of the service-level transition, though there may be constraints as to which service sessions can use which transport domain, which should be known to the FRMCS Mobile Gateway.

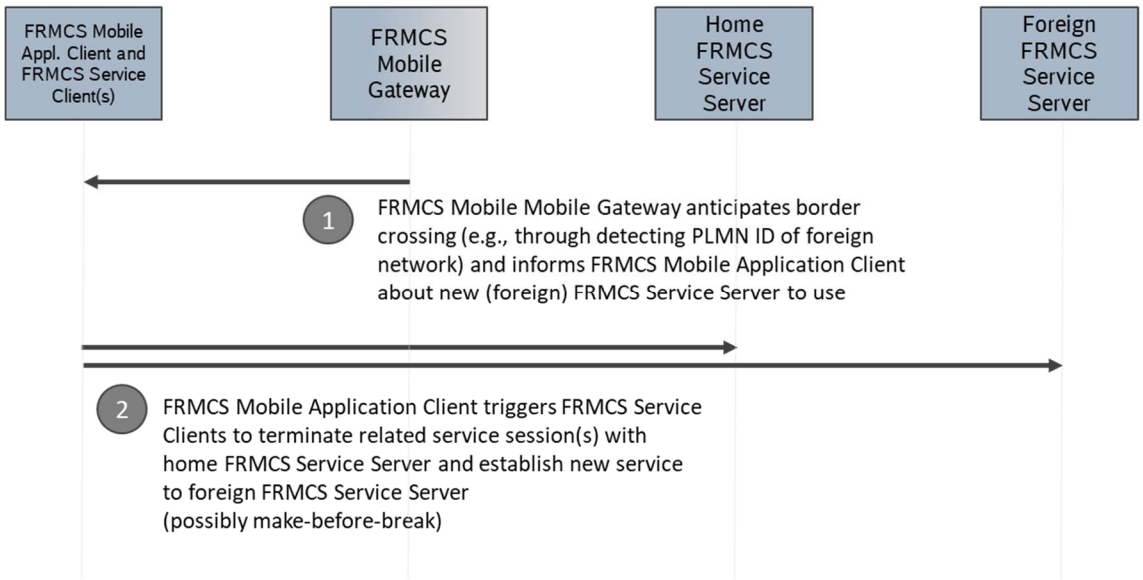

Figure 7-10: Service transition steps in case of border crossing scenario 4b

7.6.4 Scenario 4c: Border-crossing scenario (shared application and service domain)

In this scenario, only the transport domain changes when crossing the border, while the application and service domains stay the same. In principle, the setup may be the same as in deployment scenario 2 depicted in figure 7-3, with the difference that the two transport domains are not utilized permanently, but a one-time transition from one transport domain to the other takes place at the border.

This scenario can in essence be seen as a subset of deployment scenario 2, (with the difference that there is only once a switchover from one to another transport domain instead of a permanent utilization of multiple transport domains), and it is hence not elaborated in further detail here.

8 Possible technical realization of the FRMCS system

8.1 General

Clause 8 elaborates on possible technical realizations of the FRMCS system, with the aim to:

- Investigate which 3GPP building blocks may be mapped to the FRMCS logical architecture depicted before and satisfy the identified deployment scenarios.
- Identify whether the reference points between logical entities in the FRMCS logical architecture may adopt interfaces already standardized in 3GPP or be further standardized.
- Provide an analysis of potential technical solutions for the usage of multiple transport domains by one FRMCS onboard/handheld system.
- Provide clarity on topics that are often prone to misunderstandings (such as the difference between logical and technical architecture in the context of the FRMCS onboard/handheld system).

8.2 Potential 3GPP building blocks and reference points mapped to FRMCS logical architecture

This clause identifies the potential main 3GPP building blocks that may be mapped to the FRMCS logical architecture. This is done following the principle that Transport Stratum, Service Stratum and Application Stratum are decoupled to guarantee the evolution process in the Transport Stratum as well as in the Service Stratum. Furthermore, the goal is to address generic approaches that allow a further evolution of the technical FRMCS system architecture. Hence, possible implementation options are excluded.

In figure 8-1 and figure 8-2, two possible usages of 3GPP building blocks for the technical realization of the FRMCS system are shown, which are shortly described in the following.

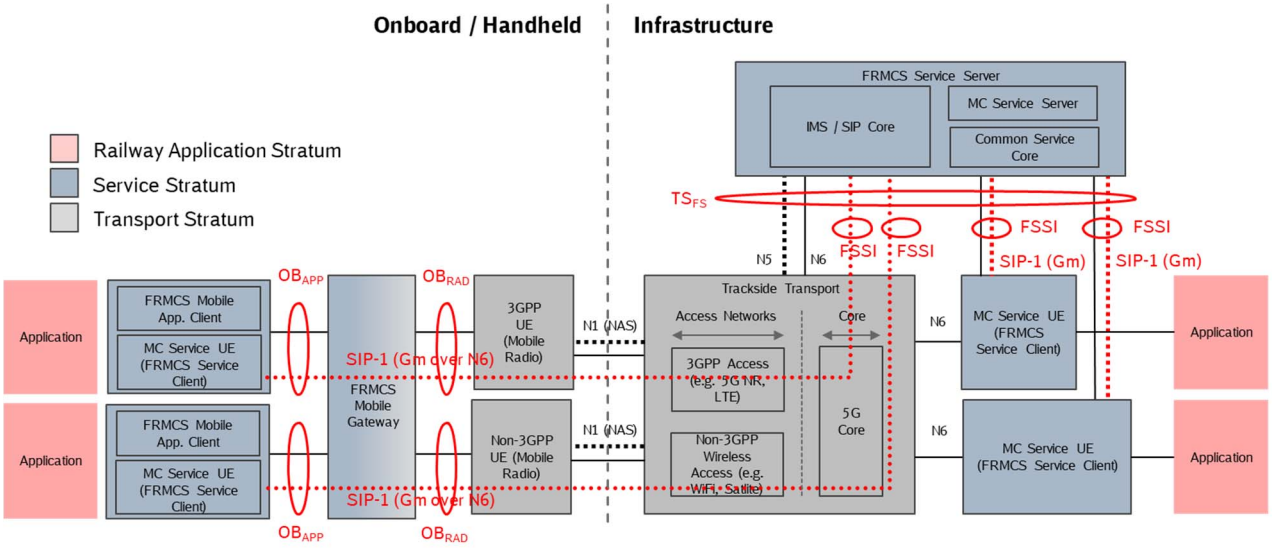

Figure 8-1: Potential technical realization of FRMCS system architecture with independent wireless and wireline transport domains

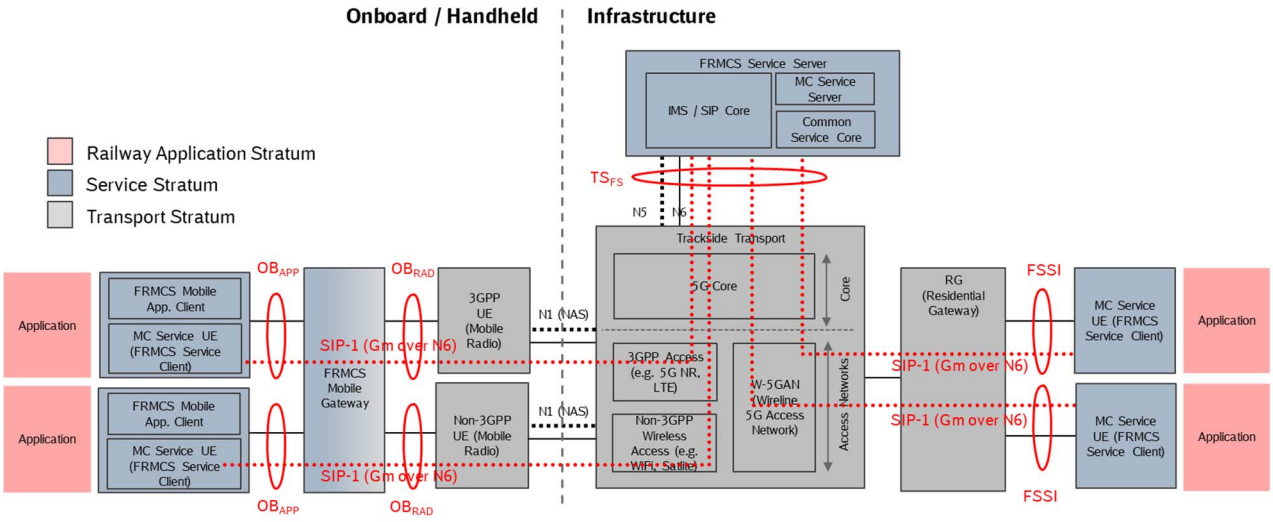

Figure 8-2: Potential technical realization of FRMCS system based on wireless and wireline convergence under a 5G core network

Transport Stratum

As shown in the figures, the global FRMCS approach pursues the decoupling between Railway Application Stratum, Service Stratum and Transport Stratum. The Transport Stratum, which forms the bridge between FRMCS Service Client and FRMCS Service Server in the Service Stratum, should consist of an access-agnostic 5G Core (5GC), Mobile Radio and Access Networks. The 5GC supports the connectivity of the Mobile Radio via 3GPP Access Networks (e.g. 5G NR, LTE) or non-3GPP Access Networks (e.g. WLAN, Satellite). For the connection via 3GPP Access Networks, a 3GPP UE should be use as Mobile Radio. For the connection via non-3GPP Access, a 3GPP UE or non-3GPP UE may be used as Mobile Radio. The use of 3GPP LTE E-UTRA access should be ensured accordingly if this is necessary in the coexistence phase of FRMCS and GSM-R. The Transport Stratum should provide unicast, multicast and, if necessary, broadcast transport options. Multicast and broadcast may require special precautions which should be considered in the normative work.

Furthermore, 5G presents an opportunity for industry to define a flexible and modular architecture allowing network providers to operate and manage a single 5G core network supporting all access types. Beside the wireless access types mentioned above, also a wireline access network can be supported in the 5G architecture, see 3GPP TS 23.501 [i.5]. As shown in figure 8-2, the Residential Gateway (RG) is a device providing communication services to other devices in IM's premises in the infrastructure side. Two types of RGs are defined, namely 5G-RG and FN-RG (Fixed Network Residential Gateway) depending on whether N1 signalling with 5G Core is supported or not [i.5]. The wireline 5G Access Network (W-AGF) will be connected to the 5G Core Network CP and UP functions via N2 and N3 interfaces, respectively. RG is then connected via W-5GAN to the 5G Core. Such convergence of wireline and wireless allows the use of the necessary subscriber credentials and service definitions regardless of whether wireless or wireline access and is ensured for the first time by 3GPP in the 5GS context. In the FRMCS context, it enables the integration of wireline access, formerly FTS, and also enables targeted QoS control in this access segment. Accordingly, FRMCS does not need to differentiate between mobile and FTS users and provide the service more consistently and effectively. A user then mainly differs according to its role and service options. On the other hand, such convergence deployment may introduce more complexity and therefore the cost effectiveness of convergence deployment should be analysed.

Service Stratum

The MC service system in the FRMCS Service Server, including MC Service Server and Common Service Core, provides point-to-point and group communications for voice, video and data. In addition to communication services, it supports various functions, e.g. role-based identification, user authorization, location service, interworking with GSM-R, and functional aliasing, etc. The IMS in the FRMCS Service Server forms the basis for all the functions mentioned, which enables the simultaneous use of various services (voice, video and data) for one user. The users of the Service Stratum should be unambiguously identifiable and may additionally activate and use alternative identification features for operational purposes. The Service stratum may consist of several independent service domains with their own identification, which includes mutual use (roaming) of the service users.

NOTE 1: It is to be concluded in the normative FRMCS work which necessary functions (e.g. role-based identification, user authorization, location service, interworking with GSM-R, and functional aliasing) from the MC framework are to be adopted in the FRMCS System architecture.

NOTE 2: It is FFS whether the media plane always needs to go through the FRMCS Service Server, as this point may be especially problematic for latency-critical applications.

Reference Points

Interfaces or reference points between strata are for the exchange of control plane information. For example, the N5 reference point between 5G Core in Trackside Transport and IMS in FRMCS Service Server is used for policy control (see 3GPP TS 23.280 [i.11]). The same applies to the system entities within a stratum enabling the exchange of control plane information. For example, in the Service Stratum the SIP-1 reference point between MC Service UE and the IMS in the FRMCS Service Server for establishing a session in support of MC service, uses the Gm reference point as defined in ETSI TS 123 002 [i.15]. Moreover, in the Transport Stratum the N1 reference point is used by UE for transmitting non radio signalling (NAS) between UE and AMF in the 5G Core via 3GPP or non-3GPP wireless access.

While the user plane is not covered in detail in figure 8-1 and figure 8-2 and the subsequent descriptions, it should be noted that for latency-critical services, such as those in some cases requiring < 10 ms E2E latency as captured in 3GPP TR 22.889 [i.3], it is important that the user plane can be decentralized and is not required to go through centralized points in the trackside infrastructure. In principle, this could be realized in two ways:

- In the ideal case, the user plane does not have to go through the FRMCS Service Server, but can be handled via decentralized UPFs in the 5G core that are co-located with latency-critical applications (for instance in Edge deployments).
- Alternatively, it may be possible to decentralize related user plane parts of the IMS/SIP Core.

As FRMCS may also be based on 4G, e.g. in non-European regions, Annex A.4 also elaborates on how a functional subset of the an FRMCS system (e.g. possibly not meeting all FRMCS requirements) could also be realized with an EPC.

8.3 Potential solutions for the support of multiple Mobile Radios and/or multiple Trackside Transport domains

8.3.1 Introduction

The motivation of deployment scenario 1 (see figure 7-1 and figure 7-2) and scenario 2 (see figure 7-3) defined in clause 7 is to address various requirements from TOBA-7510 [i.2] and 3GPP TR 22.889 [i.3] listed in clause 5.2 and clause 5.3 through the usage of multiple Mobile Radios and/or multiple Trackside Transport domains. More specifically, the usage of multiple Mobile Radios and/or multiple Trackside Transport domains may be motivated by the need for, e.g.:

- **Bearer flexibility** (see, e.g. requirement R9 in clause 5.2 and R-12.9-001 in clause 5.3): The FRMCS system should be able to operate with different kinds of Trackside Transport domains (railway dedicated or public) sequentially or simultaneously using different transport technologies (e.g. 4G, 5G, Wi-Fi, Satellite, etc.);

NOTE 1: Relocation from one Trackside Transport domain to another may occur during migration, during border crossing, when reselecting from a dedicated Trackside Transport domain to a public operators Trackside Transport domain.

- **Availability, reliability, resilience, and the avoidance of single points of failure** (see, e.g. requirement R4 in clause 5.2 and R-12.22-002 in clause 5.3): For certain applications, especially but not exclusively the critical ones, a high availability, reliability and resilience of the connection to the trackside may be instrumental in establishing redundant nodes (avoiding single points of failures) and/or redundant radio links. The usage of multiple Mobile Radios and/or multiple Trackside Transport domains may here be an important component to addressing the stated KPIs;

- **Capacity** (see, e.g. requirement R12 in clause 5.2): Especially for capacity-demanding communication use cases, it may be needed to aggregate capacity over different transport domains.

In the following, different possible solutions in the Service Stratum and Transport Stratum are compared that could be applied individually or in combination to support multiple Mobile Radios and/or multiple Trackside Transport domains. These are then assessed against the related requirements from TOBA-7510 [i.2] and 3GPP TR 22.889 [i.3].

NOTE 2: No decision has yet been taken on the usage of the following solutions, as most still require further study.

8.3.2 Service-level solution based on the MC framework

The 3GPP MC framework itself provides a solution to support multiple Mobile Radios, i.e. via mechanisms in the Service Stratum. More precisely, the following mechanism uses already available functions from 3GPP TS 23.228 [i.9] by linking Public User Identities (3GPP TS 23.003 [i.10]) by means of virtual identities, called Globally Routable Agent URI (GRUU). A Public User Identity from that of the GRUU set is assigned to the mobile radio. The GRUU set is maintained within the FRMCS server (i.e. IMS). This principle is illustrated in figure 8-3. For further background on identities in general, the reader is also referred to clause 5.4.

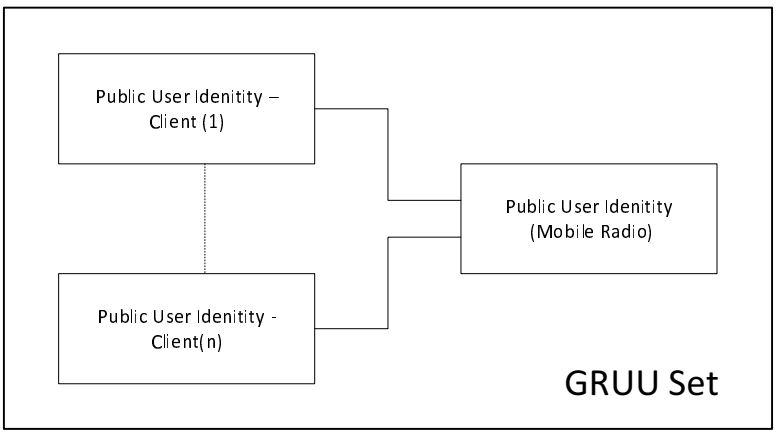

Figure 8-3: Principle of GRUU [i.9]

The client's Public User Identity can be used several times in different GRUU sets. The corresponding priority of the GRUU sets is left to the implementation. The routing of traffic, if multiple Mobile Radios or only one Mobile Radio are considered, is also left open in 3GPP specifications and can be determined by implementation.

It is understood that this approach can be used to support the usage of multiple Mobile Radios as such:

- The FRMCS Mobile Gateway provides functionality (based on CAPIF or similar) to inform registered FRMCS Mobile Application Clients about the GRUU sets associated to Public User Identities that are available to be used (this information may of course be application-specific, i.e. if the Gateway knows that a certain application cannot use a certain UE, it doesn't inform the FRMCS Mobile Application Client about the related GRUU sets associated Public User Identity).

- This information, however, contains only the GRUU sets associated to Public User Identities that can be used, i.e. the FRMCS Mobile Application Client cannot tell from this whether these are related to 5G, Wi-Fi™, etc., or the current connectivity status of the related transport domains.

- Based on this information, the registered FRMCS Mobile Application Clients then instantiate (or retrigger) FRMCS Service Clients (e.g. realized through MC Service Clients) and consequently MC service sessions that are related to all GRUU sets associated to Public User Identities available for the related application.

NOTE: The usage of any of the concepts above will be addressed in the normative FRMCS work.

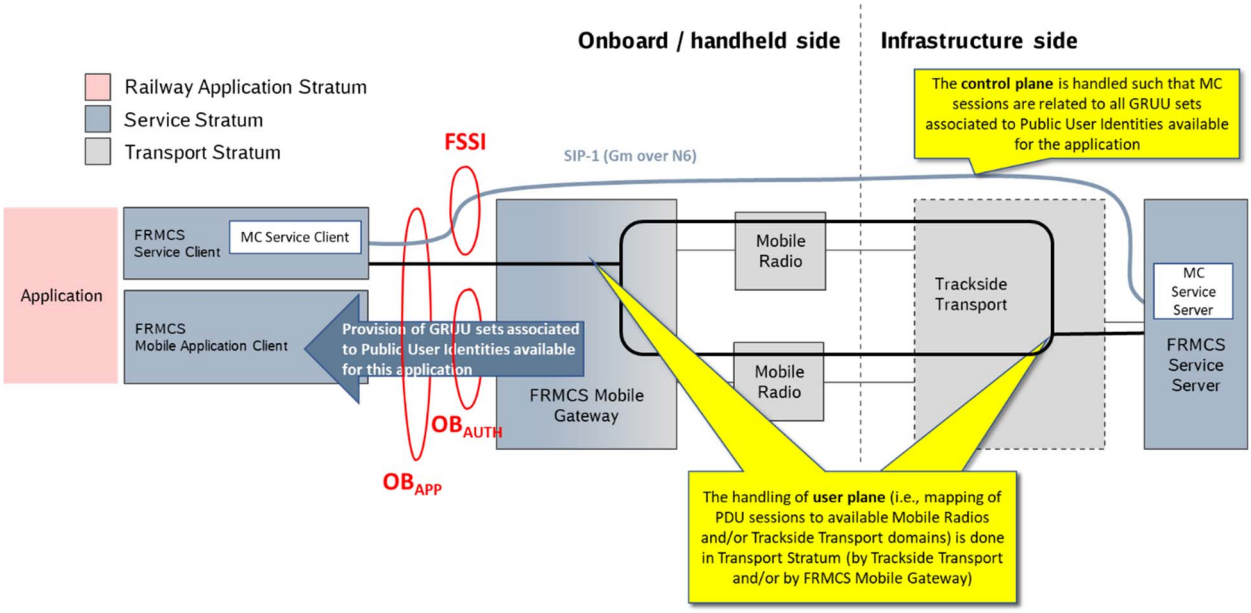

Figure 8-4: Service-level approach to handle multiple UEs on onboard side (and its relation to handling of the user plane in the Transport Stratum)

It has to be noted that the depicted service-level solution allows for the control of multiple Mobile Radios only, while the handling of the user plane (e.g. the functionality to decide which PDU sessions to map to which Mobile Radio or which Trackside Transport domain, etc.) has to be covered by additional mechanisms in the Transport Stratum, more precisely in the FRMCS Mobile Gateway and/or the Trackside Transport, as also shown in figure 8-4.

It has to be further noted that the concepts described in this clause apply if multiple transport networks are integrated under a 5G core.

Solutions in the Transport Stratum that may complement the shown service-level approach are elaborated in the following clauses.

8.3.3 Transport-level solutions: Core-centric integration using ATSSS

In order to ensure seamless connectivity between multiple transport domains, 3GPP has studied in 5G Release 16 a function called ATSSS (Access Traffic Steering, Switching & Splitting) that manages different IP flows over multiple access technologies for a single UE. The integration of multiple radio access types in ATSSS is within a 5G deployment in the transport stratum. More specifically, ATSSS would need a 5G core for allowing to push operators' policies to the UE via a 5G Core.

The three main operations supported by the ATSSS are traffic steering, switching and splitting, see 3GPP TS 24.193 [i.16]. One or more of the two steering functionalities are specified in the standard: MPTCP functionality and ATSSS-LL functionality. Here, MPTCP resembles high-layer steering functionalities operating above the IP layer, while ATSSS-LL functionality is considered as low-layer steering functionalities, operating below the IP layer.

Multiple architecture schemes are specified in 3GPP TS 23.501 [i.5]:

- 3GPP access and non-3GPP access are located in the same PLMN; and
- 3GPP access and non-3GPP access are located in the different PLMNs.

The former approach, shown in figure 8-5, could be applied to deployment scenarios 1a and 1b as defined in clause 7.2 and clause 7.3, respectively. The latter approach, shown in figure 8-6, could be applied to deployment scenario 2 defined in clause 7.4. Note that in both cases, a single UE (Mobile Radio) is registered to the PLMN(s) over 3GPP and non-3GPP accesses. One important condition of ATSSS according to 3GPP Rel 16 is that the number of radio accesses is limited to two, one strictly being 3GPP access and the other a non-3GPP access.

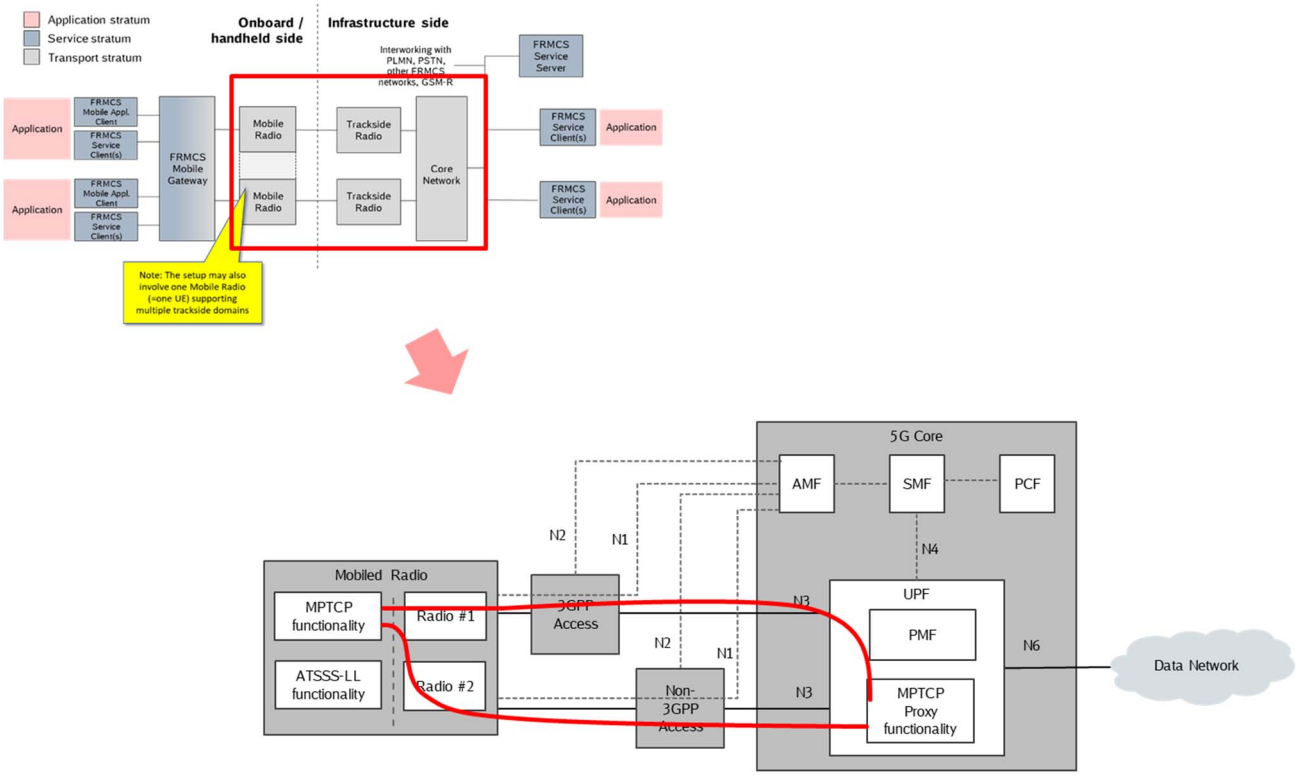

Figure 8-5: ATSSS approach for deployment scenarios 1a and 1b, where the UE is registered to the same PLMN, see 3GPP TS 23.501 [i.5], clause 4.2.10

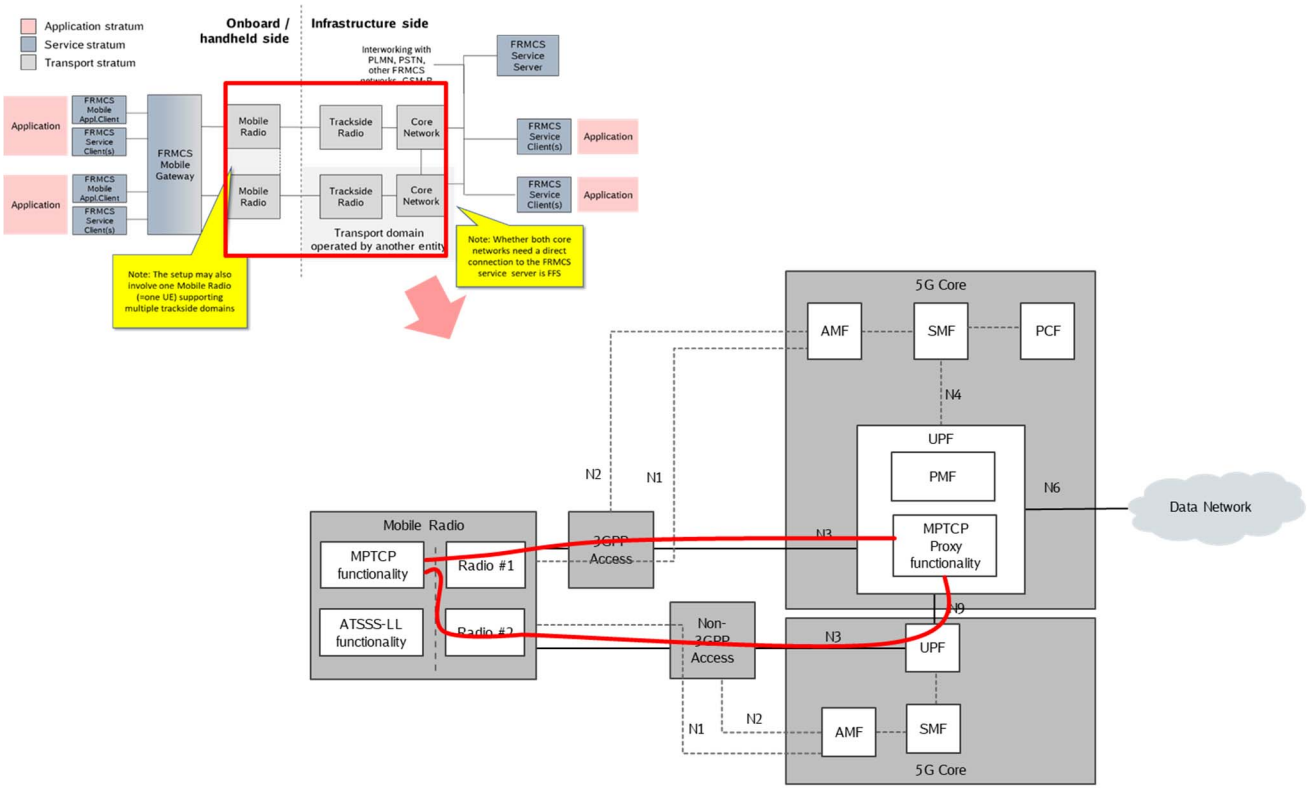

Figure 8-6: ATSSS solution for deployment scenario 2, where the UE is registered to different PLMNs, see 3GPP TS 23.501 [i.5], clause 4.2.10

8.3.4 Transport-level solutions: Above-the-core using MAMS

In contrast to ATSSS (a core-centric integration approach) which necessitates multiple radio interfaces to present a common IP address to the upper layer (Service Stratum), the Multi Access Management Services (MAMS) framework [i.17] enables each individual radio interface to be independently addressable. Furthermore, it is also possible to emulate ATSSS behaviour outside of the 3GPP transport. This independent IP addressing then facilitates deployment scenarios where different entities (e.g. 5G Core, EPC) can be responsible for managing the access networks associated with the different radio interfaces, and hence why the term "above-the-core integration" is adopted.

The MAMS framework [i.17] enables a flexible and dynamic selection of access and core network paths between a multi connectivity capable device and the network. The MAMS framework is illustrated in figure 8-7. The MAMS control plane consists of the Network Connection Manager (NCM) and the Client Connection Manager (CCM). Network Multi Access Data Proxy (N-MADP) and Client Multi Access Data Proxy (C-MADP) are the user plane functional elements. NCM and CCM exchange the MAMS control plane messages and configure the user plane protocols and traffic distribution at C-MADP and N-MADP.

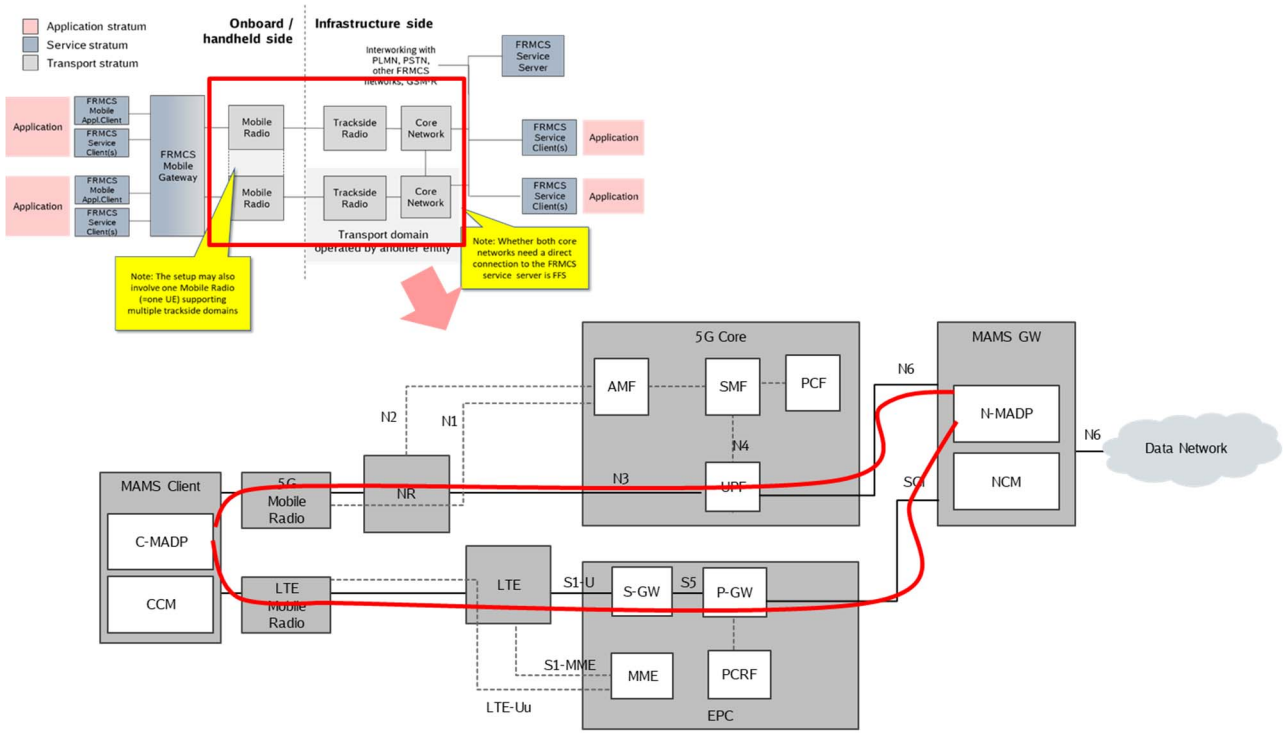

Figure 8-7: Above-the-core integration using MAMS for deployment scenario 2

8.3.5 Transport-level solutions: Above-the-core using ATSSS-Emulated solution

Another alternative is to emulate the ATSSS behavior by implementing the 5G ATSSS functions in *ATSSS-5G-Core-like GW* and *ATSSS-UE-like Client* which are outside of 3GPP transport, as illustrated in figure 8-8. In the figure, the two core networks (5G Core and EPC) manage independently from each other their respective 5G and LTE Mobile Radio. The *ATSSS-UE-like Client* is managing two data paths coming from the two UE (5G/4G). This *ATSSS-UE-like Client* is not seen by EPC nor by 5G Core and is only known by the *ATSSS-5G-Core-Like Gateway*.

The benefit of this approach is that most ATSSS functionalities defined in 3GPP could be re-used in order to manage registering of the on-board gateway (ATSSS-UE-Like), mutual authentication (between both ATSSS-UE-Like and ATSSS-5G-Core-Like), end-to-end multi path session management, user plane monitoring.

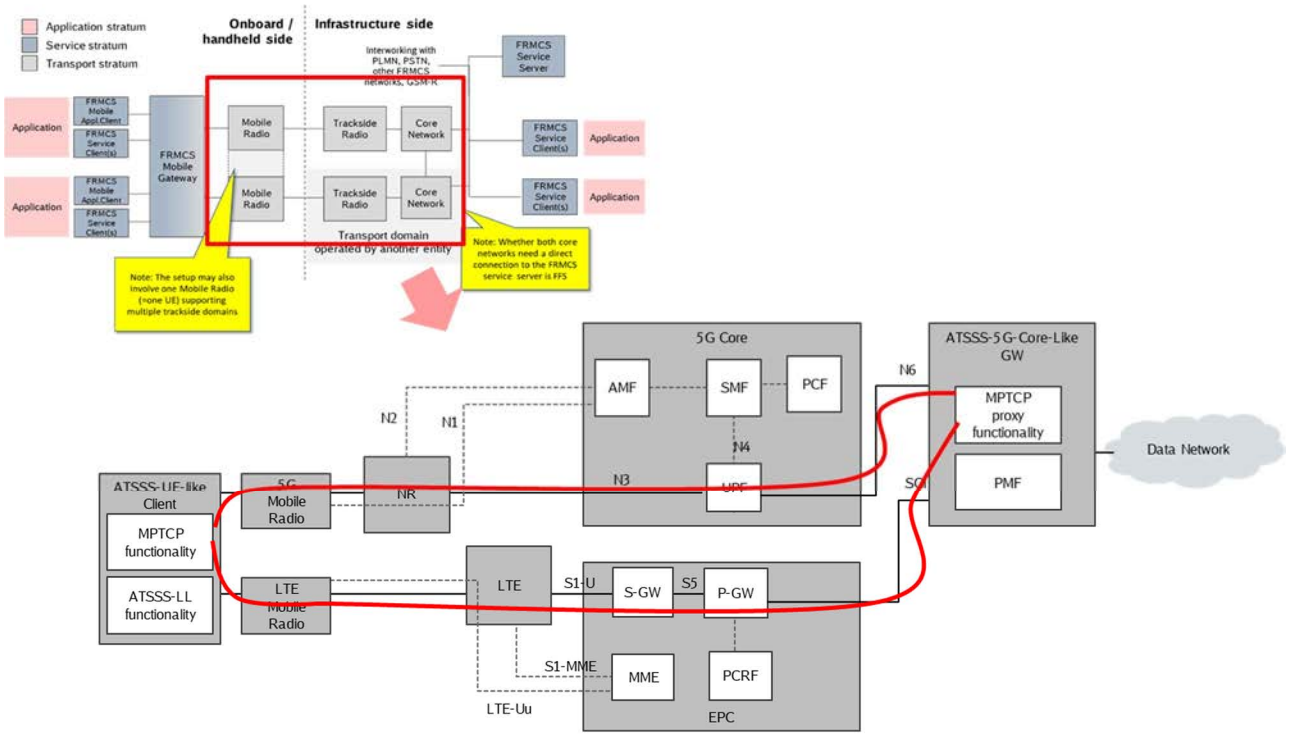

Figure 8-8: Above-the-core integration using ATSSS-Emulated solution for deployment scenario 2

8.3.6 Comparison of the possible solutions

Table 8-1 provides a preliminary comparison of the possible approaches to support multiple Mobile Radios and/or multiple Trackside Transport domains. Furthermore, Table 8-2 then shows how the possible technical solutions fulfil the requirements defined in TOBA-7510 [i.2] and in 3GPP TR 22.889 [i.3]. Note that no conclusions have been drawn yet, as further studies are required.

Table 8-1: Preliminary assessment of possible technical solutions for support of multiple Mobile Radios and/or multiple Trackside Transport domains

	Service-level approach	ATSSS	MAMS	ATSSS Emulated
Type	Solution in **Service Stratum**	Core-centric integration in **Transport Stratum**	Above-the-Core integration in **Transport Stratum**	Above-the-Core integration in **Transport Stratum**
Supports multiple Mobile Radios/UEs	Yes	No (only one UE)	Yes	Yes
Supports multiple Trackside Transport domains	Yes	Yes (though strictly one 3GPP and one non-3GPP)	Yes	Yes
Transport RAN	Access agnostic	Access agnostic	Access agnostic	Access agnostic
Transport Core	3GPP transport Core required	5G Core required	Core agnostic	Core agnostic
Native support of Transport QoS mechanism	Yes, AF may reside in the MC service system or in the IMS according to 3GPP TS 23.280 [i.11]. And then all QCI topics in 3GPP TS 23.501 [i.5] are applicable	Yes, flow-based 5G QoS can be natively supported	Policy control can be provided through MCX service and can be applied to underlying core networks	Policy control can be provided through MCX service and can be applied to underlying core networks
Implications in the Service Stratum	To be further clarified	To be further clarified	Multiple IP sessions managed in parallel for individual access links. it is transparent to the service stratum	Multiple IP sessions managed in parallel for individual access links. it is transparent to the service stratum

	Service-level approach	ATSSS	MAMS	ATSSS Emulated
Standard	3GPP TS 23.228 [i.9] 3GPP TS 23.280 [i.11]	3GPP Rel 16	IETF Internet-Draft	Proprietary, reusing 5G functionality
User plane protocol	Any protocols	ATSSS-LL: any MPTCP: TCP	Any protocols	Any protocols

Table 8-2: Assessment of the solutions w.r.t. their fulfilment of requirements in TOBA-7510 [i.2] and 3GPP TR 22.889 [i.3]

Quoted requirement	Service-level approach	ATSSS	MAMS	ATSSS Emulated
7.2.2.1: "*The FRMCS On-Board System shall have the capability to simultaneously control multiple FRMCS Radio Modules.*"	To be further defined	A Rel-16 UE that can be connected to two accesses, namely a 3GPP and a non-3GPP one	MAMS client	ATSSS-UE like client
7.4.2.1: "*The FRMCS On-Board System shall have the capability to share FRMCS Radio Modules among different communication services (e.g. multiple applications using the same FRMCS Radio Module).*"	Yes	Yes	Yes	Yes
7.2.2.2: "*The FRMCS On-Board System shall detect the non-availability/availability of transport capabilities provided by the FRMCS Radio Modules.*"	Interface between Mobile GW and service client	Interface between Mobile Radio and Mobile GW	Interface between MAMS client and service client	Interface between ATSSS-UE like Client and service client
7.3.2.5: "*The FRMCS On-Board System shall provide a mechanism to allow re-establishment of transport services using a different FRMCS Radio Module in case of a failure of the FRMCS Radio Module in use or upon detection of a persistent service outage of the FRMCS Radio Module in use.*"	To be further defined	ATSSS client based on the measurement of round-trip time	MAMS client	ATSSS-UE like client
7.3.2.3: "*The FRMCS On-Board System shall be able to establish multiple communication service sessions for the same application using the transport services from a single FRMCS Radio Module or different FRMCS Radio Modules.*"	Yes	Yes (two radios supported, one 3GPP and one non-3GPP)	Yes	Yes

Quoted requirement	Service-level approach	ATSSS	MAMS	ATSSS Emulated
7.2.2.5: "*The FRMCS On-Board System shall provide a mechanism to reallocate a communication session to a preferred transport service when it becomes available.*"	To be further defined. Selection intelligence would be in the service client (onboard) in the application	Defined in the 5G QoS policy. Optional in 3GPP Rel 16	Defined in MAMS framework, IETF RFC 8743 [i.17]	To be further defined. Selection intelligence would be in the ATSSS UE-like Client (onboard) and ATSSS-5G-Core-like GW (trackside)
7.1.2.5: "*Based on the QoS Profile, the FRMCS on-board system shall be able to determine:* • *The need for using multiple transport services (increased reliability)* • *The need for bandwidth aggregation* • *The suitable transport services/FRMCS Radio Modules* • *The preferred transport service/FRMCS Radio Module* • *The Initial FRMCS Radio Module* • *Which transport service to offload in case of capacity limitations.*"	To be further defined	Rel-16 ATSSS supports 4 steering modes: active-standby, smallest delay, load-balancing, high-priority, covering the mentioned requirements, QoS profiles are mapped to steering modes via ATSSS rules	Yes, refer to IETF RFC 8743 [i.17] - appendix B., section 8.5 (user plane configuration), and section 8.7 (traffic steering) (The aggregation ability is supported by configuring appropriate convergence protocol e.g. MPTCP in the user plane, section 11, IETF RFC 8743 [i.17])	Yes, as long as the Rel-16 ATSSS steering modes are implemented
7.2.2.6: "*The FRMCS On-Board system shall provide a mechanism to reallocate transport services to other FRMCS Radio Modules in order to optimise the overall FRMCS on-board system capacity. The transfer may also be triggered from trackside.*"	To be further defined. Selection intelligence would be in the service client (onboard) in the application	Defined in the 5G QoS policy, UE Route Selection Policies (URSPs) and ATSSS rules	Defined in MAMS IETF RFC 8743 [i.17].	To be further defined. Selection intelligence would be in the ATSSS UE-like Client (onboard) and ATSSS-5G-Core-like GW (trackside)
7.3.2.4: "*The FRMCS On-Board System shall be capable to aggregate the data received from multiple service or transport sessions and to split data to be sent across multiple service or transport sessions.*"	No. However, this could be complemented by combining with other transport-level solutions	Defined in the 5G QoS policy and URSP	Defined in MAMS IETF RFC 8743 [i.17]. The aggregation ability is supported by configuring appropriate convergence protocol e.g. MPTCP in the user plane, refer Section 11, IETF RFC 8743 [i.17]	To be further defined. Aggregation intelligence would be in the ATSSS UE-like Client (onboard) and ATSSS-5G-Core-like GW (trackside)

Quoted requirement	Service-level approach	ATSSS	MAMS	ATSSS Emulated
R-12.22-002: "*The FRMCS System shall provide a mechanism that minimizes the risk of single point of failure.*"	MC Service Server needs to be redundant	5G core needs to be redundant. Mobile GW should be considered to be redundant as well	MAMS GW needs to be redundant. Yes, MAMS is access agnostic - the control plane messaging is carried as user plane traffic transparently over the access network, and use of L4 multi-access protocols at user plane	ATSSS-5G-Core-like GW needs to be redundant. The UE-like Client (onboard) and ATSSS-5G-Core-like GW (trackside) should be considered to be redundant by implementing multiple instances
R-12.9-001: "*The FRMCS System shall be able to manage 3GPP access systems and non-3GPP access systems (terrestrial and non-terrestrial) simultaneously.*"	Yes	Partially, non-terrestrial is not yet supported in Rel-16 and is currently under study by 3GPP. Furthermore, a Rel-16 UE can be connected to only two accesses, namely a 3GPP and a non-3GPP one	Yes	Yes. Based on the ATSSS UE-like Client implementation
R-12.9-002: "*If provided by the FRMCS Equipment, the FRMCS Application on the FRMCS Equipment shall be able to make use of 3GPP and non-3GPP access systems simultaneously.*"	No, as no simultaneous support of multiple trackside domains	Yes	Yes	Yes
R-12.9-003: "*The FRMCS User shall not experience service interruptions in the usage of applications due to a change of an access system.*"	No. However, this could be complemented by combining with other transport-level solutions	Session will be kept, but delay, higher latency or quality degradation can be experienced. The definition of the acceptable interruption should be further detailed. URLLC can be a problem during access change	Session will be kept, but delay, higher latency or quality degradation can be experienced. The definition of the acceptable interruption should be further detailed	Session will be kept, but delay, higher latency or quality degradation can be experienced. The definition of the acceptable interruption should be further detailed
R-12.9-009: "*The FRMCS System shall consider the availability of radio bearer services at the position of the FRMCS User to allow communication.*"	No	ATSSS relies on RTT and access availability measurements. How this information is used is up to FRMCS implementation	Yes	Up to FRMCS System implementation
R-12.9-010: "*The FRMCS System shall select appropriate radio bearer service with consideration of the FRMCS applications configurable preconditions (e.g. ranking of the available bearer services)*"	No	URSP and ATSSS rules enable such preferences. How they are configured is up to FRMCS implementation	Yes, refer to Appendix B of IETF RFC 8743 [i.17]	Up to FRMCS System implementation

Quoted requirement	Service-level approach	ATSSS	MAMS	ATSSS Emulated
R-12.10.2-034: "*The FRMCS System shall take into account the service attributes to allow selection of the available bearer services.*"	No	ATSSS rules determine how each access is used. How the FRMCS requirements are translated to ATSSS rules is up to FRMCS implementation	Yes, refer to Appendix B of IETF RFC 8743 [i.17]	Up to the UE-like Client, ATSSS-5G-Core-like GW and FRMCS implementation

8.3.7 Preliminary conclusion

Based on the preliminary analysis of the aforementioned possible approaches to support multiple Onboard Mobile Radios and/or multiple Trackside Transport domains, it appears that there is no single solution that meets all requirements, but that rather a combination of a service stratum based approach (see clause 8.3.2) with one of the transport stratum based approaches (either ATSSS, MAMS or ATSSS emulated), where it should be noted that ATSSS only supports a single onboard Mobile Radio unit strictly serving one 3GPP access and one non-3GPP access.

The MAMS or ATSSS emulated approaches all require that transport stratum functionality is placed in the FRMCS Mobile Gateway.

The exact choice of the Transport Stratum based approach is FFS.

8.4 Potential physical implementation of onboard system

Especially for the FRMCS onboard system, it is important to stress that there may be many different physical implementation possibilities of the logical architecture described in clause 6, depending on the specific constellation of onboard applications, offerings from vendors, etc. For illustration purposes, the most likely options are shortly described here, as also shown in figure 8-9:

EXAMPLE 1: Especially legacy applications (for instance currently utilizing a serial interface towards an GSM-R EDOR) will need some conversion to IP to utilize the FRMCS system. In this context, it may be realistic to assume that a vendor would provide a dedicated "conversion" box which includes an implementation of the FRMCS Mobile Application Client and FRMCS Service Client(s) needed to interface over the OB_{APP} reference point to the (physical) mobile gateway.

EXAMPLE 2: For applications where it is not reasonable that these implement the required FRMCS client functionality to interface to the FRMCS system, the physical mobile gateway may provide this functionality. In this case, the interface between the application and the physical gateway may simply be based on the IP protocol.

EXAMPLE 3: A vendor may provide the FRMCS client functionality as a separate physical implementation that constitutes an "FRMCS proxy". In this case, the application would interface (e.g. via IP) to the proxy, and this would interface via OB_{APP} to the (physical) mobile gateway.

EXAMPLE 4: The FRMCS client functionalities may be co-implemented with the application. This would for instance likely be the case for the ETCS migration variant 3 mentioned in clause 5.5 and detailed in UIC TOBA-7540 [i.12].

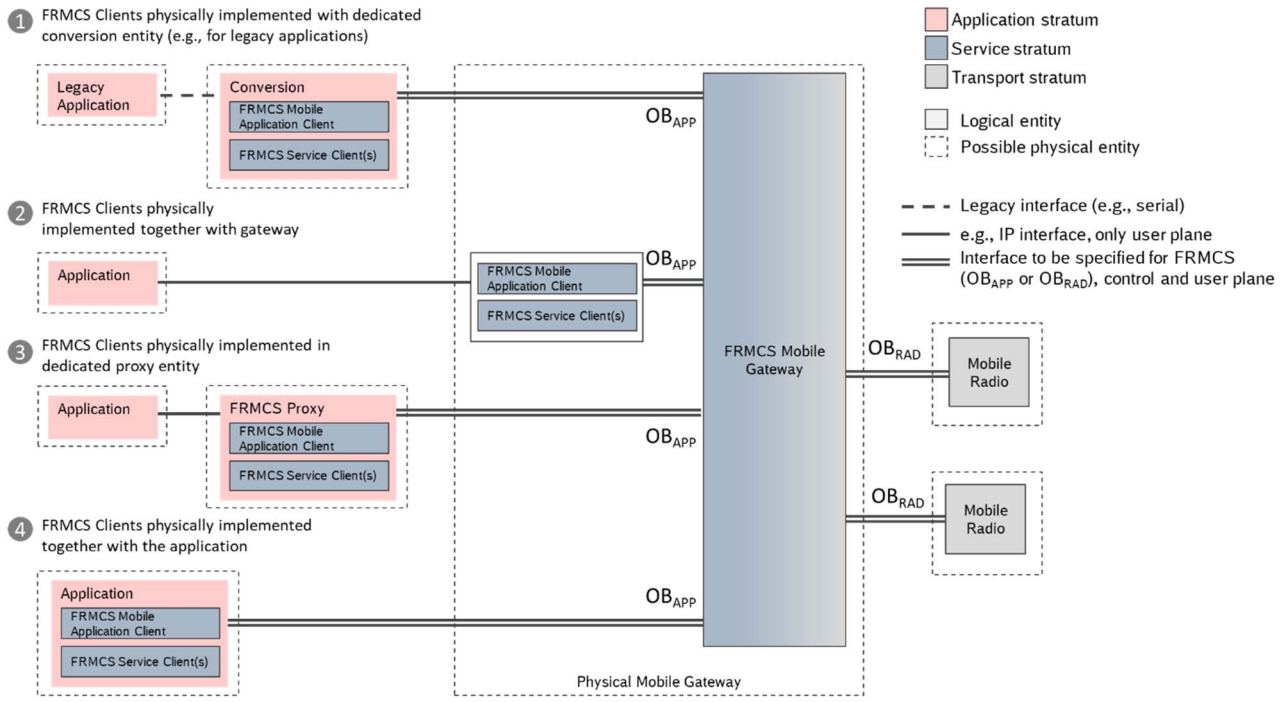

Figure 8-9: Examples for possible physical realizations of the FRMCS onboard/handset architecture

Considering that the FRMCS Clients and also the FRMCS Mobile Gateway will likely be implementable as software, it is of course also reasonable to assume that these could in principle be hosted on a shared platform/runtime environment together with some or all applications.

8.5 Potential physical implementation of trackside system

Similar to the onboard side, also on the trackside there could be many options how to physically implement the required functionality. For instance, it may also here be thinkable that the FRMCS Service Client functionalities required for each application are co-implemented with parts of the Trackside Transport, the FRMCS Service Server, or the application.

8.6 Potential technical realization of a handheld device

As mentioned in clause 6.1, a handheld device should follow the same onboard architecture as the onboard system of a train. However, it will likely be strongly reduced in setup (i.e. it would likely only contain few applications and only one mobile radio unit/one UE) and functionality. A possible technical realization is shown in figure 8-10.

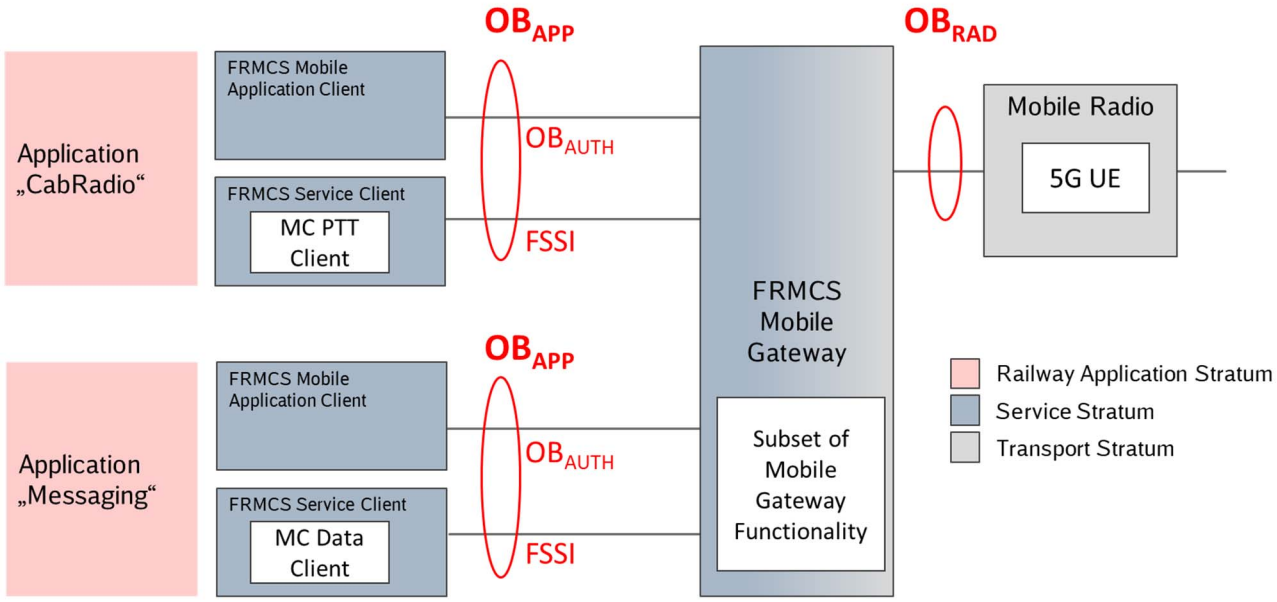

Figure 8-10: Possible technical realization of FRMCS handheld device

In this case, the functionality of the FRMCS Mobile Gateway would likely be reduced to (see clause 6.2):

General functions:

- Provides mechanisms to authorize applications located in the application stratum.
- Monitors the operation of Mobile Radio unit(s) and takes actions if these are down or service is otherwise interrupted.
- May provide O&M functionality (it is FFS whether this is to be specified in ETSI).

Functions specifically related to border-crossing scenarios:

- Anticipates border crossing and informs registered FRMCS Mobile Application Clients about new FRMCS Service Server to be used (aka service exposure function).

It should be noted that in a physical implementation of a handheld device, both the FRMCS Mobile Gateway and Mobile Radio could be co-implemented.

NOTE: It is FFS whether the OB_{AUTH} interface would have to be implemented to the full extent for a handheld device, as the limited set of applications residing on a handheld device may all be considered trusted.

9 Gap analysis

9.1 Mapping of functional service requirements to standardized 3GPP functions

As a step towards a functional gap analysis, the table 9-1 provides a preliminary mapping of the functional service requirements of the railway applications, as captured in the UIC URS [i.1], to functions provided by the 3GPP MC framework or the 3GPP 5G system.

Table 9-1: Mapping of functional service requirements of railway applications to standardized 3GPP functions

Functional needs according to UIC [i.1]	Proposed mapping to standardized components
Basic access and QoS	
Authorization of communication (clause 8.5 in [i.1])	For authentication and authorization of applications and users, the **identity management** and **key management** in the MC common service core can be leveraged. The identity management server contains the knowledge and means to authenticate by verifying the credentials supplied by the user. The key management server stores and provides security related information (e.g. encryption keys) to the key management client, group management server and MC service server(s) to achieve the security goals of confidentiality and integrity of media and signalling.
Authorization of application (clause 8.7 in [i.1])	
QoS Class Negotiation (clause 8.8 in [i.1])	**SIP service**: The Gm reference point between signalling user agent and the SIP service is used for MC session management ((session set-up, session tear down and session control) in support of MC service. **Rx** reference point between **PCF** and **SIP service** is used for policy control and QoS management. **SMF** is responsible for the enforcement of 5G bearer session management related policy decisions from **PCF**, related to service flow detection, QoS, charging, gating, traffic usage reporting and traffic steering.
Advanced QoS	
Assured Voice Communication (clause 8.1 in [i.1])	
Assured data communication (clause 8.10 in [i.1])	
Arbitration (clause 8.12 in [i.1])	Arbitration is performed solely by the Service Stratum and covered in the MC framework.
Advanced identity and location	
Role management and presence (clause 8.3 in [i.1])	The **configuration management server** in the MC common service core provides the functional alias management server functionality. Functional aliasing is still under standardization process in 3GPP Rel. 17.
Location services (clause 8.4 in [i.1])	
Group support	
Inviting-a-user messaging (clause 8.11 in [i.1])	
Multi-user talker control (clause 8.2 in [i.1])	The **group management server** in the MC common service core provides for management of groups supported within the MC service provider.
Recording	
Voice Recording and access to the recorded data (clause 5.19 in [i.1])	
Data recording and access (clause 5.20 in [i.1])	
Additional Functional Needs	
FRMCS should have the capability to route traffic to the target application in a distributed cloud (traffic steering)	As railway applications may be deployed in both Edge and Cloud depending on the latency and computation requirements, **UPF** and **SMF** in the 5GC play central roles in routing the traffic to desired applications and network functions. For enabling flexible and efficient routing of the traffic to applications: 1) the UPF can be seen as a distributed and configurable data plane; 2) the SMF plays a critical role in selecting and controlling the UPF and configuring its rules for traffic steering; 3) the SMF exposes service operations to allow FRMCS server as a 5G AF to influence the selection/re-selection of UPFs as well as request services to configure the rules to allow the traffic steering.

9.2 Identified risks

At the time of conclusion of this TR, no essential gaps are seen. However, there are various points where the realization of the FRMCS system depends on progress in 3GPP and other bodies, and some risks are seen, which are listed in the following:

- **Delayed MC support of 5G**. A key risk related to the FRMCS standardization is that the adaptation of the MC framework to 5G is delayed in 3GPP. The railway community is currently aiming to alleviate this risk by introducing a phased approach, i.e. to still have basic MC support of 5G in 3GPP Rel. 17 and a full adaptation of the MC framework to 5G in subsequent releases.
- **MAMS approach handled by a different standards body**. As the MAMS approach, as elaborated in clause 8.3, is standardized in IETF, it is difficult to ensure that the railway needs are sufficiently taken into account. Further, it is to be noted that the usage of MAMS would require further effort in the ETSI FRMCS standardization.
- **Support of latency-critical Railway Applications**. It is at this point not clear whether in the usage of the MC framework requires that user plane connectivity always has to go through a central MC core. If this would be the case, the FRMCS system would likely not be able to support E2E latencies below 10 ms, as required for some use cases in 3GPP TR 22.889 [i.3]. 3GPP has identified this point as a key issue in the context of 3GPP TR 23.783 [i.18], but it will likely not be addressed before 3GPP Rel. 18.

10 Topics for further study

Beyond various points marked in this technical report as "for future study", the following topics could not be covered well in the context of the present document and should hence be studied in further detail alongside the normative FRMCS work:

- Interworking between GSM-R and FRMCS.
- Realization of the FRMCS system in the form of a Service-Based Architecture (SBA).
- Cyber-security principles that go beyond the scope of 3GPP (e.g. related to cyber security for onboard bus systems).

Annex A:
Supportive Material on MC, 4G and 5G Support for Rail Communication

A.1 Mission Critical service support for Rail Communication

A.1.1 General

The FRMCS System will rely on the Mission Critical (MC) service functionality to provide point-to-point and group communication. It will encompass the service types voice, video and data.

For data centric Railway Applications the question can be raised, if applications should utilize the MCData functions and features or if such applications simply require a plain data pipe, which is provided by the core and transport layers of the FRMCS architecture.

It seems undisputable that data centric applications, which require group communication would benefit significantly from the MCX framework functions to exchange data between all members of a group based on centralized configuration and dynamic group associations. Examples range from railway emergency alert and shunting data communication to trackside warning system, etc.

In the MC service environment only authorized users using their associated unique identification are able to participate to standalone and group communication. This clear assignment of the communication streams to users allows to detect anomalies in the use of communication or its misuse. The user identification is necessarily implemented by the service stratum, i.e. MC service system so that users can also be served who do not use 3GPP UE.

TC RT agreed that point-to-point voice calls will be handled by the MCPTT framework and handled as private calls. For coherency reasons the same applies for data communication service handling.

A.1.2 Arguments for loose coupling of data centric Railway Applications

Some applications may not require to be MC service aware but require unique identification to exchange information between involved train born and trackside entities. MC service unawareness for data communication can be resolved by using MCData IP connectivity service capability (see ETSI TS 123 282 [i.26]). The MC service unaware data host will be able to exchange data using a MCData IP connectivity client that does not necessarily reside on the data host. With this capability the data communication will be identifiable and may obtain a functional alias. The MCData IP connectivity client may not be part of the data host. This loose coupling concept contributes to the decoupling between application and communication services and thus allows an independent evolution of data applications.

A.1.3 Integration of data centric Railway Applications

The FRMCS System needs to be aware of all applications using the system to allow control and management of functions and enable the admission and prioritization not only on the transport tier but also at communication tier. As example, some use cases in 3GPP TR 22.889 [i.3] require the arbitration of communications and the feedback capability to inform the corresponding user, which are pre-empted by the transport. In conclusion, a pure QoS based approach on the transport layer does not support the admission, pre-emption and arbitration requirements.

With the support of MC service capabilities, the application user makes use of a unique identity, which authorizes the applications user within the system, makes the user entities addressable, and support the interaction and if necessary pre-emption of corresponding communication in case of resource shortage or outage, etc. Arbitration determines the rank of simultaneous active user communications regardless of transport uncertainties. One key characteristic of the FRMCS System is the flexibility and independence of applications to communication services and transport services. In other words, the application will not manage the requests for a specific transport bearer and corresponding QoS profile, but rather generically request communication services from the FRMCS System. The FRMCS System will in response and based on the available resource and radio technologies assign the transport bearer to the communication. Hence any transport service relocation events are transparent to the Application Stratum.

Finally, applications which are already deployed and are complex to be adapted (e.g. legacy Railway Applications) or off-the-shelf applications or devices which are non-railway-specific (e.g. IP cameras, IoT sensors, etc.), could be supported with the introduction of a loose coupling concept which may allow various implementation choices.

A.1.4 Conclusion

Based on the previous points, TCRT will continue to consider that the MC framework is used for all FRMCS Railway Applications, in particular to ensure that all users and communication are identifiable. For Railway Applications that are not explicitly MC-aware, a functional entity in the FRMCS system will ensure communication.

A.2 FRMCS/4G support for Railway Applications

A.2.1 General

The assessment of the appropriate 3GPP core technology should be based on evaluating the needs of the following Use Cases.

Table A.2-1: Support of railway use cases through 4G features

Use Case	Applicable 4G Features
Allocation and isolation of FRMCS communication resources (was End-to-End Network Slicing for FRMCS)	Precursor techniques are available in 4G, such as APN-based slice selection, PLMN-ID based slice selection, DÉCOR and eDECOR.
FRMCS Bearer Flexibility	LTE EPS provides mobility mechanisms to support frequent handovers within and across 3GPP legacy systems or E-UTRAN and non 3GPP access systems in order to avoid service degradation. Furthermore, there are LTE-U, LAA, LWA and MulteFire which provide further options to augment standard LTE carriers with the unlicensed bands of WiFi networks. Satellite access can be connected via fixed IP connection.
QoS in a Railway Environment	See clause A.2.2.
FRMCS System Security Framework	LTE Authentication: EPS AKA (Authentication and Key Agreement) procedure is used in LTE networks for mutual authentication between users and networks. NAS Security: it is designed to securely deliver signalling messages between UEs and MMEs over radio links, performs integrity check (i.e. integrity protection/verification) and ciphering of NAS signalling messages. Different keys are used for integrity check and for ciphering. While integrity check is a mandatory function, ciphering is an optional function. NAS security keys, such as integrity key (KNASint) and ciphering key (KNASenc), are derived by UEs and MMEs from KASME. AS Security: it is purposed to ensure secure delivery of data between a UE and an eNB over radio links. It conducts both integrity check and ciphering of RRC signalling messages in control plane, and only ciphering of IP packets in user plane. Different keys are used for integrity check/ciphering of RRC signalling messages and ciphering of IP packets. Integrity check is mandatory, but ciphering is optional.

Use Case	Applicable 4G Features
Roaming	Basic 4G roaming supported. MCX users who roam onto a visiting network would roam onto the visiting MCX server. The visiting network server would query the home network MCX server Functional Alias info via the MCPTT-1 interface.
Service awareness	See clause A.2.2.
Availability - increasing measures	LTE supports fall-back to other RATs.
FRMCS Equipment capabilities for multiple FRMCS Users	LTE can allocate one IPv4 or IPv6 address for the PDU sessions within an APN.

A.2.2 QoS Management in LTE

Given the large diversity of communication requirements of the envisioned FRMCS applications, for instance ranging from a few kbps to multiple Mbps, and from latency requirements on the order of seconds to those on the order of 10 ms [i.3], it is essential that the FRMCS System is able to differentiate data packets related to different applications, in order to handle and prioritize these correctly according to their requirements. In this clause, the Quality of Service (QoS) management architectures and mechanisms in LTE releases is shortly elaborated.

In the LTE QoS architecture, the finest granularity of differentiating mobile data is on the level of radio bearers, which are characterized by a QoS class identifier reflecting aspects such as priority, acceptable delay and packet loss rate, and which can be of type guaranteed bit rate or non-guaranteed bit rate. Within one bearer, all data packets are treated within the same way, which would mean in an FRMCS context that multiple bearers would have to be set up for one terminal in order to be able to treat packets related to different FRMCS applications such as voice, ETCS/ATO and critical video differently, which would be rather inefficient Also, the LTE architecture always implies a one-to-one mapping of radio bearers to EPS bearers, which essentially means that the granularity of service differentiation in the core network is by definition the same as in the RAN.

A.3 FRMCS/5G support for Railway Applications

A.3.1 General

The assessment of the appropriate 3GPP core technology should be based on evaluating the needs of the following use cases.

Table A.3-1: Support of railway use cases through 5G features

Use Case	Applicable 5G Features
Allocation and isolation of FRMCS communication resources	Network Slicing requires a 5G core technology. Refer to [i.8] for more details.
FRMCS Bearer Flexibility	5G expands the use of heterogeneous network allowing a common core to control both 3GPP and non-3GPP access. It will support a harmonised QoS and policy framework that applies to multiple accesses.
QoS in a Railway Environment	See clause A.3.2.

Use Case	Applicable 5G Features
FRMCS System Security Framework	Primary authentication: Network and device mutual authentication in 5G is based on primary authentication. This is similar to 4G but there are a few differences. The authentication mechanism has in-built home control allowing the home operator to know whether the device is authenticated in a given network and to take final call of authentication. In railway this would be particularly useful for trains roaming onto another railway network. Primary authentication is radio access technology independent, thus it can run over non-3GPP technology such as IEEE 802.11 [i.24] WLANs. This would allow authentication to be consistent across the various flexible bearers. Secondary authentication: in 5G it is meant for authentication with data networks outside the mobile operator domain. For this purpose, different EAP based authentication methods and associated credentials can be used. A similar service was possible in 4G as well, but now it is integrated in the 5G architecture. Inter-operator security: Several security issues exist in the inter-operator interface arising from SS7 or Diameter in the earlier generations of mobile communication systems. To counter these issues, 5G Phase 1 provides inter-railway security from the very beginning. Privacy: Subscriber identity related issues have been know since 4G and earlier generations of mobile systems. In 5G a privacy solution is developed that protects the user's subscription permanent identifier against active attacks. A home network public key is used to provide subscriber identity privacy. Service Based Architecture (SBA): The 5G core network is based on a service based architecture, which did not exist in 4G and earlier generations. Thus 5G also provides adequate security for SBA.
Roaming	5G has an advantage on 4G of maintaining a network slice when roaming onto an external 5G network using Network Slicing Federation. The Slice/Service Type (SST) is used to refer to an expected network slice behaviour in terms of features and services. Standardized SST assigned by the 3GPP are used in order to identify slices uniquely around the world. Railway Industry could add its own universally recognized Network/Slice service types to fulfil FRMCS requirements. MCX users who roam onto a visiting network would roam onto the visiting MCX server. The visiting network server would query the home network MCX server Functional Alias info via the MCPTT-1 interface.
Maintainability	FRMCS on-board gateway will contain SIM cards to support multiple frequency bands For partition within a frequency band 5G New Radio has introduced the feature Carrier Bandwidth Parts. A carrier bandwidth part is a contiguous set of physical resource blocks, selected from a contiguous subset of the common resource blocks for a given numerology on a given carrier.
Service awareness	See clause A.3.2.
Availability - increasing measures	5G RAN supports Multi-RAT dual connectivity where one UE can maintain 2 parallel connections over 2 separate RATs.
FRMCS Equipment capabilities for multiple FRMCS Users	The UE would manage a separate IP address for each FRMCS user managed by the UE. 5G includes an UE IP address management which allows allocation and release of the UE IP address as well as renewal of the allocated IP address, where applicable. The UE would request a PDU session for each FRMCS User managed. The UE sets the requested PDU Session Type during the PDU Session Establishment procedure based on its IP stack capabilities as follows: UE supporting IPv6 and IPv4 should set the requested PDU Session Type according to UE configuration or received policy (i.e. IPv4, IPv6, or IPv4v6).

A.3.2 QoS Management in 5G/NR

The QoS management architecture in 5G has from the beginning been designed to allow for a much more fine-granular treatment of different data packets, and also a more flexible and independent QoS handling in core network and RAN.

This is enabled through the introduction of so-called QoS flows, which are described through QoS profiles which for instance contain the information whether the flow is of type guaranteed bit rate or non-guaranteed bit rate, and an Allocation and Retention Priority (ARP), and which are defined and managed by the Session Management Function (SMF) in the 5G core network. A single PDU session can relate to multiple QoS flows, so that even within a PDU session data packets can be treated in a differentiated way.

In the downlink, the User Plane Function (UPF) in the core network then uses Service Data Flow (SDF) classification rules provided by the SMF to map individual data packets to the defined QoS flows, and the new Service Data Adaptation Protocol (SDAP) in the RAN then maps these to Data Radio Bearers (DRBs). In the uplink, the terminal evaluates individual data packets against QoS rules provided by the SMF and assigns these accordingly to QoS flows and subsequently to data radio bearers. Alternatively, so-called reflective QoS handling can be applied, where the terminal uses the classification of downlink packets to derive that of uplink packets.

5G Policy framework has an Application detection mechanism in the core so watch service flow can be assigned its own prioritization, pre-emption and arbitration rules and can be gated for only authorized traffic.

5G policy framework only communicates its policy decision to end-points via Applications Functions. In the case of FRMCS this would be an MCX server. Therefore, each FRMCS user requiring a notification of pre-emption would need to be registered on the MCX server. However autonomous FRMCS applications would have a deterministic high priority arbitration rule applied to them similar to the Ultra-Reliable-Low-latency devices introduced in 5G. These devices would always have prioritized access to resources and could never be pre-empted. As such there would be no need for them to use the MCX framework.

A.3.3 Comparison and Suitability of QoS Management Options for Rail Operations

The key properties of the different QoS management options are summarized in the following table A.3-2.

Table A.3-2: Comparison of QoS management options in LTE and 5G/NR

	LTE	5G/NR
Granularity of QoS differentiation	Radio bearers/EPS bearers	Individual data packets within a PDU session
QoS management in core network and RAN	Coupled	Independent, i.e. core network maps packets to QoS flows, and RAN independently maps QoS flows to radio bearers

While both the LTE and 5G QoS architectures would in principle support FRMCS application needs, it is expected that the 5G approach is significantly more efficient, as a single terminal could be served with one radio bearer, while still allowing for the differentiation of packets relating to different FRMCS applications. In addition, the 5G approach also allows to differentiate packets within one PDU session. This is for instance beneficial for any applications based on protocols (like TCP) that require an initial session setup, as packets related to this setup could be prioritized for faster session establishment, while subsequent packets, e.g. conveying video data, could be treated at normal priority.

A.4 Possibility to realize FRMCS System with 4G core network

As mentioned in clause 8.2, it may also be considered to realize an FRMCS system with a 4G core network, for instance as migration step for non-European countries that are now rolling out 4G for rail operation but desire to migrate to FRMCS later. This option is shown in figure A.4-1.

As indicated in figure A.4-1, it should be noted that even if a 4G core network is used, the interfaces from the core network to the Service Stratum should be based on the N5 and N6 interfaces standardized by 3GPP for 5G, as opposed to their LTE counterparts Rx and SGi. Hence, the Trackside Transport has to provide required protocol conversion in this case.

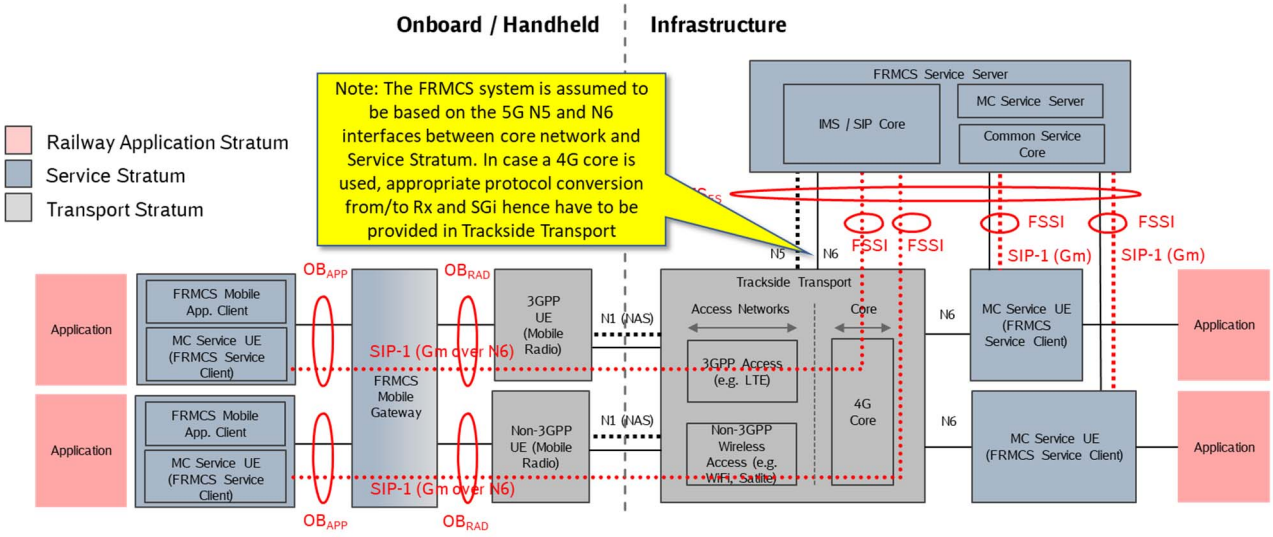

Figure A.4-1: Possible technical realization of FRMCS system based on 4G core network

Annex B:
Change History

Date	Version	Information about changes
July 2016	0.0.1	First publication of the TR after kickoff meeting held 26 February 2016 by ETSI On-line meeting
September 2016	0.0.2	Version 0.0.2 prepared by the Rapporteur with contribution from FEEI (Fachverband der Elektro- und Elektronikindustrie Bereich Technik) for the review dated 16 September 2016
October 2016	0.0.3	
July 2018	0.0.4	Structure of the TR adapted to the update of the Work Item
September 2018	0.0.5	Stable draft version of the TR
November 2018	0.0.6	Version presented for approval at TC RT #71
November 2018	0.0.7	Version presented for approval by Remote Consensus
December 2019	0.1.0	Version updated for discussion in f2f workshop on December 12, 2019
April 2020	0.1.1	Stable draft of revised TR uploaded on April 9, 2020
July 2020	0.2	Final draft for approval uploaded on June 15, 2020

History

Document history		
V1.1.1	January 2019	Publication
V1.2.1	August 2020	Publication