Draft **ETSI TS 103 765-1** V1.0.0 (2025-07)

TECHNICAL SPECIFICATION

**Rail Telecommunications (RT);
Future Railway Mobile Communication System (FRMCS);
Building Blocks and Functions;
Part 1: Transport Stratum**

Reference

DTS/RT-0083

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

Important notice

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

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Railway Telecommunications (RT) and is now submitted for the combined Public Enquiry and Vote phase of the ETSI Standardisation Request deliverable Approval Procedure (SRdAP).

The present document is part 1 of a multi-part deliverable covering Building Blocks and Functions for the Future Railway Mobile Communication System (FRMCS), as identified below:

Part 1: **"Transport Stratum";**

Part 2: "Service Stratum";

Part 3: "Train On-Board functions and interfaces";

Part 4: "Trackside functions and interfaces";

Part 5: "User Equipment (UE) capabilities".

Modal verbs terminology

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

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

1 Scope

The present document specifies the FRMCS Transport Stratum for the Future Railway Mobile Communications System (FRMCS). In general, the FRMCS Transport Stratum provides data connectivity and the related services.

The present document covers:

- 3GPP terrestrial access.

- Transport stratum interconnection scenarios in all aspects.

- 3GPP access sharing, mobility within transport stratum.

- QoS and policy control.

- Authentication and authorization for the use of the transport stratum.

- Transport stratum common features.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 necessary for the application of the present document.

[1] ETSI TS 123 501 (V18.9.0): "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 18.9.0 Release 18)".

[2] ETSI TS 127 001 (V18.0.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); General on Terminal Adaptation Functions (TAF) for Mobile Stations (MS) (3GPP TS 27.001 version 18.0.0 Release 18)".

[3] ETSI TS 127 007 (V18.8.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; AT command set for User Equipment (UE) (3GPP TS 27.007 version 18.8.0 Release 18)".

[4] ETSI TS 138 201 (V18.0.0): "5G; NR; Physical layer; General description (3GPP TS 38.201 version 18.0.0 Release 18)".

[5] ETSI TS 138 300 (V18.5.0): "5G; NR; NR and NG-RAN Overall description; Stage-2 (3GPP TS 38.300 version 18.5.0 Release 18)".

[6] ETSI TS 103 765-2: "Rail Telecommunications (RT); Future Railway Mobile Communication System (FRMCS); Building Blocks and Functions; Part 2: Service Stratum".

[7] ETSI TS 103 765-3: "Rail Telecommunications (RT); Future Railway Mobile Communication System (FRMCS); Building Blocks and Functions; Part 3: Train On-Board functions and interfaces".

[8] FRMCS FFFIS-7950: "FRMCS FFFIS - Form Fit Functional Interface Specification", V2.0.0.

[9]   ETSI TS 124 501 (V18.10.0): "5G; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (3GPP TS 24.501 version 18.10.0 Release 18)".

[10]   ETSI TS 123 502 (V18.9.0): "5G; Procedures for the 5G System (5GS) (3GPP TS 23.502 version 18.9.0 Release 18)".

[11]   ETSI TS 138 211 (V18.6.0): "5G; NR; Physical channels and modulation (3GPP TS 38.211 version 18.6.0 Release 18)".

[12]   ETSI TS 138 212 (V18.6.0): "5G; NR; Multiplexing and channel coding (3GPP TS 38.212 version 18.6.0 Release 18)".

[13]   ETSI TS 138 213 (V18.6.0): "5G; NR; Physical layer procedures for control (3GPP TS 38.213 version 18.6.0 Release 18)".

[14]   ETSI TS 138 214 (V18.6.0): "5G; NR; Physical layer procedures for data (3GPP TS 38.214 version 18.6.0 Release 18)".

[15]   ETSI TS 138 321 (V18.5.0): "5G; NR; Medium Access Control (MAC) protocol specification (3GPP TS 38.321 version 18.5.0 Release 18)".

[16]   ETSI TS 138 322 (V18.2.0): "5G; NR; Radio Link Control (RLC) protocol specification (3GPP TS 38.322 version 18.2.0 Release 18)".

[17]   ETSI TS 138 323 (V18.5.0): "5G; NR; Packet Data Convergence Protocol (PDCP) specification (3GPP TS 38.323 version 18.5.0 Release 18)".

[18]   ETSI TS 138 331 (V18.5.1): "5G; NR; Radio Resource Control (RRC); Protocol specification (3GPP TS 38.331 version 18.5.1 Release 18)".

[19]   ETSI TS 129 522 (V18.9.0): "5G; 5G System; Network Exposure Function Northbound APIs; Stage 3 (3GPP TS 29.522 version 18.9.0 Release 18)".

[20]   ETSI TS 133 501 (V18.9.0): "5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 18.9.0 Release 18)".

[21]   IETF RFC 9113: "HTTP/2".

[22]   IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[23]   ETSI TS 123 289 (V18.10.0): "5G; Mission Critical services over 5G System; Stage 2 (3GPP TS 23.289 version 18.10.0 Release 18)".

[24]   ETSI TS 129 513 (V18.9.0): "5G; 5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3 (3GPP TS 29.513 version 18.9.0 Release 18)".

[25]   ETSI TS 129 512 (V18.9.0): "5G; 5G System; Session Management Policy Control Service; Stage 3 (3GPP TS 29.512 version 18.9.0 Release 18)".

[26]   ETSI TS 129 511 (V18.3.0): "5G; 5G System; Equipment Identity Register Services; Stage 3 (3GPP TS 29.511 version 18.3.0 Release 18)".

[27]   IETF RFC 8684: "TCP Extensions for Multipath Operation with Multiple Addresses".

[28]   ETSI TS 124 193 (V18.8.0): "5G; 5G System; Access Traffic Steering, Switching and Splitting (ATSSS); Stage 3 (3GPP TS 24.193 version 18.8.0 Release 18)".

[29]   ETSI TS 129 514 (V18.9.0): "5G; 5G System; Policy Authorization Service; Stage 3 (3GPP TS 29.514 version 18.9.0 Release 18)".

[30]   ETSI TS 129 214 (V18.4.0): "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Policy and charging control over Rx reference point (3GPP TS 29.214 version 18.4.0 Release 18)".

[31]   ETSI TS 138 104 (V18.9.0): "5G; NR; Base Station (BS) radio transmission and reception (3GPP TS 38.104 version 18.9.0 Release 18)".

[32]   ETSI TS 138 133 (V18.9.0): "5G; NR; Requirements for support of radio resource management (3GPP TS 38.133 version 18.9.0 Release 18)".

[33]   Recommendation ITU-T G.8271.1: "Network limits for time synchronization in packet networks with full timing support from the network".

[34]   Recommendation ITU-T G.8271.2: "Network limits for time synchronization in packet networks with partial timing support from the network".

[35]   ETSI TS 103 793: "Rail Telecommunications (RT); Future Railway Mobile Communication System (FRMCS); Radio Characteristics".

[36]   ETSI TS 103 765-5: "Rail Telecommunications (RT); Future Railway Mobile Communication System (FRMCS); Building Blocks and Functions; Part 5: User Equipment (UE) capabilities".

[37]   ETSI TS 129 591 (V18.9.0): "5G; 5G System; Network Exposure Function Southbound Services; Stage 3 (3GPP TS 29.591 version 18.9.0 Release 18)".

[38]   ETSI TS 123 122 (V18.10.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (3GPP TS 23.122 version 18.10.0 Release 18)".

[39]   IETF RFC 8200: "Internet Protocol, Version 6 (IPv6) Specification".

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1]   ETSI TR 103 791: "Rail Telecommunications (RT); Future Railway Mobile Communication System (FRMCS); Terminology for FRMCS specifications".

[i.2]   IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".

[i.3]   IETF RFC 8915: "Network Time Security for the Network Time Protocol".

[i.4]   ETSI TS 138 413 (V18.5.0): "5G; NG-RAN; NG Application Protocol (NGAP) (3GPP TS 38.413 version 18.5.0 Release 18)".

[i.5]   ETSI TS 138 423 (V18.5.0): "5G; NG-RAN; Xn Application Protocol (XnAP) (3GPP TS 38.423 version 18.5.0 Release 18)".

[i.6]   ETSI TS 138 463 (V18.0.0): "5G; NG-RAN; E1 Application Protocol (E1AP) (3GPP TS 38.463 version 18.0.0 Release 18)".

[i.7]   ETSI TS 138 473 (V18.5.0): "5G; NG-RAN; F1 Application Protocol (F1AP) (3GPP TS 38.473 version 18.5.0 Release 18)".

[i.8]   ETSI TS 136 423 (V18.4.0): "LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 Application Protocol (X2AP) (3GPP TS 36.423 version 18.4.0 Release 18)".

# 3	Definition of terms, symbols and abbreviations

## 3.1	Terms

For the purposes of the present document, the terms given in ETSI TR 103 791 [i.1] and the following apply:

gNodeB: base station that provides NR radio access for 5G networks

multipath dataflow: application flow of IP packets processed by the FRMCS Multipath Function, characterized by its application-related attributes and identified via IP-5-tuples

multipath data path: network route within a Transport Domain

multipath policy: set of rules assessed by the FRMCS Multipath Function to determine the distribution of a Multipath Dataflow to one or more Multipath Datapaths

multipath protocol: protocol operating over an IP transport network supporting the use of multiple network interfaces (such as MP-TCP, MP-QUIC, etc.)

## 3.2	Symbols

Void.

## 3.3	Abbreviations

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

5G NR	5G New Radio
5GC	5G Core Network
5G-EIR	5G-Equipment Identity Register
5GS	5G System
5QI	5G QoS Identifier
AF	Application Function
AKA	Authentication and Key Agreement
AMF	Access and Mobility Function
API	Application Programming Interface
APTS	Assisted Partial Timing Support
ARP	Allocation and Retention Priority
AUSF	Authentication Server Function
AVP	Attribute Value Pair
BSF	Binding Support Function
CP	Control Plane
CSC	Communication Session Category
CSCF	Call Server Control Function
DL	Downlink
DN	Data Network
DNS	Domain Name Server
DRB	Dara Radio Bearer
DSCP	Differentiated Service Code Point
EF	Expedited Forwarding
ESP	Encapsulating Security Payload
FFFIS	Form Fit Functional Interface Specification
FQDN	Fully Qualified Domain Name
FRMCS	Future Railway Mobile Communication System
GBR	Guaranteed Bit Rate
gNodeB	Next generation Node B
GNSS	Global Navigation Satellite System
GPSI	Generic Public Subscription Identifier
GSM-R	Global System for Mobile Communications - Railway

GW	Gateway
HPLMN	Home PLMN
HR	Home Routed
HTTP	Hyper Text Transfer Protocol
ID	Identity
IKEv2	Internet Key Exchange version 2
IM	Infrastructure Manager
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identifier
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv6	IP version 6
I-UPF	Intermediate UPF
JSON	JavaScript Object Notation
LBO	Local Breakout
LIF	Lawful Intercept Function
MAC	Medium Access Control
MC	Mission Critical
MCC	Mobile Country Code
MCPTT	Mission Critical Push To Talk
MCS	Mission Critical Services
MCX	Mission Critical Services
ME	Mobile Equipment (in the 3GPP context)
MIMO	Multi Input Multi Output
MNC	Mobile Network Code
MNO	Mobile Network Operator
MO	Mobile Originated
MOCN	Multi Operator Core Network
MP	Multipath Protocol
MPF	Multipath Function
MPLS	Multiprotocol Label Switching
MPM	Multipath Management
MP-QUIC	Multipath QUIC
MP-TCP	Multipath TCP
MPU	Multipath User plane
MT	Mobile Termination (in the 3GPP context)
N9HR	N9 Home Routing
NAI	Network Access Identifier
NAS	Non-Access Stratum
NEF	Network Exposure Function
NF	Network Function
NR SA	NR Stand-Alone
NR	New Radio (In the context of 5G)
NRF	Network Repository Function
NTP	Network Time Protocol
O&M	Operation & Management
OB	On-Board
OTDOA	Observed Time Difference of Arrival
PCC	Policy and Charging Control
PCF	Policy Control Function
P-CSCF	Proxy Call Service Control Function
PDR	Packet Detection Rule
PDU	Protocol Data Unit
PFD	Packet Flow Description
PLMN	Public Land Mobile Network
PRTC-A	Primary Reference Time Clock - Class A
PTP	Precision Time Protocol
QFI	QoS Flow identifier
QoS	Quality of Service
QUIC	Quick UDP Internet Connection
RAN	Radio Access Network
RAT	Radio Access Technology

RF	Radio Frequency
RLC	Radio Link Control
RMR	Railway Mobile Radio
RU	Railway Undertaking
SBA NF	Service-Based Architecture Network Function
SCP	Service Communication Proxy
SDI	Session Description Information
SEG	Security Gateway
SEPP	Security Edge Protection Proxy
SIB	System Information Block
SIM	Subscriber Identity/Identification Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SM	Session Management
SMF	Session Management Function
SUCI	Subscriber Concealed Identifier
SUPI	Subscriber Permanent Identifier
TAP	Transport Access Point
TCMS	Train Control & Monitoring System
TCP	Transport Control Protocol
TDD	Time Division Duplex
TE	Terminal Equipment (in the 3GPP context)
UAC	Unified Access Control
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment (in the 3GPP context)
UICC	Universal Integrated Circuit Card
UL	Uplink
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
VAS	Voice Application Subsystem
VPLMN	Visited PLMN

4   Principles and concept

4.1   General

Clause 4 describes the system architecture of the FRMCS Transport Stratum to support packet switched data connectivity and service enabling deployments. The system architecture applicable for FRMCS is the 3GPP 5G System (5GS) and the related 5GS architecture defined in ETSI TS 123 501 [1].

4.2   Architecture

4.2.1   Common Architecture Principles

The Transport Stratum consists of the access domain and the 5G core network domain (see Figure 4.2.2-1).

The transport stratum User Equipment (UE) is part of the transport stratum and requires appropriate credentials necessary to make use of the transport stratum. FRMCS Transport Stratum identities are described in clause 10.

The FRMCS Transport Stratum utilizes terrestrial wireless 3GPP access based on 5G NR RAT and shall be implemented as described in ETSI TS 138 201 [4], ETSI TS 138 300 [5] and ETSI TS 123 501 [1].

For 5GC, the UE supports N1-reference point for Non-Access Stratum (NAS) signalling for the types of access.

The 5G core domain used for FRMCS Transport Stratum shall provide the convergence between the types of access for the control plane N2-reference point and for the user plane N3 - reference point. In the case of devices (e.g. VAS controller) integrated in IM/RU internal IT/LAN structures, FRMCS transport access control is granted using best practice methods, and FRMCS service access control is granted based on FRMCS SIP Core and MCX procedures. QoS within the underlying trackside IP network (for both gNodeB - UPF connection or outside of 5G) is based on implementations that map FRMCS QoS towards QoS mechanisms in the IP network. FRMCS SIP Core is as specified in ETSI TS 103 765-2 [6].

In general, a UE in transport stratum is considered to be a logical block is subdivided into several domains separated by reference points. It may consist of one or multiple physical units for different types of access. A UE is subdivided into the UICC and the Mobile Equipment (ME), which can be further subdivided into Mobile Termination (MT) and Terminal Equipment (TE) in accordance with - ETSI TS 127 001 [2] and ETSI TS 127 007 [3]. In a broader sense, the UE allows a service client to obtain transport services for its communication. The FRMCS Transport Stratum shall support IPv6 IP addressing as specified in IETF RFC 8200 [39].

Accordingly, two Transport Access Points (TAP) shall be provided for interaction between the 5G transport stratum and the service stratum:

- **TAP Service Client** forms the transition to the potential service clients.

- **TAP Service Agent** is located at the edge of the 5G core domain. N5/Rx-reference point or N33-reference point (if NEF is deployed in 5GC) shall be used for the control plane and N6-reference point shall be used for the user plane in accordance with ETSI TS 123 501 [1].

4.2.2   Architecture for a Standalone FRMCS Transport Domain

The Standalone FRMCS Architecture represents a FRMCS network without external connections, neither to foreign FRMCS Domain, nor to a GSM-R system or a Mobile Network Operator's 5G Core domain.
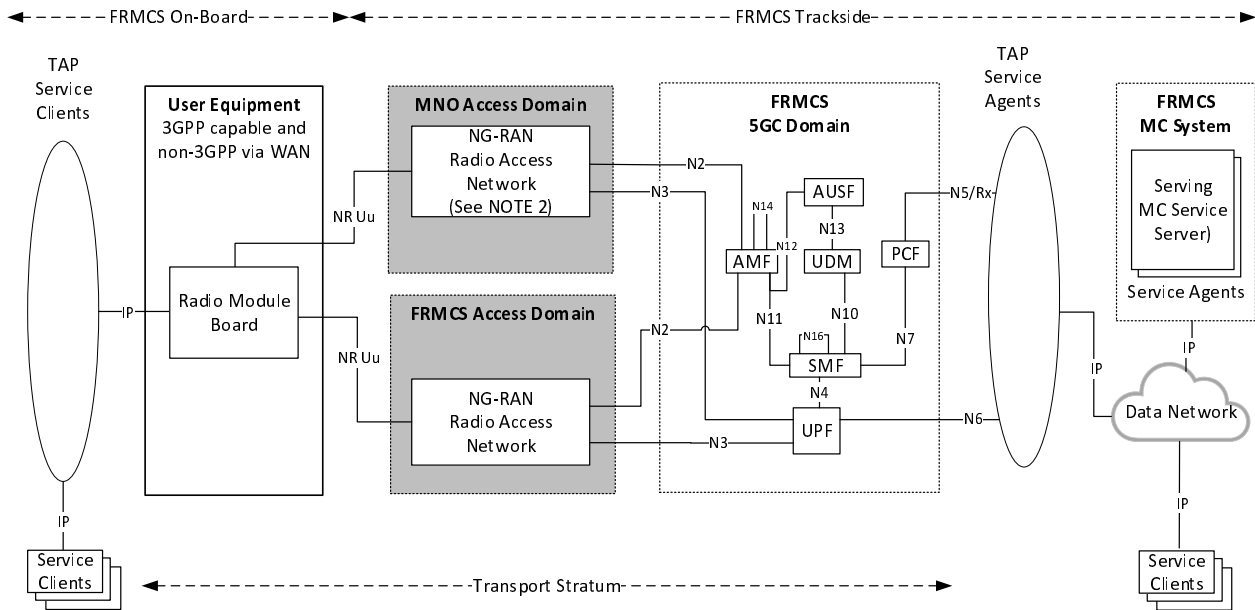
Figure 4.2.2-1:FRMCS Standalone Transport Domain Architecture (non-roaming)

NOTE 1: N2 and N3 reference points are protected by ESP and IKEv2 certificates-based authentication as per clauses 9.2 and 9.3 in ETSI TS 133 501 [20]. IPsec is mandatory to implement on the gNodeB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

NOTE 2: Use of MOCN is subject to subject to FRMCS operator policy.

The minimum 5G system (5GS) for a standalone FRMCS Domain Architecture shall be based on the non-roaming reference architecture as outlined in clauses 4.2.2 (Network Functions and entities) and 4.2.3 (Non-roaming reference architecture) of ETSI TS 123 501 [1] and shall contain the logical following building blocks:

- Authentication Server Function (AUSF).

- Access and Mobility Management Function (AMF).

- Data Network (DN), e.g. operator services, Internet access or 3rd party services.

- Policy Control Function (PCF).

- Session Management Function (SMF).

- Unified Data Management (UDM).

- Unified Data Repository (UDR).

- User Plane Function (UPF).

- User Equipment (UE).

- (Radio) Access Network ((R)AN).

4.2.3 Architecture for a FRMCS Transport Domain in interaction with other FRMCS Domains

4.2.3.0 General

A FRMCS Transport Domain in interaction with other FRMCS Domains shall implement a home routed interconnected domain architecture depicted in Figure 4.2.3.0-1, which enables the UE (from the own FRMCS Transport Domain or from another FRMCS Transport Domain) in a visited FRMCS network to communicate with the service stratum of its home network.
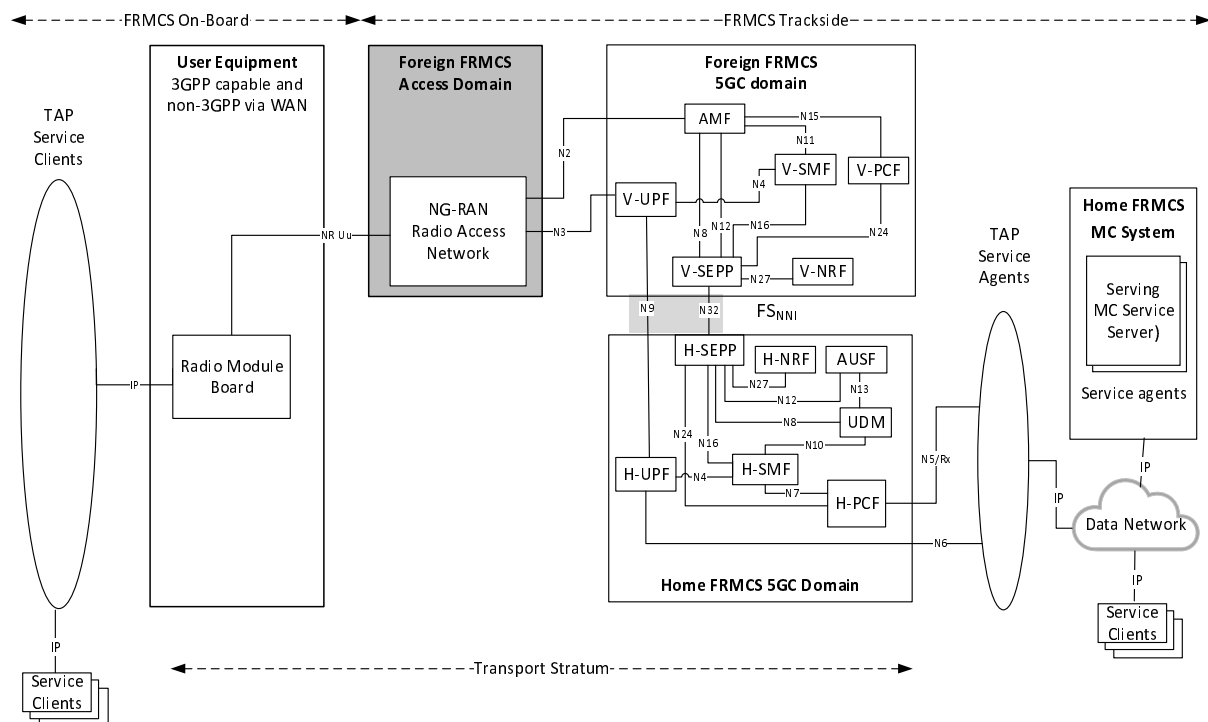
**Figure 4.2.3.0-1: Architecture for a FRMCS Transport Domain in interaction with
a foreign FRMCS Domain, MC services provided by the Primary (Home) FRMCS MC system**

NOTE: N2 and N3 reference points are protected by ESP and IKEv2 certificates-based authentication as per clauses 9.2 and 9.3 in ETSI TS 133 501 [20]. IPsec is mandatory to implement on the gNodeB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

The minimum 5G system (5GS) for a FRMCS Transport Domain in interaction with other FRMCS Domains shall be based on the roaming reference architecture as outlined in clauses 4.2.2 (Network Functions and entities) and 4.2.4 (Roaming reference architecture) of ETSI TS 123 501 [1] and shall comprise of the building blocks listed in clause 4.2.2 of the present document and the following additional logical building blocks for security reasons, mostly:

- Network Repository Function (NRF).

- Security Edge Protection Proxy (SEPP).

FS_{NNI} in Figure 4.2.3.0-1 refers to the Network-to-Network Interconnection (NNI), connecting different FRMCS Domains.

4.2.3.1　　　FS$_{NNI}$ reference point (at FRMCS Transport Domain level)

The FS_{NNI} reference point is the reference point between FRMCS Domains. At FRMCS Transport Domain level, it enables mobility of FRMCS Users between FRMCS Domains.

The FS_{NNI} reference point is composed of the 5GC reference points listed in Table 4.2.3.1-1 for Local Breakout (LBO), Home Routing (HR) or both.

Table 4.2.3.1-1: FS$_{NNI}$ basic reference points

Reference point	Between	Purpose	LBO/HR
N8	AMF (VPLMN) ↔ UDM (HPLMN)	Subscription retrieval	Both
N9	UPF (VPLMN) ↔ UPF (HPLMN)	User-plane traffic forwarding	HR
N10	SMF (VPLMN) ↔ UDM (HPLMN)	Session-related subscription data	LBO
N12	AMF (VPLMN) ↔ AUSF (HPLMN)	Authentication	Both
N16	SMF (VPLMN) ↔ SMF (HPLMN)	Inter-PLMN session management	Both
N24	PCF (VPLMN) ↔ PCF (HPLMN)	Mobility-related policies	Both
N32	SEPP (VPLMN) ↔ SEPP (HPLMN)	Secure inter-PLMN control-plane communication	Both

NOTE: N14 can be implemented to enable smooth mobility and network selection across different PLMNs in 5G, by allowing AMFs to exchange all necessary information to maintain UE service continuity.

A FRMCS Transport Domain shall support the reference points listed in Table 4.2.3.1-1.

A FRMCS Transport Domain should implement the N27 reference point to enable SBA NF discovery (under communication model B and C as described in ETSI TS 123 501 [1], clause E.1).

4.2.4　　　FRMCS National Roaming Architecture (Home Routed)

National roaming allows the use of Mobile Network Operator spectrum in a National Roaming architecture. This architecture uses the FRMCS Access Domain radio module, which is equipped to handle Mobile Network Operator (MNO) spectrum as well, or a separate MNO radio module in the On-Board FRMCS, which is configured to roam on the MNO network. The FRMCS Multipath Function, specified in clause 5.3, determines which On-Board FRMCS Radio Module is used for the Multipath Datapath of the application.

In the home routed national roaming architecture (depicted in Figure 4.2.4-1), FRMCS On-Board Service Clients can use FRMCS On-Board UE that is attached to MNO roaming partner's radio access. Home routed FRMCS bearers traverse both the VPLMN MNO's 5G Core and the Home FRMCS 5G core. Serving MC System's FRMCS Service Agents and wireline Service Clients are connected to the Home FRMCS Operator's domain.
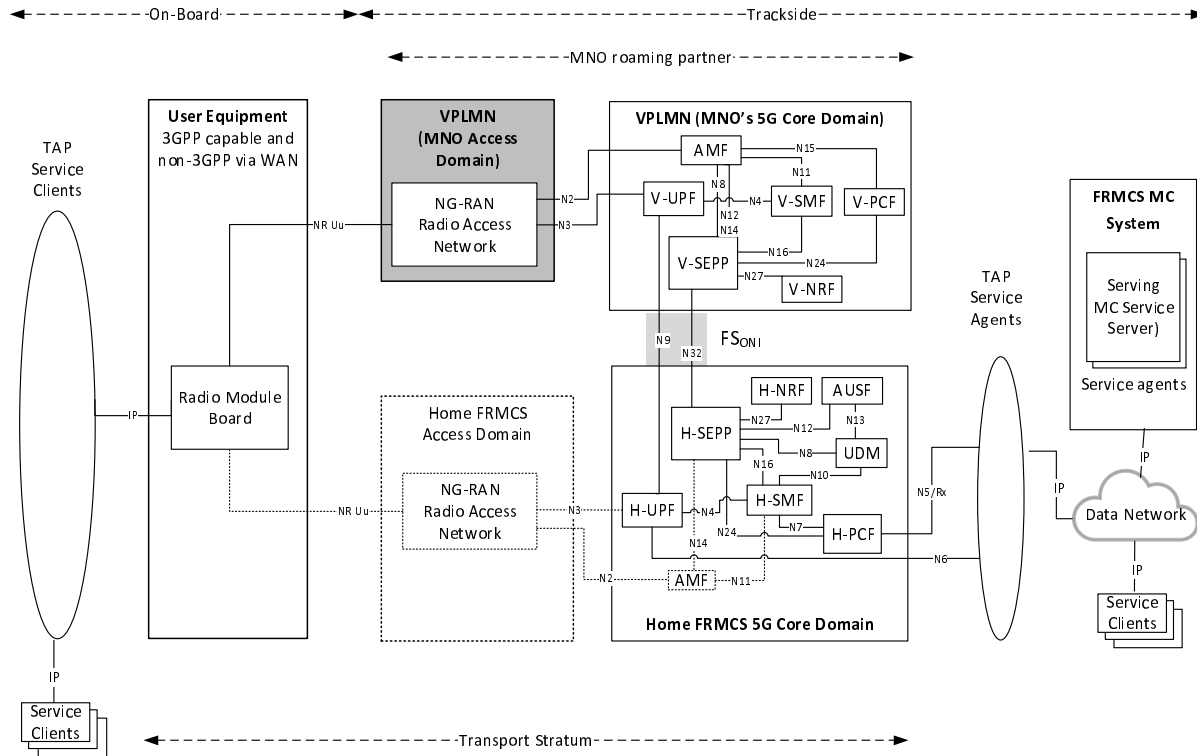
**Figure 4.2.4-1: FRMCS National Roaming Architecture
(Home Routed, as per Figure 4.2.4-6 in ETSI TS 123 501 [1])**

NOTE: N2 and N3 reference points are protected by ESP and IKEv2 certificates-based authentication as per clauses 9.2 and 9.3 in ETSI TS 133 501 [20]. IPsec is mandatory to implement on the gNodeB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

The interface functionalities and interactions between an MNO core and an FRMCS core is known as the FS_{ONI} reference point.

The following interdomain reference points shall be supported for national roaming with home routing:

- N32: Between the SEPPs of each 5G Core Domain.

- N9: Connecting visited UPF and home UPF.

4.2.5   FRMCS Roaming Architecture (Local Breakout)

In roaming architecture with Local Breakout (Figure 4.2.5-1), FRMCS On-Board Service Clients use FRMCS On-Board UE that is attached to a foreign FRMCS (LBO roaming partner's) access domain. FRMCS bearers traverse only the foreign FRMCS 5G Core. The Home FRMCS 5G core is accessed for signaling only (e.g. for UE authentication). Serving MC System's FRMCS Service Agents and wireline FRMCS Service Clients are connected to the foreign FRMCS Domain.

**Figure 4.2.5-1: FRMCS Roaming Architecture
(Local Breakout, as per Figure 4.2.4-4 in ETSI TS 123 501 [1])**

NOTE: N2 and N3 reference points are protected by ESP and IKEv2 certificates-based authentication as per clauses 9.2 and 9.3 in ETSI TS 133 501 [20]. IPsec is mandatory to implement on the gNodeB. On the core network side, a SEG may be used to terminate the IPsec tunnel.
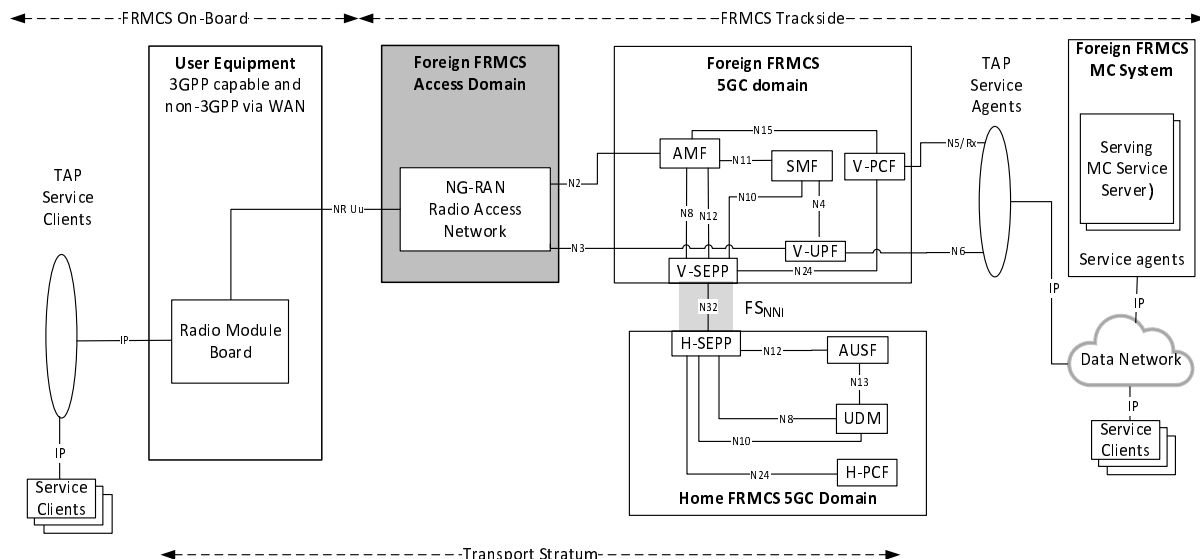
The following reference points shall be supported for roaming with LBO:

- N32: Between the SEPPs of each FRMCS Operator's 5G Core Domain.

4.3   FRMCS Transport Stratum Capabilities

4.3.1   General

For the use of the FRMCS Transport Stratum certain capabilities, e.g. UE mobility, are required encompassing one or various related functions for proper operation.

4.3.2   Access Capabilities

4.3.2.1   3GPP Radio Access

4.3.2.1.1   General

FRMCS assumes the use of a dedicated spectrum n100 and n101 (as specified in ETSI TS 103 793 [35]) as a default approach to radio coverage.

FRMCS allows the use of MNO spectrum in a MOCN configuration utilizing specific predefined shared MNO frequencies as described in clause 5.1.2.2.

One of the FRMCS system principles is to handle voice and data communications using single path and multipath. Multipath is the coordination of at least two UEs serving in parallel the same On-Board application. This is discussed in the FRMCS Multipath Function, clause 5.3 of the present document.

FRMCS allows roaming onto MNO network using the architecture specified in clause 4.2.4. Roaming onto MNO network requires the FRMCS Multipath Function to route the traffic onto FRMCS transport and non-FRMCS transport as appropriate to meet the QoS requirements of the underlying FRMCS application.

4.3.2.1.2   5G NR capabilities

For the provision of point-to-point, the corresponding 5G NR radio bearer type unicast shall be used.

For the use of radio bearers, the FRMCS Transport Domain shall support the following functional areas (see Figure 4.3.2.1.2-1):

- For the physical layer as specified in the standards ETSI TS 138 211 [11], ETSI TS 138 212 [12], ETSI TS 138 213 [13] and ETSI TS 138 214 [14]:

  - Physical resources.

  - Physical channels UL/DL.

  - Physical signals UL/DL.

  - Modulation/Demodulation.

  - Channel Coding, Multiplexing.

  - Transport Channels.

  - Physical control and procedures.

- For the data link layer as specified in the standards ETSI TS 138 321 [15], ETSI TS 138 322 [16], ETSI TS 138 323 [17] and ETSI TS 138 331 [18]:

  - Medium Access Control (MAC) for UL/DL.

  - Radio Link Control (RLC) for UL/DL.

  - Radio Resource Control.

  - Packet Data Convergence.

  - Mobility, Session, QoS.
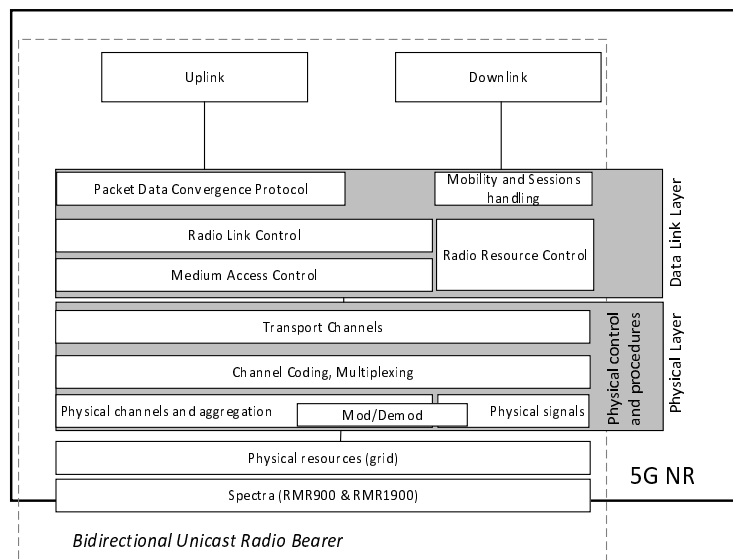
Figure 4.3.2.1.2-1: Functional areas for unicast radio bearer

4.3.3   Core capabilities

4.3.3.1   General

The FRMCS Transport Stratum Core, using the 5GC forms the connectivity layer for the FRMCS Service Stratum. 3GPP access can either be using the FRMCS Access Domain RMR spectrum or shared MNO spectrum.

Wireline access is provided by interfacing with the core Data Network. The wireline FRMCS users (e.g. VAS controllers) are outside of the Transport Domain 5G network.

4.3.3.2   3GPP NAS capabilities

5G Core capabilities are further detailed in clause 5 and shall apply for use by the FRMCS Transport Stratum.

5   FRMCS Transport Stratum Constituents

5.1   FRMCS Transport Stratum Access Domain Constituents

5.1.1   General

The access domain for FRMCS shall support one or more of the following types of wireless access networks:

- 3GPP terrestrial radio access using 5G NR radio access within FRMCS Access Domain spectrum portions controlled by a FRMCS 5GC. This type of wireless access network is specified in clause 5.1.2.1.

- 3GPP terrestrial radio access using 5G NR radio access within Mobile Network Operator (MNO) spectrum portions controlled by a FRMCS 5GC using MOCN architecture. This type of wireless access network is specified in clause 5.1.2.2.

- 3GPP terrestrial radio access using 5G NR within Mobile Network Operator (MNO) spectrum portions controlled by a FRMCS 5GC using a national roaming architecture. This type of wireless access network is out of scope of the present document.

5.1.2   FRMCS Transport Wireless Access

5.1.2.1   RMR Access

For RMR access, FRMCS Transport Domain shall comply to ETSI TS 103 793 [35], clauses 4 and 5.

For RMR access in band n101, FRMCS Transport Domain shall comply to ETSI TS 103 765-5 [36], Annex A.

5.1.2.2   MOCN Access

In MOCN access for a FRMCS operator A, a MOCN gNodeB (operated by MOCN operator B which can be an MNO operator or another FRMCS operator B) is shared between FRMCS operator A and MOCN operator B. The traffic belonging to FRMCS operator A will go to the FRMCS core network of the operator A, and the traffic belonging to operator B will go to the core network B of the operator B. The MOCN architecture maintains the same IP and QoS framework as in case where only FRMCS Access Domain access is used. The FRMCS UEs can be configured to be either both FRMCS Access Domain and MOCN capable, or MOCN capable only. The MOCN gNodeB sites broadcast the PLMN ID for the FRMCS operator A as well as PLMN ID of the operator B, whereas FRMCS Access Domain sites broadcast FRMCS PLMN ID of the FRMCS operator A exclusively. When a UE is under both FRMCS Access Domain and MOCN coverage, it constructs neighbour lists of both FRMCS Access Domain and MOCN cells and the UE can select either FRMCS Access Domain or MOCN, based on pre-configured criteria discussed in the Intra-RAT handoff described below.

Subject to the agreement in place with MOCN operator B offering MOCN shared radio resources, the FRMCS Operator A of the FRMCS Transport Domain can select between two QoS mechanisms (or both):

- 5QI flow prioritization on the MOCN bands in line with the prioritization configured in the RMR bands. This would guarantee prioritization of FRMCS traffic over mobile broadband traffic using the MOCN shared radio resources.

- Partitioning the MOCN band so that the FRMCS traffic is isolated for mobile broadband traffic in usage of radio resource blocks. This would guarantee that FRMCS traffic would have exclusive use of radio resources in the MOCN band. In addition, the 5QI flows can be configured in the FRMCS core to apply only on the FRMCS partition of the shared radio access.

The standards referenced in ETSI TS 138 331 [18] and ETSI TS 138 413 [i.4] to ETSI TS 136 423 [i.8] are applicable to MOCN.

5.2   FRMCS Transport - Core

5.2.1   Core Architectural Element and Functions

5.2.1.1   Access and Mobility Management Function (AMF)

The Access and Mobility Management Function (AMF) is specified in ETSI TS 123 501 [1], clause 6.2.1.

The AMF is responsible for providing the following capabilities in FRMCS:

a)   Termination of interfacing with RAN Control Plane.

b)   Termination of NAS, NAS ciphering and integrity protection.

c)   Registration management.

d)   Connection management.

e)   Reachability management.

f)   Mobility Management; Provide transport for Session Management messages between UE and SMF.

g)   Transparent proxy for routing of Session Management messages.

h)   Access Authentication.

i)   Access Authorization.

j)   Location Services management and transport.

k)   UE mobility event notification.

The AMF is required to support the following cybersecurity functionalities:

a)   Signalling data confidentiality.

b)   Signalling data integrity.

c)   Subscriber privacy.

NOTE: In order to protect the N2 and N3 reference points, it is required to implement IPsec ESP and IKEv2 certificates-based authentication, see clauses 9.2 and 9.3 in ETSI TS 133 501 [20]. IPsec is mandatory to implement on the gNodeB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

In a FRMCS Domain, the AMF shall support at least the following reference points:

- **N1:** The reference point between the AMF and the UE. It is used for signaling and management, including authentication and security procedures. N1 messages are delivered to the AMF via the gNodeB through the N2 reference point (hence not depicted in architecture diagrams).

- **N2:** The reference point between the AMF and the RAN (gNodeB). It is used for connection management, UE context management, and PDU session management.

- **N8:** The reference point between the AMF and the UDM. It is used to retrieve user data and crucial during the user registration process.

- **N11:** The reference point between the AMF and the SMF. It Is used for session management and mobility handling.

- **N12:** The reference point between the AMF and the AUSF. It is used for exchange of authentication-related data between the two NFs.

- **N14:** The reference point between the two AMF instances. It is used to transfer User Equipment (UE) context during events like handovers, ensuring seamless mobility between cells managed by different AMFs.

- **N15:** The reference point between AMF and the PCF. It is used to exchange information about policy control and access management.

5.2.1.2   Session Management Function (SMF)

The Session Management Function (SMF) is specified in ETSI TS 123 501 [1], clause 6.2.2.

The SMF is responsible for providing the following capabilities in FRMCS:

a)   Session Management.

b)   UE IP address allocation & management.

c)   Selection and control of User Plane Function.

d)   Configures traffic steering at UPF to route traffic to proper destination.

e)   Termination of interfacing with Policy Control Functions.

f)   Charging data collection and interfacing support with charging.

g)   Termination of Session Management parts of NAS messages.

h)   Downlink Data Notification.

i)   Determine Session and Service Continuity mode of a session.

j)   Provisioning of external parameters (Expected UE Behaviour parameters or Network Configuration parameters).

k)   Support P-CSCF discovery for IP Multimedia Subsystem (IMS) services.

If roaming is enabled for a UE, the SMF is responsible for providing the following capabilities in FRMCS:

a)   Roaming functionality.

b)   Handle local enforcement to apply QoS SLAs (in the VPLMN).

c)   Charging data collection and charging interface (in the VPLMN).

If Lawful Intercept is applicable, the SMF facilitates Lawful intercept (in coordination with the UPF and the LIF).

In a FRMCS Domain, the SMF shall support at least the following reference points:

- **N4:** The reference point between the SMF and the UPF. It is used for managing and establishing user data plane sessions.

- **N7:** The reference point between the SMF and the PCF. It is used for the exchange of session management policy information corresponding to the PDU session of the UE.

- **N10:** The reference point between the SMF and the UDM. It is used to exchange subscriber data and the UE context information for SMF to manage sessions based on the subscriber's profile and policies defined by the UDM.

- **N11:** The reference point between the SMF and the AMF. It Is used for session management and mobility handling.

5.2.1.3   User Plane Function (UPF)

The User Plane Function (UPF) is specified in ETSI TS 123 501 [1], clause 6.2.3.

The UPF is responsible for providing the following capabilities for FRMCS:

a) Packet routing and forwarding.

b) Packet inspection.

c) QoS handling.

d) Traffic usage reporting.

e) Acts as external PDU session point of interconnect to Data Network (DN).

f) Serves as the anchor point for intra- and inter-RAT mobility.

If Lawful Intercept is applicable, the UPF facilitates Lawful intercept for User Plane data collection.

In a FRMCS Domain, the UPF shall support at least the following reference points:

- **N3:** The reference point between the RAN (gNodeB) and the (initial) UPF.

- **N4:** The reference point between the Session Management Function (SMF) and the UPF.

- **N6:** The reference point between the Data Network (DN) and the UPF.

- **N9:** The reference point between two UPFs (i.e. the Intermediate I-UPF and the UPF Session Anchor).

UPFs can be deployed in series and connected via a reference point referred to as N9. There are three main use cases for this:

- Network-wide mobility - To provide full mobility with a stable IP anchor across the full network, there may be a need to connect two UPFs depending on the IM network configuration.

- Break-out of selected data flows -Ability to apply classification and traffic management in the UPF to selectively send IP packets to different IP destination, for example, to terminate some traffic at, or close to, the edge to ensure low data latency or prevent sensitive data from being intercepted in more central areas of the network. This requires two UPFs connected in series.

- Roaming with home routing - 5G roaming is referred to as N9 home routing (N9HR) and is needed for some FRMCS applications (e.g. TCMS).

NOTE: In order to protect the N2 and N3 reference points, it is required to implement IPsec ESP and IKEv2 certificates-based authentication, see clauses 9.2 and 9.3 in ETSI TS 133 501 [20]. IPsec is mandatory to implement on the gNodeB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

5.2.1.4   Policy Control Function (PCF)

The Policy Control Function (PCF) is specified in ETSI TS 123 501 [1], clause 6.2.4.

The PCF is responsible for providing the following capabilities in FRMCS:

a) Unified policy framework.

b) Policy rules to CP functions.

c) Access subscription information for policy decisions in UDR.

In a FRMCS Domain, the PCF shall support at least the following reference points:

- **N5** or **Rx:** The reference point between the AF and the PCF. In FRMCS, the AF is either the MC Service Server or the P-CSCF in the FRMCS SIP or IMS Core.

- **N7:** The reference point between the PCF and the SMF. It is used for the exchange of session management policy information corresponding to the PDU session of the UE.

- **N15:** The reference point between the PCF and the AMF. It is used to exchange information about policy control and access management.

- **N24:** The reference point between the vPCF and the hPCF. It is used in roaming architectures for exchange of the policies information for the subscriber session.

5.2.1.5 Authentication Server Function (AUSF)

The Authentication Server Function (AUSF), as defined in ETSI TS 123 501 [1], clause 6.2.8, shall be implemented in FRMCS.

The AUSF is responsible for providing the following capabilities in FRMCS:

a) Supports authentication for 3GPP access, as specified in ETSI TS 133 501 [20].

In a FRMCS Domain, the AUSF shall support at least the following reference points:

- **N12:** The reference point between the AUSF and the AMF. It is used for exchange of authentication-related data between the two NFs.

- **N13:** The reference point between the AUSF and the UDM. It is used by AUSF to request the authentication vectors from the UDM and for the UDM to provide these vectors to the AUSF.

5.2.1.6 Unified Data Management (UDM)

The Unified Data Management (UDM) is specified in ETSI TS 123 501 [1], clause 6.2.7.

The UDM is responsible for providing the following capabilities in FRMCS:

a) Generation of Authentication and Key Agreement (AKA) credentials for UEs.

b) UE User identification handling.

c) UE Access authorization.

d) UE Subscription management.

In a FRMCS Domain, the UDM shall support at least the following reference points:

- **N8:** The reference point between the UDM and the AMF. It is used to communicate user data crucial for the user registration process.

- **N10:** The reference point between the UDM and the SMF. It is used to exchange subscriber data and the UE context information for SMF to perform session management based on the subscriber's profile and policies defined by the UDM.

- **N13:** The reference point between the AUSF and the UDM. It is used by AUSF to request the authentication vectors from the UDM and for the UDM to provide these vectors to the AUSF.

5.2.1.7 Unified Data Repository (UDR)

The Unified Data Repository (UDR) is specified in ETSI TS 123 501 [1], clause 6.2.11.

The following functions are supported in the UDR:

a) Storage and retrieval of subscription data by the UDM.

b) Storage and retrieval of policy data by the PCF.

c) Storage and retrieval of application-related data (including of Packet Flow Descriptions (PFDs) for application detection).

5.2.2 Conditional Core Architectural Elements

5.2.2.1 General

In addition to the minimal architectural components listed in clause 4.2.2, the FRMCS core architecture may require the following conditional architectural components. These components are not mandatory in the minimized FRMCS architecture. They may be required to fulfil national rules or to enhance the operation of FRMCS.

5.2.2.2 5G-Equipment Identity Register (5G-EIR)

The 5G-Equipment Identity Register (5G-EIR) is used to check the status of equipment's identity (e.g. to check that it has not been listed as unauthorized or stolen). If the FRMCS Operator implements 5G-EIR, it shall be implemented according to ETSI TS 129 511 [26] and ETSI TS 123 502 [10]. This element is conditional on national rules requiring that mobile equipment be checked against a prohibited mobile equipment list before a signalling connection is allowed.

The reference point N17 (see Figure 5.2.2.2-1) shows the interaction between the 5G-EIR and the Access and Mobility Function (AMF) enabling the check of the status of the mobile equipment identity.
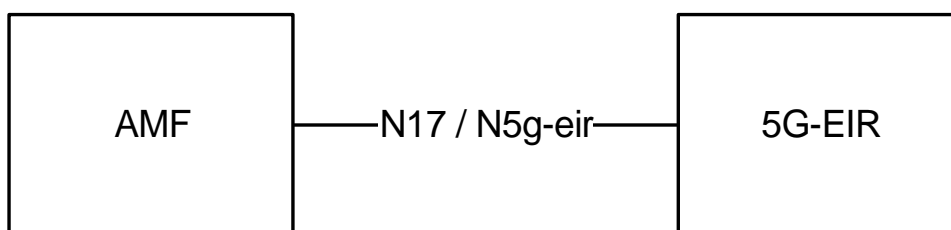
Figure 5.2.2.2-1: Reference Model - N5g-eir

During any procedure establishing a signalling connection with the UE, the network may perform a mobile equipment and identity check with 5G-EIR via the N5g-eir_Equipment Identity Check Service exhibited by 5G-EIR.

5.2.2.3 Network Exposure Function (NEF)

The usage of Network Exposure Function (NEF) is conditional on the requirement to connect the FRMCS Transport Domain to additional Core Application Functions (AF) other than the MC Service Server.

The NEF securely exposes network capabilities and events provided by 3GPP Network Functions to Application Functions.

The NEF provides means for securely provisioning of information from AF to 3GPP network and may authenticate, authorize and assist in throttling the AF. The NEF translates information exchange between the AF and internal 3GPP NFs. The usage of NEF is left to Infrastructure Manager, and it is subject to cyber security policies of the FRMCS operator.

If the FRMCS Operator implements NEF, the NEF APIs shall be implemented according to ETSI TS 129 522 [19] and NEF Services as per ETSI TS 129 591 [37].

5.2.2.4 Network Repository Function (NRF)

The Network Repository Function (NRF) is specified in ETSI TS 123 501 [1], clauses 6.2.6, 6.3.26 and 7.2.6. The NRF provides a centralized repository for all the 5G Network Functions (NFs) in the FRMCS Transport Domain. The NRF allows 5G NFs to register and discover each other via a standards-based API.

5.2.2.5 Binding Support Function (BSF)

The Binding Support Function (BSF) is conditional on the need for a geo-redundant 5G core configuration. The Binding Support Function is used to bind sessions with the correct PCF instances.

If FRMCS Operator implements BSF, it shall be implemented according to ETSI TS 123 501 [1], clause 7.2.15.

5.2.2.6   Service Communication Proxy (SCP)

The Service Communication Proxy (SCP) is conditional on the need for a geo-redundant 5G core configuration or for other functions specified ETSI TS 123 501 [1], clause 6.2.19. It is used in geo-redundant 5G core configurations to provide functionalities such as message forwarding and routing, Delegated Discovery, Indirect Communication, load balancing and distribution between the geo-redundant cores or local 5G core network elements.

If FRMCS operator implements SCP, it shall be implemented according to ETSI TS 123 501 [1], clause 6.2.19 and clause 6.3.16.

5.2.2.7   Security Edge Protection Proxy (SEPP)

The Security Edge Protection Proxy (SEPP) is specified in ETSI TS 123 501 [1], clause 6.2.17.

5.3   FRMCS Multipath Function

5.3.1   General

The FRMCS Multipath Function distributes incoming Multipath Dataflows across one or multiple Multipath Datapaths according to available Multipath Datapaths and Multipath Policy. The FRMCS Multipath Function can make use of Multipath Datapaths over a FRMCS Transport Domain or over a Non-FRMCS Transport Domain.

The FRMCS Multipath Function is a distributed function split between a Multipath Client and a Multipath Gateway.

The Multipath Client within an On-Board FRMCS can make use of available On-Board FRMCS Radio Modules and other On-Board Radio Modules attached to a single Transport Domain or to multiple Transport Domains.

Subject to Multipath Policy, a Multipath Dataflow can be transparently allocated by the FRMCS Multipath Function to a single Multipath Datapath or be allocated, sequentially or simultaneously, to multiple Multipath Datapaths.

NOTE: "Transparently" is to be understood as a feature of the FRMCS Multipath Function which lets the application access a communication resource through a defined interface without having to know the details of the resource or underlaying communication network(s). It is to be understood in the common sense that the underlying network is invisible to the application.

The FRMCS Multipath Function requires the underlying Transport Domain to provide IP service connections. Transport Domains used by the FRMCS Multipath Function is the 3GPP based 5G network as defined in clause 4 but can explicitly include also other 3GPP based or non-3GPP based transport networks.

5.3.2   FRMCS Multipath Function capability

The FRMCS Multipath Function supports the following features:

- Multipath Datapath selection, i.e. determination of one or more eligible Multipath Datapaths based on evaluation of the Multipath Policy associated to a Multipath Dataflow.

- QoS control, i.e. conveyance of QoS requirements to associate to a Multipath Datapath if supported by its Transport Domain.

- Multipath Datapath switching, i.e. change the allocation of a Multipath Dataflow from one Multipath Datapath to another Multipath Datapath.

- Multipath Datapath splitting, i.e. distribute the packets of a Multipath Dataflow across multiple Multipath Datapaths.

- Multipath Datapath duplication, i.e. duplicate the packets of a Multipath Dataflow across multiple Multipath Datapaths.

5.3.3 Architecture

Figure 5.3.3-1 and Figure 5.3.3-2 illustrate the functional architecture of the FRMCS Multipath Function.

It is constituted of two functions, the Multipath Client and the Multipath Gateway.

The Multipath Client and the Multipath Gateway are connected via two reference points:

- FS_{MPM} which enables the FRMCS Multipath control plane function, including Multipath Gateway discovery, information exchange on available Multipath Datapaths.

- FS_{MPU} which enables the user plane transport of a Multipath Dataflow based on a Multipath Protocol over one or more Multipath Datapaths.

NOTE: The protocol details of FS_{MPM} are not specified in the present document.

On the client side, a Multipath Dataflow ingresses/egresses the Multipath Client via the TAP Service Clients and ingresses/egresses the Multipath Gateway via the TAP Service Agents.
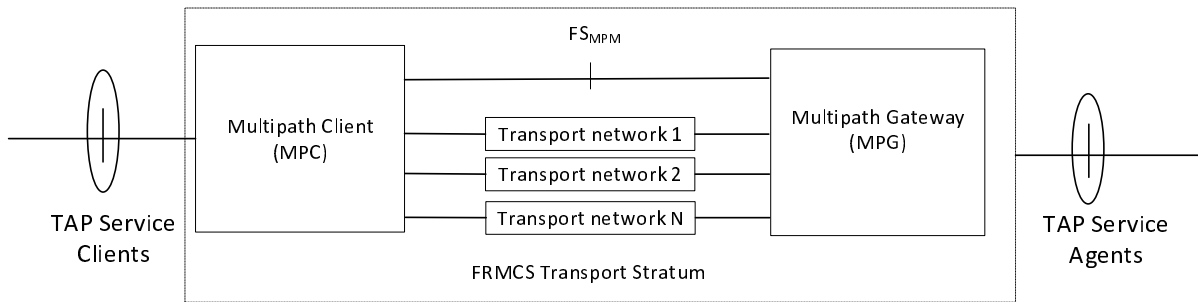
Figure 5.3.3-1: Functional architecture of the FRMCS Multipath Function
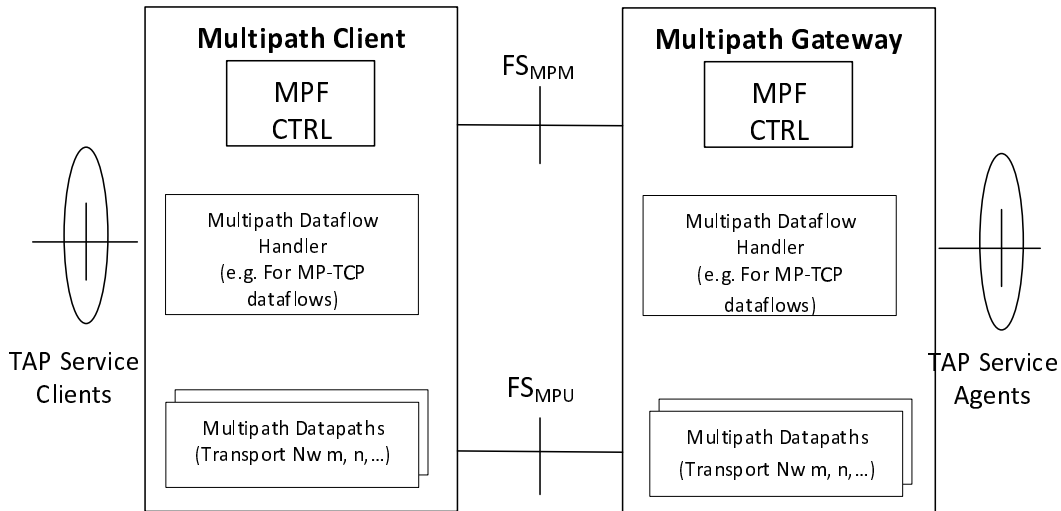
Figure 5.3.3-2: Functional architecture of Multipath Client and Multipath Gateway

The Multipath Client enables the interaction with TAP Service Clients that represents FRMCS Service Client(s) in Figure 4.1-1 of ETSI TS 103 765-2 [6].

The Multipath Gateway enables the interaction with the TAP Service Agents. The TAP Service Agent is responsible to forward control information and user plane traffic from the FRMCS service control layer to the Multipath Gateway.

The Multipath Gateway and Multipath Client are logical entities which contain the following functional entities:

- One MPF-CTRL, i.e. the function within the entity responsible for control functions (discovery, negotiation, instantiation of Multipath Dataflow Handlers, etc.).

- One or more Multipath Dataflow Handlers, i.e. the function instances implementing a specific Multipath Protocol between a Multipath Client and a Multipath Gateway.

5.3.4   Multipath Gateway

The MPF-CTRL function of Multipath Gateway has the following responsibilities:

- Control of multipath setup between a Multipath Client and the Multipath Gateway.

- Instantiation of Multipath Dataflow Handlers.

- Handling of IP Address management for each Multipath Dataflow Handler.

- Allocation of each Multipath Dataflow to a Multipath Dataflow Handler instance.

- Configure a Multipath Dataflow Handler for handling of a Multipath Dataflow.

- Implementation of a N5/Rx/N33 QoS Proxy:

  - To handle incoming QoS requests via the TAP service Agent and forward the appropriate QoS Requests towards the associated Transport Domain(s) via the TAP Transport Core Network CP.

  - To modify/duplicate forwarded QoS requests to reflect the selected set of Multipath Datapaths associated to a Multipath Dataflow.

A Multipath Gateway's Multipath Dataflow Handler has the following responsibilities:

- Steer a Multipath Dataflow over one or more Multipath Datapaths as configured by the MPF-CTRL of Multipath Gateway.

- Duplicate or stop the duplication of the packets of a Multipath Dataflow across multiple Multipath Datapaths as configured by the MPF-CTRL of Multipath Gateway.

- Add and remove Multipath Datapaths as configured by the MPF-CTRL of Multipath Gateway or as a result of detecting availability/unavailability of Multipath Datapaths.

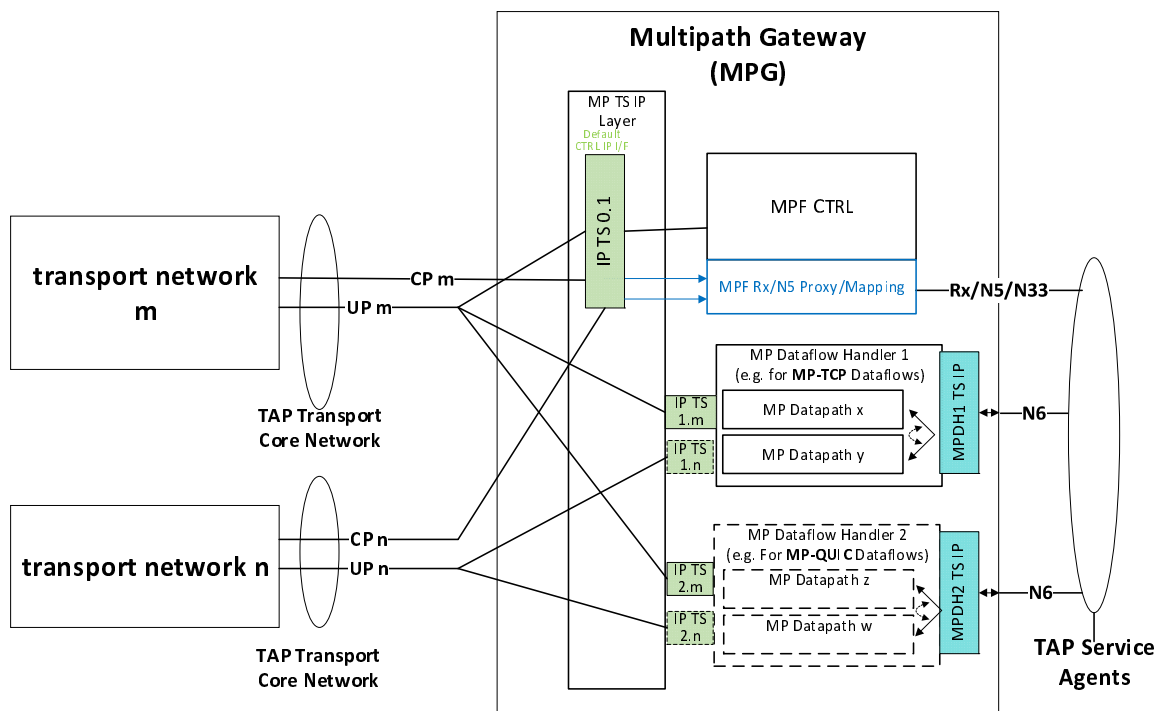Figure 5.3.4-1 illustrates the functional architecture of the Multipath Gateway.

Figure 5.3.4-1: Multipath Gateway
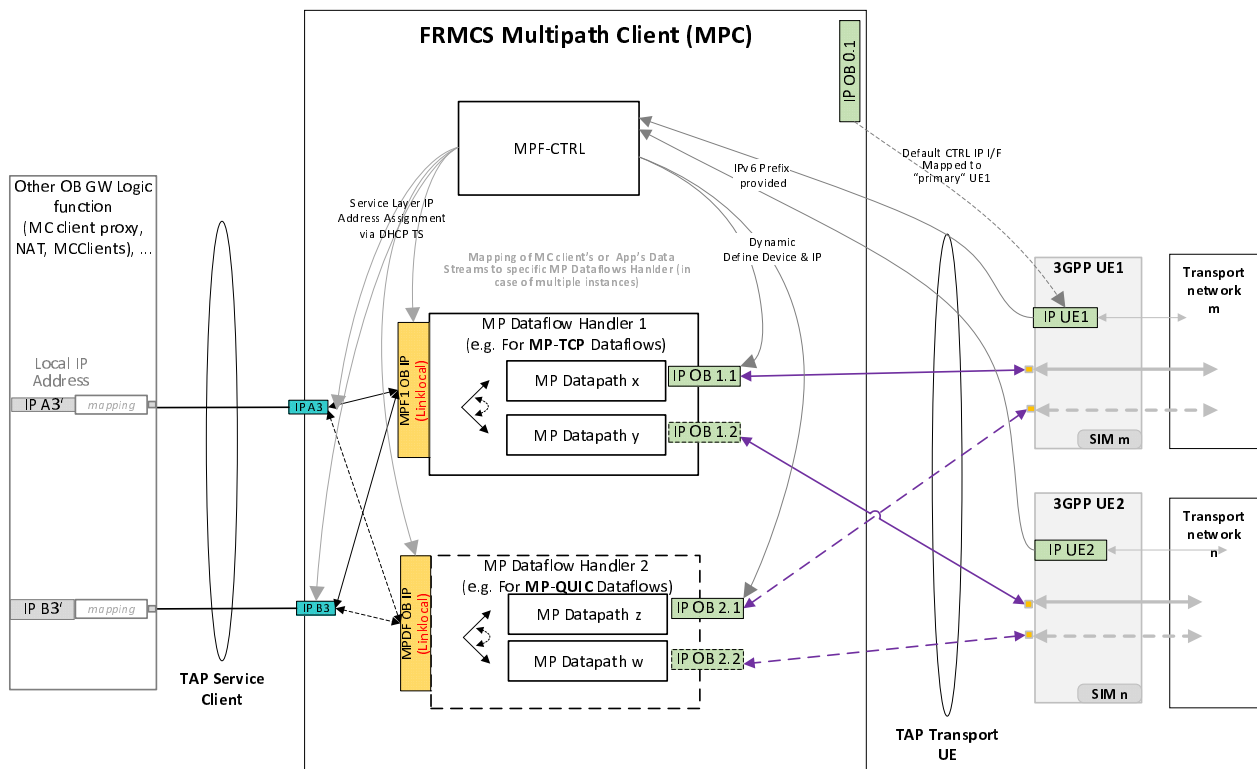
5.3.5   Multipath Client

The MPF-CTRL function in the Multipath Client has the following responsibilities:

- Control of multipath setup between the Multipath Client and a Multipath Gateway, based on control information received from the Multipath Gateway.

- Instantiation of Multipath Dataflow Handlers, based on control information received from the Multipath Gateway.

- Handling of IP Address management for each Multipath Dataflow Handler.

- Allocation of each Multipath Dataflow to a Multipath Dataflow Handler instance.

- Configure Multipath Dataflow Handler instance for handling of a Multipath Dataflow.

- Send to Multipath GW the transport identities of the underlying transport paths under its control.

A Multipath Client Multipath Dataflow Handler has the following responsibilities:

- Steer a Multipath Dataflow over one or more Multipath Datapath as configured by the MPF-CTRL of the Multipath Client.

- Duplicate or stop the duplication of the packets of a Multipath Dataflow across multiple Multipath Datapaths as configured by the MPF-CTRL of the Multipath Client.

- Add and remove Multipath Datapaths as configured by the MPF-CTRL of the Multipath Client or as a result of availability/unavailability of Multipath Datapaths.

Figure 5.3.5-1 illustrates the functional architecture of the Multipath Client.

Figure 5.3.5-1: Multipath Client

In Figure 5.3.5-1, the MPF-CTRL of Multipath Client manages control plane exchanges with the MPF-CTRL of Multipath Gateway over the FS_{MPM} reference point. At least one On-Board Radio Module needs to be available to enable those exchanges. In case of unavailability the On-Board Radio Module used to support the FS_{MPM} reference point, the On-Board FRMCS shall switch to another On-Board Radio Module.

The MPF-CTRL of Multipath Client also determines which On-Board Radio Module(s) is used for the FS_{MPU} reference point for a given Multipath Dataflow, based on exchanges with the MPF-CTRL of Multipath Gateway.

5.3.6   IP Address Assignment

IP Address assignment is required:

    a)   for public service layer IP address for each Multipath Dataflow Handler; and

    b)   for each transport domain Multipath Datapath for each Multipath Dataflow Handler.

The 5G Core provides IPv6 prefix during the initial default data connection establishment to each UE. The procedure is IPv6 Prefix Delegation. The IPv6 prefix is assigned via DHCPv6.

As illustrated in Figure 5.3.5-1 (Multipath Client), the transport-related IP addresses on the OB side (IP OB 1.1, IP OB 2.1, etc.) are appended with this prefix. The IPv6 prefix is delegated from the 5G Core directly, thus the IP addresses, that are part of the prefix, are reachable and routable from the 5G Core to the correct UE.

The Multipath Client uses the given IPv6 prefix from the 5GC/UE to define the full transport related IP address on the Multipath Client's side (IP OB 1.1, IP OB 2.1, etc.) by IPv6 stateless autoconfiguration:

- The transport-related IP addresses on the Multipath Client's side (IP OB 1.1, IP OB 2.1, etc.) are defined locally on the Multipath Client. These IP addresses shall be propagated to the Multipath Gateway so that the Multipath Gateway can populate the mapping table for each Multipath Dataflow Handler to map the correct trackside transport Multipath Datapath IP address to the On-Board transport IP Multipath Datapath address.

- The MPF-CTRL of Multipath Client shall assign the IPv6 addresses to the TAP Service Clients interfaces. They may be public addresses (e.g. Global Unicast Addresses, GUA) or Link-Local addresses, based on the specific address plan in use.

5.3.7   FRMCS Multipath Function procedures

5.3.7.1   FRMCS Multipath Function discovery procedure

The FRMCS Multipath Function discovery procedure allows a Multipath Client to discover the presence of a Multipath Gateway within a FRMCS Transport Domain.

The following high-level steps are undertaken:

    1)   The MPF-CTRL of Multipath Client shall select a default connection mapped to a locally selected On-Board FRMCS Radio Module on the FRMCS Transport Domain to be used in the following steps for IP connection between the MPF-CTRL of Multipath Client and the MPF-CTRL of Multipath Gateway. The default connection shall use a predefined default QoS setting on the transport network:

        a)   If the default connection over the FRMCS Transport Domain is not available, the next available other transport domain connection shall be used by the Multipath Client.

    2)   The MPF-CTRL of Multipath Client shall use a configured DNS server IP address and send a DNS request towards the trackside to resolve a predefined generic FQDN representing the next available Multipath Gateway.

    3)   If the generic FQDN representing the next available Multipath Gateway can be successfully resolved, an IP address for the Multipath Gateway will be received by the Multipath Client:

        a)   The Multipath Client shall negotiate the multipath capabilities with the Multipath Gateway as specified in clause 5.3.7.3.

        b)   The Multipath Gateway shall negotiate the multipath capabilities with the Multipath Client as specified in clause 5.3.7.3.

    4)   If the generic FQDN representing the next available Multipath Gateway is not successfully resolved or no response to the DNS query is received by the Multipath Client, the latter shall execute the FRMCS Multipath Function fallback procedure as specified in clause 5.3.7.5.

5.3.7.2   FRMCS Multipath Function Multipath Datapaths handling and selection procedure

Once the discovery procedure in clause 5.3.7.1 is successful:

Multipath Client:

1)   shall allocate transport domain IP Addresses for each Multipath Datapath for each Multipath Dataflow Handler based on one of the methods specified in clause 5.3.6;

2)   shall allocate public service layer IP Addresses for each Multipath Dataflow based on one of the methods specified in clause 5.3.6;

3)   shall instantiate a Multipath Dataflow Handler for each Multipath Dataflow it receives from the TAP service agent.

Multipath Gateway:

1)   shall allocate public service layer IP Addresses for each Multipath Dataflow based on one of the methods specified in clause 5.3.6;

2)   shall allocate transport domain IP Addresses for each Multipath Datapath for each Multipath Dataflow Handler based on one of the methods specified in clause 5.3.6, this assignment shall correspond to the number of Multipath Datapaths defined at the Multipath Client for each Multipath Dataflow Handler;

3)   shall instantiate a Multipath Dataflow Handler for each Multipath Dataflow it receives from the MPF-CTRL of Multipath Client.

The Multipath Datapath selection shall be executed by the Multipath Dataflows Handler based on application specific Multipath policy and capability negotiation in clause 5.3.7.3.

5.3.7.3   FRMCS Multipath Function capability negotiation procedure

The FRMCS Multipath Function capability negotiation procedure is executed between a Multipath Client and a Multipath Gateway. The Multipath Gateway shall determine the parameters and Multipath Policy used.

The following multipath capability negotiation shall apply on a per Multipath Dataflow Handler basis:

1)   Multipath Protocol decision:

Table 5.3.7.3-1 lists possible results of multipath capability negotiation.

Table 5.3.7.3-1: Possible outcomes of multipath capability negotiation

Description	Comment
MP-NONE	No Multipath Gateway function is supported or shall be used for this Multipath Dataflow, and traffic shall be steered via Multipath Client autonomously or not at all if only one On-Board Radio Module is used
MP-TCP	Multipath Dataflow Handler supports MP-TCP
MP-QUIC	Multipath Dataflow Handler supports MP-QUIC
MP-Tunnel Only	Multipath Gateway provides only tunnel termination with no control over path selection
NOTE: MP-Tunnel Only is intended for the case when no multipath control is present. It is used to set up a tunnel for failover and packet duplication use cases where QoS control is not needed.	

The Multipath Client shall provide the information about the On-Board FRMCS Radio Modules available for control including their operating bands and IMSI towards the Multipath Gateway.

The Multipath Gateway shall provide in the response a single value which represents the selected Multipath method and Multipath Protocol to be used. The Multipath Client shall respect the method provided by the Multipath Gateway.

The Multipath Gateway shall provide the Multipath Client with policy control regarding the use of the UEs under the Multipath Client's control.

2)   QoS requirements:

The Multipath Client shall indicate the QoS requirements via a string value.

The Multipath Client provides the Communication Category value as provided via OB$_{APP}$ API (communicationCategory::= UTF8String()), as per FRMCS FFFIS-7950 [8], A.2 OB$_{APP}$ parameters, and ETSI TS 103 765-3 [7], clause 7.3.2.1.

The multipath capability negotiation shall be performed via HTTP/2-based REST protocol. The Multipath Gateway acts as HTTP/2 server and the Multipath Client acts as HTTP/2 client:

- HTTP/2, as defined in IETF RFC 9113 [21], shall be used.

- The data contained in the body of HTTP request; HTTP response shall be encoded in JSON as specified in IETF RFC 8259 [22].

The use of the JSON format shall be signalled by the content type *application/json.*

5.3.7.4   FRMCS Multipath Function capability definition procedure

If the selected Multipath Protocol decided during Multipath capability negotiation as per clause 5.3.7.3 Point 1 is MP-TCP, the MP-TCP protocol shall be implemented according to IETF RFC 8684 [27].

If the selected Multipath protocol decided during Multipath capability negotiation as per clause 5.3.7.3 Point 1 is MP-QUIC, the MP-QUIC protocol shall be implemented according to the following definitions:

- QUIC layer as defined in ETSI TS 123 501 [1], clause 5.32.6.2.2, Item 3) "QUIC layer"

Usage of Datagram mode 1 as defined in ETSI TS 123 501 [1], clause 5.32.6.2.2.1, and ETSI TS 124 193 [28], clause 6.4.2 which is using QUIC Datagram frames with unreliable transport but with sequence numbering, packet reordering and congestion control.

5.3.7.5   FRMCS Multipath Function fallback procedure

The FRMCS Multipath Function fallback procedure shall be executed if the Multipath Client does not get a valid response on the DNS query. This is considered as an indication that there is no trackside MPF available or that it shall not be used. In this case, the IP assignment as per clause 5.3.6 shall be used.

5.3.7.6   FRMCS Multipath Function cleanup procedure

The following steps are undertaken:

1) For each Multipath Dataflow of the Multipath Client, the procedure in clause 5.3.7.7 shall be performed.

2) The Multipath Gateway shall release the Multipath Dataflows Handler.

5.3.7.7   Release of FRMCS Multipath Dataflow

The following steps are undertaken:

1) The Multipath Client shall request the release of the Multipath Dataflow.

2) The Multipath Gateway shall perform the release of Multipath Dataflow.

6   Transport Stratum Procedures

6.1   On-Board Radio Module Registration Procedure

Upon selection by the On-Board FRMCS of a FRMCS Transport Domain to register to, the On-Board FRMCS Radio Module shall execute the network selection, ETSI TS 123 501 [1], clause 5.2.2. PLMN selection procedure in "manual network selection" mode as specified in ETSI TS 123 122 [38], clause 4.2 towards the designated FRMCS Transport Domain shall be followed.

The On-Board FRMCS Radio Module shall perform UE Initial Registration to the designated FRMCS Transport Domain as specified in ETSI TS 123 501 [1], clause 5.3, Registration and Connection Management and in ETSI TS 123 502 [10], clause 4.2. The Initial Registration procedure involves execution of Network Access Control functions as defined in clause 5.2 (i.e. user authentication and access authorization based on subscription profiles in UDM). The On-Board FRMCS Radio Module uses the identities stored in the SIM profile (SUPI/SUCI using IMSI identifier).

6.2 Transport path establishment for Mission Critical signalling procedure

The On-Board FRMCS Radio Module shall execute the "UE Requested PDU Session Establishment" procedure as specified in ETSI TS 123 502 [10], clause 4.3.2.2. It covers both the non-roaming and roaming case with LBO case (clause 4.3.2.2.1in ETSI TS 123 502 [10]) and the Home-Routed roaming case (clause 4.3.2.2.2 in ETSI TS 123 502 [10]).

MC signalling is assigned a transport bearer with higher prioritization. The standard 5QI for Mission Critical delay sensitive signalling (e.g. MCPTT signalling, MC Video signalling) is 69. Policy control decision in FRMCS is enabled by dynamic service input provided by the MC Service Server to the PCF through reference point Rx or N5. This may be direct or via the FRMCS SIP Core.

The SMF receives policy rules from the PCF via N7 and sends instructions for QoS enforcement, traffic steering and charging control via N4 to the UPF. The UPF enforces the rules via Packet Detection Rules (PDRs) and forwarding actions.

6.3 On-Board Radio Module deregistration procedure

The On-Board FRMCS Radio Module shall execute the "UE-initiated Deregistration" procedure as specified in ETSI TS 123 502 [10], clause 4.2.2.3.2.

6.4 Roaming Home-Routed Transport Path Establishment

In the Home-Routed case, the On-Board FRMCS Radio Module shall execute the "UE Requested PDU Session Establishment" procedure as specified in ETSI TS 123 502 [10], clause 4.2.3.2.2.

This procedure is typically used in FRMCS to:

- Enable roaming of a UE onto an MNO network with home routing to the Home FRMCS Domain (National Roaming with only home routing).

- Enable roaming of a UE onto a foreign FRMCS Domain where home routing to the Home FRMCS Domain is necessary:

    - In Inter-FRMCS-Domain Transition.

    - In use cases where home routing to the Home FRMCS Domain is desirable (such as an application of Application Type IV).

6.5 Release of transport path

If the transport path is a Multipath Dataflow, the procedure in clause 5.3.7.7 shall be performed.

If the transport path is not a Multipath Dataflow, the UE-requested PDU session release as specified in ETSI TS 123 502 [10], clause 4.3.4 shall be performed.

7   Interaction of Service Stratum and Transport Stratum

The ETSI reference point to be used for interaction between the transport stratum and service stratum including FRMCS SIP core as defined in ETSI TS 103 765-2 [6] and in ETSI TS 123 501 [1], clause 6.2.10.

The following functions are supported between the transport stratum and service stratum:

a)   Interacting with the 5G Policy framework for policy control (PCF).

b)   Interactions of the FRMCS SIP Core and HTTP connection for MC signalling with the 5G Core via the Data Network (DN).

8   FRMCS Transport Stratum Quality of Service Framework

8.1   FRMCS Quality of Service Principles

The FRMCS Transport Stratum QoS framework is based on the following principles:

a)   QoS is applied via PDU sessions (up to 15 per UE) and QoS flows (up to 63 per PDU session).

b)   QoS is enforced at UE, gNodeB and UPF based on rules propagated from the UDM/PCF or pre-configured.

c)   QoS policy is controlled from the FRMCS service stratum via messaging over reference points Rx or N5.

d)   The gNodeB can map multiple QoS flows with similar characteristics to a single Data Radio Bearer (DRB).

e)   QoS flows can be of type GBR (Guaranteed Bit Rate), non-GBR and delay critical GBR.

f)   Each QoS flow is associated with a QoS profile, including:

   i)   A QFI (QoS Flow identifiers) based on 5QI.

   ii)   An ARP (Allocation & Retention Priority).

   iii)   Type specific & optional parameters.

IP data is mapped (filtered) to QoS flows at UE (based on QoS rules) and UPF utilizing packet filter sets.

The FRMCS Application Function (AF), defined in ETSI TR 103 791 [i.1], shall perform mapping from a Session Description Information (SDI), received within the AF session signalling, to service information passed to the PCF over the N5 or Rx reference points as per ETSI TS 129 513 [24].

The FRMCS AF shall signal the PCF to request resources for media bearers using one of the following options:

i)   as per ETSI TS 123 289 [23], clause 7.2.2 (see step 3 in Figure 8.1-1) if the FRMCS SIP Core represents the FRMCS AF; or

ii)   as per ETSI TS 123 289 [23], clause 7.2.3.2 if the MC Service Server represents the FRMCS AF (see step 6 in Figure 8.2-2).
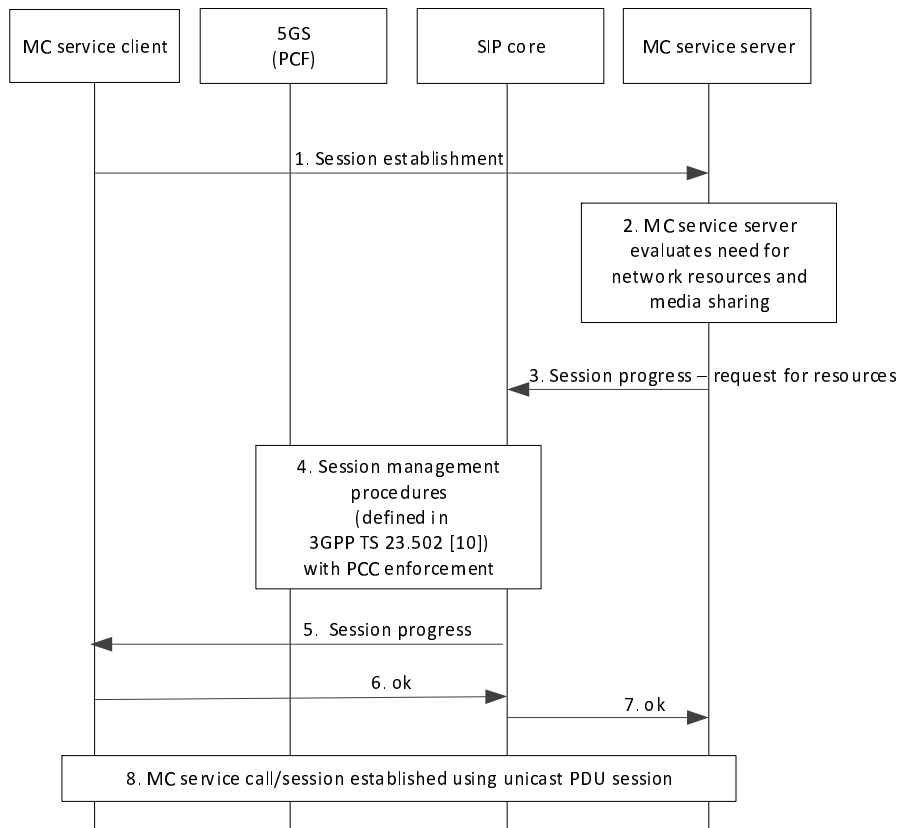
Figure 8.1-1: MC service call session establishment - FRMCS SIP core-based option
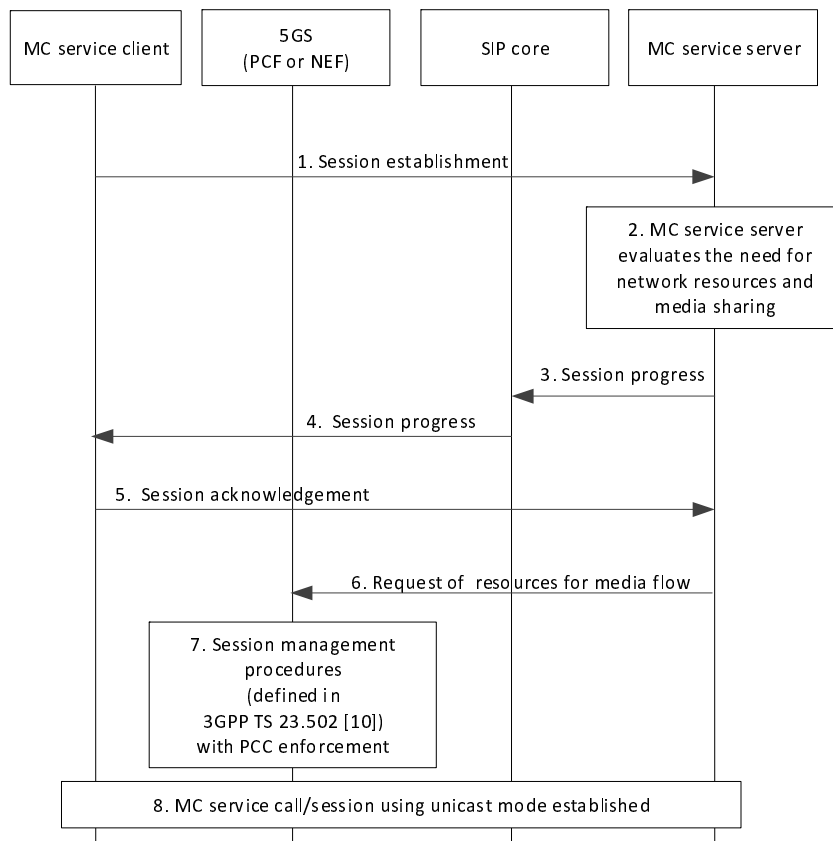
Figure 8.2-2: MC service call session establishment - Service server-based option

The MC Service Server shall utilize the Npcf_PolicyAuthorization Service as described in ETSI TS 129 514 [29] for N5 or Rx procedures in ETSI TS 129 214 [30], to request policies for the PDU session which the FRMCS MC session is bound to. The PCF shall perform mapping from the service information received over the Rx or N5 reference points to the Authorized QoS parameters that shall be passed to the SMF via the N7 reference point.

The Session binding function determines relevant PDU session and associates IP data flows to it. PCF shall consider any 5GC specific restrictions, the AF service information and other information available to the PCF. PCF associates a set of QoS parameters (5QI, ARP, etc.) to each PCC rule as per ETSI TS 129 513 [24].

The SMF shall perform mapping from the Authorized QoS parameters received from PCF to the access specific QoS parameters as per ETSI TS 129 513 [24].

FRMCS AF can use Npcf_EventExposure service to get notifications about the outcomes of UE policies delivery as per ETSI TS 129 512 [25].

The network sets up QoS flow(s) with a suitable QoS and indicates to the UE the QoS characteristics of those QoS flow(s) as per Figure 8.1-3 (reference to ETSI TS 129 513 [24], clause 7.1).
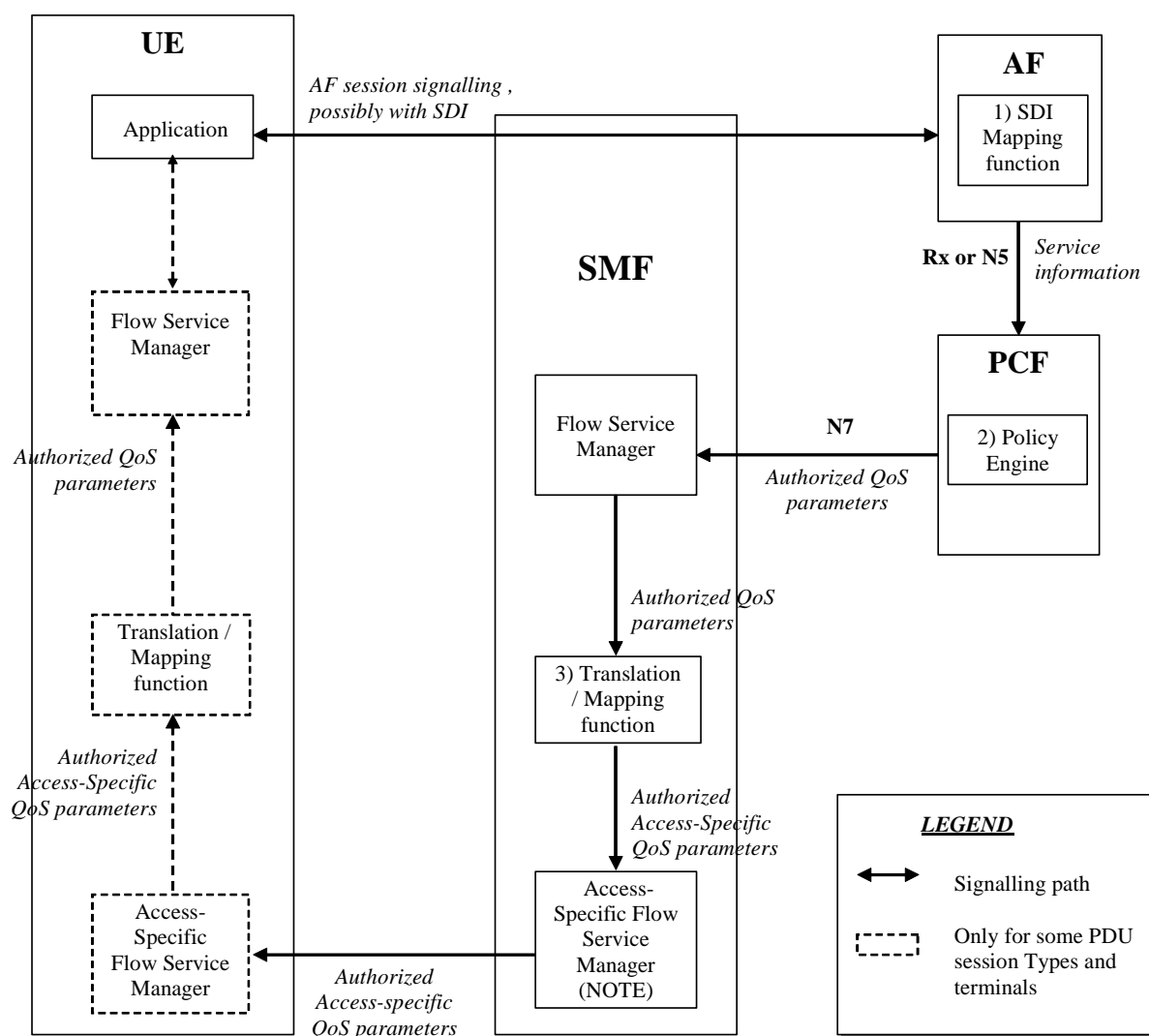
Figure 8.1-3: Flow of QoS-related messages using Rx or N5

FRMCS supports either the N5 or the Rx reference point between AF and PCF.

FRMCS shall utilize the *afAppID* on the N5 reference point or AVP parameter *AF-Application-Identifier* on the Rx reference point, as described in ETSI TS 129 514 [29] and in ETSI TS 129 214 [30], respectively. This parameter is associated, within the AF, to the <user-requested-priority> provided by the MC Service Client for the AF session, as described in ETSI TS 103 765-2 [6], clause 6.2.5.

NOTE: The mapping of the combination of Communication Session Category (CSC) and Sub-category (indicating further priority distinction within a CSC) to the afAppID needs to be consistent between the FRMCS Application Function and the (5GC of) FRMCS Transport Domain which are serving that CSC.

FRMCS shall use the *resPrio* attribute on the N5 reference point or AVP parameter *Reservation-Priority* on the Rx reference point, as described in ETSI TS 129 514 [29] and in ETSI TS 129 214 [30], respectively. This attribute shall be mapped to the value of the Resource-Priority header field of the SIP INVITE (specified in ETSI TS 103 765-2 [6], clause 6.2.6) according to Table 8.1-1.

Table 8.1-1: Mapping of Resource-Priority to resPrio and Reservation-Priority

Resource-Priority header field	resPrio	AVP Reservation-Priority
Normal	PRIO_1 (lowest priority)	0 (lowest priority)

Based on the information (*afAppId, resPrio*) received from FRMCS AF, PCF shall perform policy decisions for PDU session with particular MC service during SM policy association modification procedure as per ETSI TS 123 502 [10], clause 4.3.3.2, 1b.

8.2   FRMCS Unified Access Control (UAC)

In FRMCS, UAC enables the prioritization of access for FRMCS users and helps the gNodeB load control functions to effectively handle the high-load scenarios. Access prioritization is carried out by barring the mobile-originated access and service requests at the UE side. The UE will decide if it is allowed to submit a connection request to a network based on the instructions in the SIB1 message. This is accomplished by verifying the broadcast system data (S1B1 message) that is obtained over the network, along with the user/service data that is kept in the UE.

In high traffic load situations, the network may set up the broadcasted system information to restrict requests from certain users. UEs will follow instructions in the SIB1 message, which means no extra load is added to the RAN to restrict access. If the connection request is approved, a user can initiate a normal random-access procedure to connect to the network.

In UAC the access barring profile is a combination of FRMCS PLMN, Access Identities, and Access Categories. Barring probability in high load situations is applied according to barring profiles.

For an On-Board FRMCS radio module, the USIM file EF$_{UAC\_AIC}$ shall be configured with Access Identity equals to 2 and the MCS Indicator bit of the mobile network shall be set to valid within the FRMCS Transport Domain as specified in clauses 4.5.2 and 4.5.2A in ETSI TS 124 501 [9].

On-Board FRMCS radio module in a shared network shall be configured with zero barring probability. UEs with an Access Identity equal to zero and Access Category equal to 9 (MO Data) shall be configured with a high barring probability.

8.3   5QI and ARP Application per FRMCS Service

The FRMCS Transport Domain shall support at least the 5QI identified in Table 8.3-1.

Table 8.3-1: List of 5QI in FRMCS

5QI
4
5
8
65
69

As an example, two of the Communication Session Categories listed (informative) in ETSI TS 103 765-2 [6] Annex A, can be mapped as defined in Table 8.3-2.

Table 8.3-2: An example of mapping afAppId/AF-Application-Identifier, 5QI and
ARP to FRMCS Communication Session Category

Communication Session Category	Sub-category	afAppID/ AF-Application-Identifier	5QI	ARP
Default Data	N/A	"Default Data"	8	8
Voice	Urgent Driver-to-Controller	"Voice - Urgent Driver-to-Controller"	65	3
	Normal Driver-to-Controller	"Voice - Normal Driver-to-Controller"	65	5

NOTE: The mapping between Communication Session Category and the afAppId needs to be harmonized between the FRMCS Application Function and the (5GC of) FRMCS Transport Domain.

8.4   5QI to DSCP Mapping

The QoS of FRMCS Transport Stratum traffic is classified using 5QI. Since the traffic flow to some endpoints (Trackside Gateway, VAS controller, etc.) traverses an IP/MPLS backbone the 5QI shall be mapped to a Traffic Class.

For each QoS Flow characterized by its 5QI, the mapping of 5QI to DSCP values are done on different nodes depending on the traffic direction:

- For UL traffic, the gNodeB maps the 5QI values to transport DSCP values. For DL traffic, the mapping is done by local configuration on the SMF, which provides UPF with the transport DSCP values. The UPF then marks DL traffic on a per QoS Flow basis.

The DSCP mapping for mandatory FRMCS 5QIs from Table 8.3-1 is identified in Table 8.4-1.

Table 8.4-1: 5QI to DSCP Mapping

5QI	DSCP
4	AF43 (DSCP 38)
5	CS5 (DSCP 40)
8	AF12 (DSCP 12)
65	EF (DSCP 46)
69	CS5 (DSCP 40)

9   Transport Stratum Synchronization

9.1   Radio Network Synchronization

NR SA TDD radio networks require frequency and phase synchronization. When the Baseband Radio Node is time and phase synchronized, it is also frequency synchronized.

FRMCS TDD cells operating at the same frequency in overlapping coverage areas would benefit from time domain isolation to minimize base station-to-base station and UE-to-UE Radio Frequency (RF) interference.

There are two requirements to achieve time domain isolation:

- The cells need to use the same TDD configuration.

- The deviation in frame start timing between cells needs to be below a maximum value specified as cell phase synchronization accuracy in the 3GPP specification.

ETSI TS 138 104 [31] and ETSI TS 138 133 [32] provide specifications for frequency and phase synchronization at the radio air interface to meet NR deployment requirements across various use cases. ITU-T (Recommendation ITU-T G.8271.1 [33] and Recommendation ITU-T G.8271.2 [34]) specifies timing profiles and network budget for the transport network to meet those requirements for 5G RAN. These requirements can be classified into:

  a) NR TDD specific requirements;

  b) improved NR performance and spectrum efficiency; and

  c) use case specific requirements.

In 3GPP, cell phase synchronization between NR TDD radios is specified as 3 µs. That leaves ±1,5 µs time error accuracy from the common time reference to each radio, and a remainder of ±1,1 µs to the transport network if the common time refence is connected over the backhaul network. The frequency synchronization is specified as 50 ppb at the air interface level, and a budget of 16 ppb is typically assumed for the backhaul transport network.

Location and Positioning using 5G 3GPP techniques demand more stringent accuracy from the 5G NR radios (e.g. location accuracy and position tracking). The measurement of accurate positioning depends on a time difference measured over-the-air interfaces. One such method, observed Time Difference of Arrival (OTDOA), assumes that the relative phase offset between the reference stations are within the defined accuracy limits, and that their relative phase offset is known. 3GPP specifications define a stringent ±100 ns phase accuracy as positioning requirements between adjacent 5G NR radios.

Inter-band and intra-band CA, and the use of MIMO antennas, have a very stringent relative time alignment error of 130 ns to 260 ns measured at the antenna air interface.

9.2   Time-of-Day Synchronization

Network Time Protocol (NTP) (see IETF RFC 5905 [i.2]) or Network Time Security, IETF RFC 8915 [i.3] can be used to synchronize the time of day. The main objective of NTP is long-term event synchronization across core and radio access nodes.

The core network elements and elements in the baseband nodes can then send NTP requests via interfacing between O&M functions and the NTP server.

10   Transport Stratum Identities

FRMCS uses the following identities in the transport stratum:

  • GPSI as external identifier.

  • SUPI/SUCI using IMSI identifier.

  • NAI using IMSI with MCC and MNC.

Annex A (informative):
Generalities on synchronization

This annex is intended as informative on possible approaches to achieve synchronization requirements in the Radio Access Network.

Synchronization is typically achieved by syncing towards a common Grandmaster via, e.g. GNSS or the transport network.

Clear satellite visibility is critical for the operation of GNSS receivers. However, ionospheric delay variations, solar activities, and weather conditions are additional factors that could impact the performance accuracy of the GNSS receiver in the range of several nanoseconds. The existing single-band GNSS receivers (PRTC-A with ±100 ns accuracy) are limited to mitigate these errors, and 5G NR demands better GNSS receiver technologies to meet previously discussed deployment requirements.

GNSS and PTP are valid references for RAN synchronization.

The two references (GNSS and PTP/IP) can be used with primary and secondary reference distinguished by priority setting. When synchronization reference fails, the system falls back to the secondary reference and the holdover time can be extended in case it is assisted with Synchronous Ethernet (SyncE) protocol.

If outage occurs in the GNSS synchronization reference, the gNodeB enters holdover for a limited time and all radio services are maintained. The holdover period can be extended if the GNSS is assisted with a PTP/IP connection. This is called Assisted Partial Timing Support (APTS). The timing support enables the gNodeB to calculate the timing compensation in the PTP/IP provided by the central PTP/IP Grandmaster while the GNSS is available. The learnt compensation value is then used when switching to the PTP/IP Grandmaster at a GNSS outage.

Depending on the network conditions and the duration of the local GNSS signal time and phase synchronization presence before the GNSS outage, a gNodeB can provide accurate timing information for a longer period if the PTP/IP reference remains stable.

If the PTP/IP reference is also lost during a GNSS outage, the node loses time and phase synchronization, and the cell eventually goes down.

The PTP/IP Grandmaster can be located either centralized in the core or distributed in the network to serve dedicated clusters of gNodeB. The most common scenario for large networks is to have multiple Grandmasters to serve clusters of gNodeB to minimize the potential asymmetry introduced by the transport network. The distributed Grandmasters are then generally located at one of the cell sites in the gNodeB cluster.

History

Version	Date	Status
V1.0.0	July 2025	SRdAP process EV 20251008: 2025-07-10 to 2025-10-08