NG.145 Mission Critical Communications Roaming Guidelines

Version 1.0

27 Jan 2025

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Scope

Scope of this document is it to identify potential technical requirements and technical implementation guidelines that best suit mission critical services' use cases in international roaming environment. As part of the set of information relevant for each mission critical communication services' use cases, types of traffic are described (e.g. data, voice, Short Message Service), together with relevant scenarios where each use case applies (e.g. domestic, roaming). Different network architectures are also described together with potential technical requirements as per network architecture (e.g. 4G, 5G SA/NSA, QoS): 4G, 5G NSA are covered as phase 1 document release and 5G SA is covered as phase 2 document release. This document covers phase 1.

Additionally, legal aspects are highlighted (e.g. Legal Interception, Roaming Service Level Agreement) as well as interaction and/or interworking with network related procedures (e.g. Steering of Roaming).

1.2 Definitions

Term	Description
5G NETC – 5G Northern European Transport Corridors	5G corridors are projects designed to provide seamless 5G connectivity to vehicles even as they cross borders, thereby paving the way for autonomous driving on main road, train and maritime routes.
PCI – Pre-emption Capability Indicator	Indicates whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level: (0-enabled, 1–disabled)
ARP PL – Priority Level	Used for deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations, to decide which existing bearers to pre-empt during resources limitations: (1 to 15, 1 highest priority level)
PVI – Pre-emption Vulnerability Indicator	Indicates whether a service data flow can lose resources assigned to it in order to admit a service data flow with a higher priority level: (0-enabled, 1–disabled)
S10 Interface	used by a target MME during inter-MME tracking area updates to get information about security, active bearers from source MME or the ongoing session from the source MME to target MME during Inter-PLMN to handover

1.3 Abbreviation

Term	Description
3GPP	The 3rd Generation Partnership Project
5QI	5G QoS Identifier
AGA	Air to Ground to Air
ARP	Allocation and Retention Priority
ATP	Automatic Train Protection
ATP_OB	Automatic Train Protection On Board
ATP_TS	Automatic Train Protection Train Station
FRMCS	The Future Railway Mobile Communication System
EHPLMN	Equivalent Home Land Mobile Network
eNB	enhanced Node Base Station
ePLMN	Equivalent Land Public Mobile Network
GSMA	GSM Association
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Service
II-NNI	Inter-IMS Network to Network Interface
I/S-CSCF	Interrogating/Serving-Call Session Control Function
IMS	IP Multimedia Subsystem
IOPS	Isolated Operation for Public Safety
IPX	Internetwork Packet Exchange
ISIM	IP Multimedia Services Identity Module
IWK	Interworking
KPI	Key Performance Indicator
LMR	Land Mobile Radio
LTE	Long Term Evolution
MBMS	Multimedia Broadcast/Multicast Service
MC	Mission Critical
MCDATA	Mission Critical Data Service
MCVIDEO	Mission Critical Video Service
OTT	Over The Top Application
MCCoRe	Mission Critical Services Common Requirements
MME	Mobility Management Entity
MME-PCRF	Mobility Management Entity- Policy Control and Charging Function
MCPTT	Mission Critical Push-To-Talk
MCX	Mission Critical Communications/Services
MCX AS	Mission Critical Services Application Server
MNO	Mobile Network Operator

Term	Description
MOCN	Multi Operator Core Network
NAS	Non Access Stratum
PCC	Policy and Charging Control
PCI	Pre-emption Capability Indicator
PL	Priority Level
PLMN	Public Land Mobile Network
P-CSCF	Proxy Call Session Control Function
PCRF	Policy Control and Charging Function
PGW	Packet Data Network Gateway
PPDR	Public Protection and Disaster Recovery
PRD	Permanent Reference Document
ProSe	Proximity Services
PSA	Public Safety Agencies
PSBN	Public Safety Broadband Network
PSBN AGA	Public Safety Broadband Network Aerodromes and Ground Aids
PVI	Pre-emption Vulnerability Indicator
RAT	Radio Access Technology
RBC	Radio Block Centre
SGW	Serving GateWay
SIB	System Information Block
SMS	Short Message Service
SMSoNAS	Short Message Service over Non Access Stratum
QoS	Quality of Service
QPP	Quality of Service, Priority, and Pre-emption
S8HR	Roaming Interface S8 (SGW-PGW) Home Routed
TAI	Tracking Area Identity
TAU	Tracking Area Update
UE	User Equipment
USIM	Universal Subscriber Identity Module
VOLTE	Voice Over LTE (Long Term Evolution)
VPLMN	Visited Public Land Mobile Network

1.4 References

Ref	Doc Number	Title
[1]	3GPP TS 36.579 V16.6.0 (2024-09)	Mission Critical (MC) services over LTE; Part 1: Common test environment (Release 16)
[2]	3GPP TS 23.280 V19.4.0 (2024-09)	Common functional architecture to support mission critical services; Stage 2 (Release 19)
[3]	3GPP TS 23.179 V13.5.0 (2017-03)	Functional architecture and information flows to support mission critical communication services; Stage 2 (Release 13)
[4]	3GPP TS 23.379 V19.4.0 (2024-09)	Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT);Stage 2 (Release 19)
[5]	3GPP TS 23.501 V19.1.0 (2024-09)	System architecture for the 5G System (5GS);Stage 2 (Release 19)
[6]	3GPP TS 23.203 V19.0.0 (2024-09)	Policy and charging control architecture (Release 19)
[7]	3GPP TS 24.483 V18.4.0 (2024-09)	Mission Critical Services (MCS) Management Object (MO) (Release 18)
[8]	3GPP TS 24.484 V18.7.0 (2024-09)	Mission Critical Services (MCS) configuration management; Protocol specification (Release 18)
[9]	3GPP TS 22.281 V18.0.1 (2024-03)	Mission Critical Video services (Release 18)
[10]	3GPP TS 22.280 V19.6.0 (2024-09)	Mission Critical Services Common Requirements (MCCoRe);Stage 1 (Release 19)
[12]	3GPP TS 26.281 V18.0.0 (2024-05)	Mission Critical Video (MCVideo);Codecs and media handling (Release 18)
[13]	3GPP TS 36.579-2 V16.6.0 (2024-09)	Mission Critical (MC) services over LTE;Part 2: Mission Critical Push To Talk (MCPTT) User Equipment (UE) Protocol conformance specification (Release 16)
[14]	3GPP TS 22.282 V18.0.1 (2024-03)	Mission Critical Data services (Release 18
[15]	3GPP TS 23.282 V19.4.0 (2024-09)	Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2 (Release 19)
[16]	3GPP TS 22.011 V19.4.0 (2024-09)	Service accessibility (Release 19)
[17]	3GPP TS 23.401 V19.0.0 (2024-09)	General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 19)
[18]	3GPP TS 29.272 V18.5.0 (2024-09)	Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (Release 18)

Ref	Doc Number	Title
[19]	GSMA PRD IR.88	EPS Roaming Guidelines
[20]	GSMA PRD IR.21	GSM Association Roaming Database, Structure and Updating Procedures
[21]	GSMA PRD IR.73	Steering of Roaming Implementation Guidelines
[22]	GSMA PRD IR.34	Guidelines for IPX Provider networks (Previously Inter-Service Provider IP Backbone Guidelines)
[23]	GSMA PRD NG.113	5GS Roaming Guidelines
[24]	GSMA PRD IR.81	GRQ Measurement Implementation
[25]	GSMA PRD IR.92	IMS Profile for Voice and SMS
[26]	GSMA PRD BA.51	Roaming Service Level Agreement Guidelines

2 Background

Mission Critical Services have been defined by the 3GPP and have grown in the specifications since its start in the release13. Since then, a need has been recognized for Public Safety Agencies (PSAs) to enhance mission critical communication capabilities by leveraging on new technologies, i.e. LTE radio access technology, enhanced MBMS (Multimedia Broadcast/Multicast Service), IP Multimedia Subsystem (IMS) platform as well as on the new set of 5G services. That leads to the development of Mission Critical Broadband Network, allowing mission critical communications to exchange multimedia content in addition to voice and to get the benefit of mobile broadband access; also allowing the extension of mission critical communication to sectors of society and industries other than the most typical critical communications users i.e. the so called “blue lights” agencies (police, ambulance and the fire brigade).

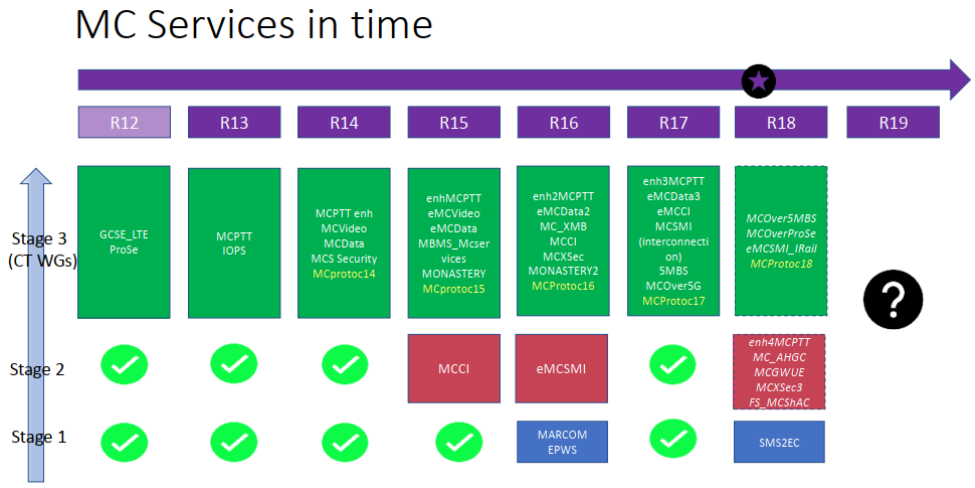


Figure 1: Mission Critical services in time

2.1 3GPP MCX Specifications

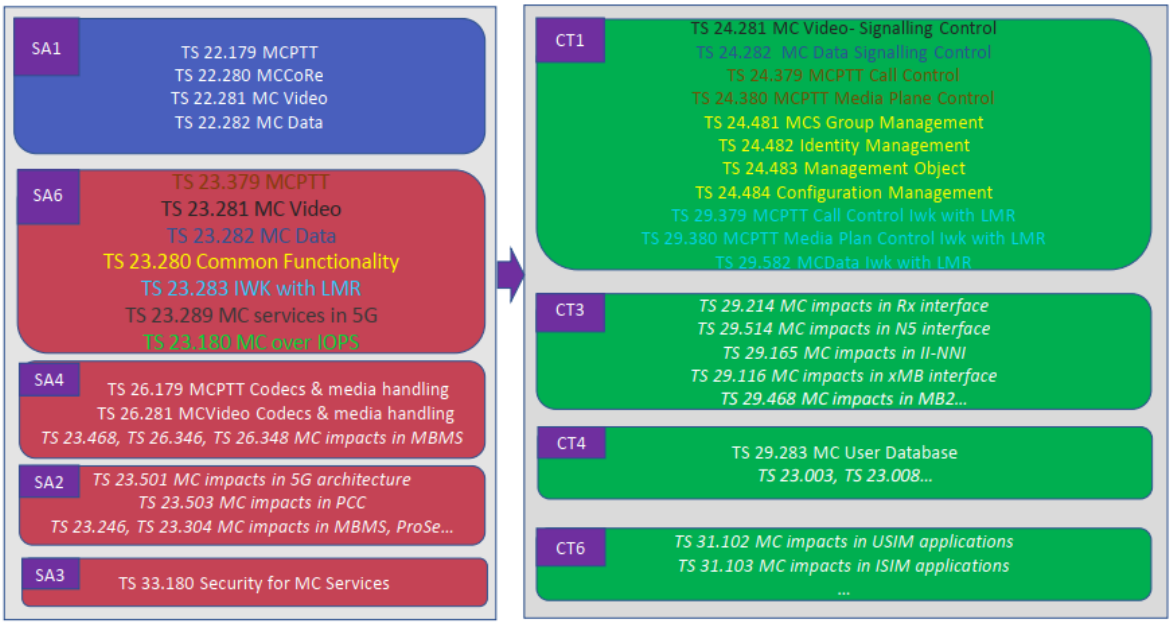


Figure 2: 3GPP MCX Specifications

3 Mission critical communication for Industries- Use cases

3.1 Wildfire

3.1.1 Description

Firefighters from country A are requested to help in an operation of a non-neighbour country B.

3.1.2 Service Flow

The firefighters from country A switches off their communication devices and travel by road or air to a visiting country (a location of the operation) and help country B. In this scenario, while operating, the country-A first-responders stay in country B, switched on their communication devices and are connected to one or multiple mobile networks (for instance, X,Y or Z) in country B depending on the location and the quality of the available coverage. Networks X,Y or Z can be commercial MNOs, national private mission critical networks, or other local private networks (e.g., tactical bubbles). Firefighters from country A need to join communication groups shared with their counterparts of country B and also need to stay in contact with their respective national colleagues in either country A or B.

4 Police chase

4.1 Description

A Suspect car from country A is being followed by a police car from country A.

The suspect car is crossing different country borders.

4.1.1 Service Flow

Police car maintains connection with the Control Room of country A regardless of whatever country they are in.

4.2 Railways – Automatic Train Protection (ATP)

4.2.1 Description

For Automatic Train Protection (ATP), the train transmits its information (such as current location, current speed, etc.) to the relevant Radio Block Centre (RBC) using FRMCS. As soon as a connection has been established between a train and an RBC, the train sends its position and speed information periodically. The RBC uses the received information to decide movement authority[1] of the train.

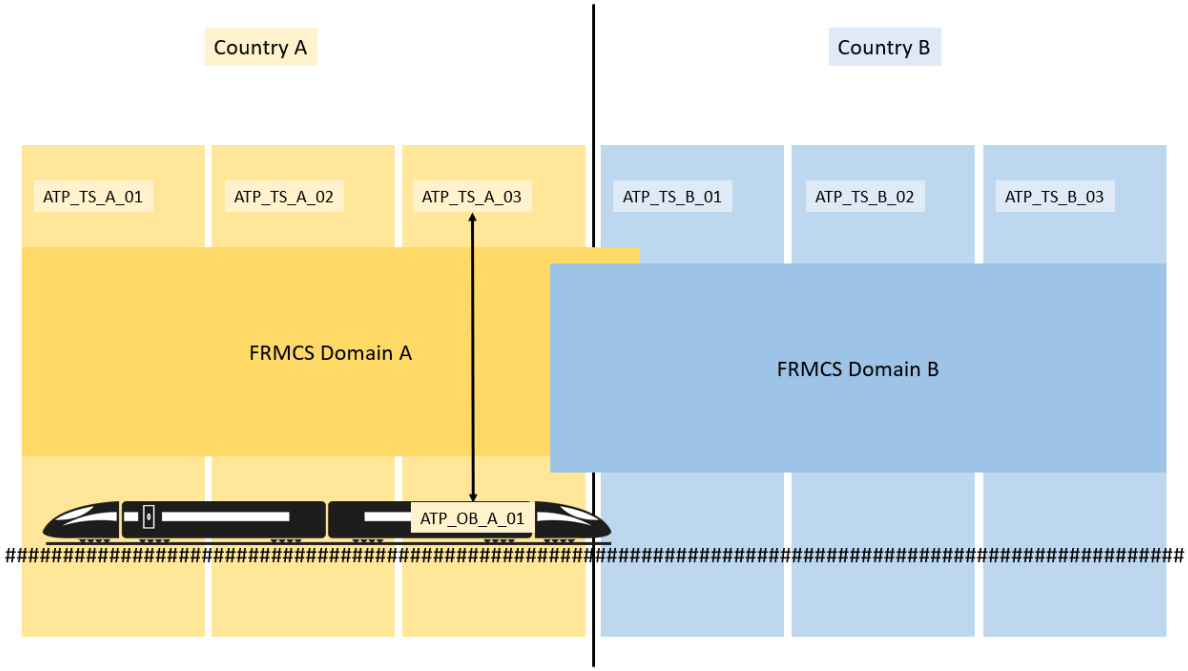


Figure 3: Railways – Automatic Train Protection

[1] Movement Authority : the permission for a train to run at a given speed and up to a given point of the track (End of Authority).

4.2.2 Pre- Conditions

The train is located in its home FRMCS Domain A (national operator of Country A).

Its onboard ATP (ATP_OB) is connected to the relevant trackside ATP (ATP_TS_A_03 as depicted in **Error! Reference source not found.**) in charge of its movement authority using FRMCS.

The onboard ATP (ATP_OB) is using a single UE to connect to FRMCS Domain A and all along the service flow in section 3.3.3.

4.2.3 Service Flow

The train is moving from its home FRMCS Domain, namely FRMCS Domain A, to a neighbour FRMCS Domain, namely FRMCS Domain B. It can be assumed that FRMCS Domain A and FRMCS Domain B are operated respectively by the national FRMCS operator of Country A and national FRMCS operator of Country B.

The onboard ATP (ATP_OB) receives the order to connect to neighbour RBC ATP_TS _B_01 in Country B.

The onboard ATP (ATP_OB) requests a connection to neighbour RBC ATP_TS _B_01 in Country B. For this purpose, the onboard MC client requests establishment of MCData one-to-one IP connectivity within FRMCS Domain B towards trackside MC client connected to the neighbour RBC ATP_TS _B_01. A bearer of suitable QoS and priority is established.

When established, the onboard ATP (ATP_OB) is connected to both ATP_TS _A_03 through FRMCS Domain A and ATP_TS_RBC_B_01 through FRMCS Domain B.

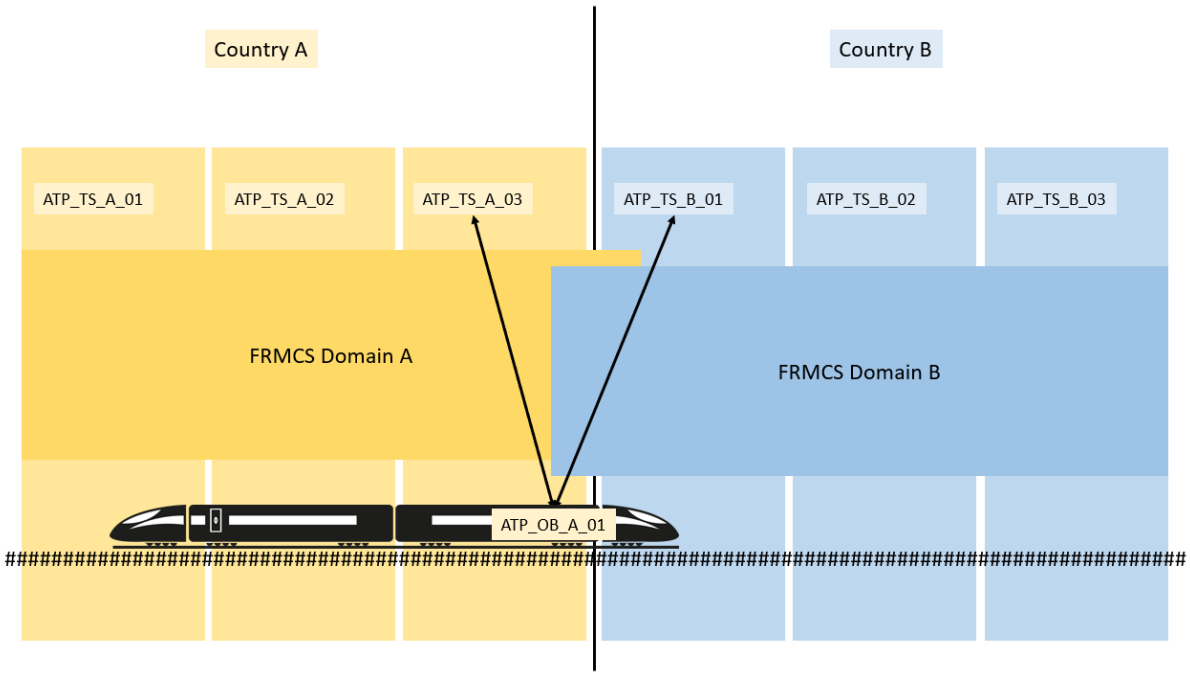


Figure 4: Service Flow

The onboard ATP (ATP_OB) receives the order to disconnect from RBC ATP_TS _A_03.

The onboard ATP (ATP_OB) requests a disconnection to RBC ATP_TS_RBC_A_03. The corresponding FRMCS services and resources are therefore released.

4.2.4 Post-Conditions

The onboard ATP (ATP_OB) is connected to ATP_TS_RBC_B_01 through FRMCS Domain B.

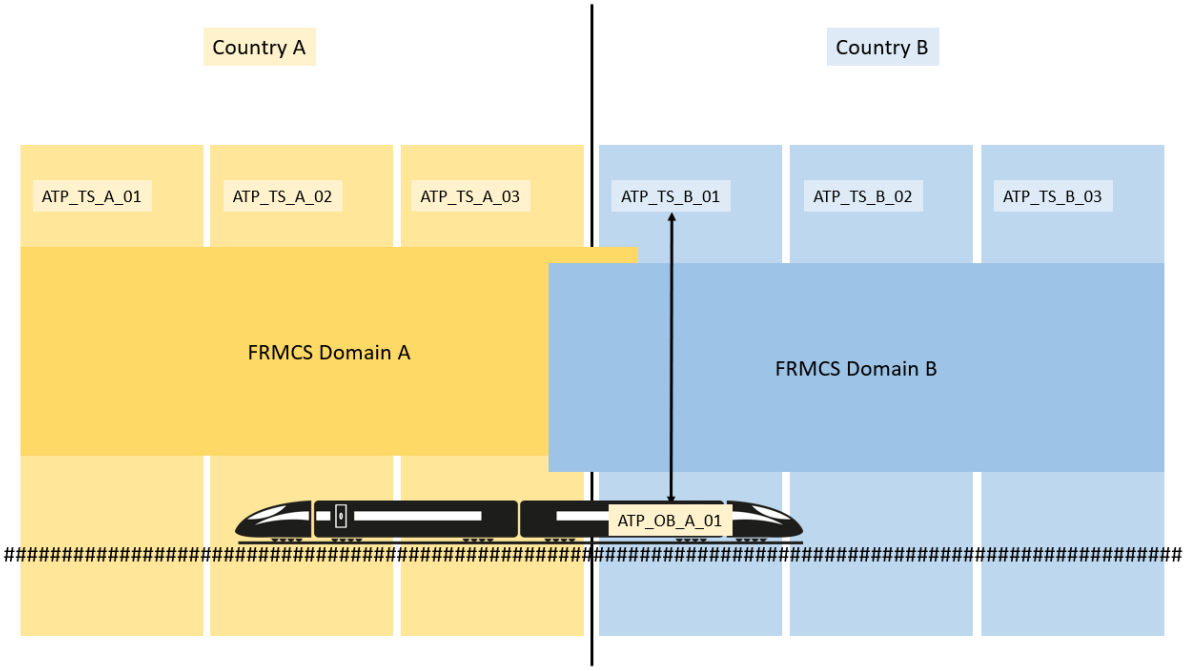


Figure 5: Post conditions

4.3 Mission Critical Cross Border Communications

This use case contains roaming scenarios in a complex situation which requires mission critical communication between several resources, such as networks, personnel, vehicles, aircrafts, cameras, sensors. The scenario described takes place at the border area in a remote location, with partly limited mobile networks coverage. Resources from at least two countries need to be involved to handle what turns out to be two critical incidents involving common resources.

4.3.1 Scenario 1

There is a large traffic accident involving two vehicles and several dead and injured passengers. The accident takes place in Country A very close to the border to Country B. Passengers and casualties are from both countries. Dispatch centres on both sides of the border have received 112 calls from passengers and people witnessing the accident.

Country B resources are asked to respond across the border in Country A to assist in rescue of passengers, traffic control and to limit material damage. Police, Fire, Ambulance vehicles,

Ambulance helicopters, Customs and Road Authorities from both countries arrive at the scene and work seamlessly together. Various teams are assigned international agency-specific and/or international multi-agency talk groups.

4.3.1.1 Service Flow

Public Safety Broadband Network (PSBN) users from Country B cross the border of Country A and connect to the PSBN or a mobile network of Country A while maintaining services.

Some PSBN users from Country A may connect to the PSBN or mobile network of Country B while in Country A while maintaining service.

Visiting and home PSBN users from Countries A and B can communicate with each other in international agency-specific and international multi-agency talk groups.

4.3.2 Scenario 2

Injured passengers are brought to the nearest hospital in Country A by ambulances from both Country A and B. The severely injured passengers are brought to a large but further away hospital in Country B by a helicopter from Country A.

4.3.2.1 Service Flow

Ambulances from Country B cross the border of Country A and connect to the PSBN or a mobile network of Country A while maintaining service.

An ambulance helicopter from Country A uses the PSBN AGA network of Country A, crosses the border of Country B and connects to the PSBN AGA network of Country B.

4.4 Scenario 3

Before the police arrived, one of the involved drivers escaped from the scene together with some of the passengers taken as hostages. This initiates a police-led search and rescue mission in both countries. The area is remote, in the forest, and the coverage is poor outside the road. A cell-on-drone with backhaul to the Public Safety operator’s network in Country B is used to give temporary coverage (establish a tactical bubble) in both countries.

4.4.1.1 Service Flow

PSBN users from Countries A and B connect to the PSBN of Country B via the cell on drone while maintaining service.

4.4.2 Scenario 4

The search area is in both countries. Country A and Country B resources are called to participate in the police-led search and rescue mission. Live incident videos are sent from helicopters, drones and first responders' body-worn cameras to the rescue teams and the operations centres in both countries. Additional information such as location information, sensor information, data base information etc. is shared between field units and operation centres.

4.4.2.1 Service Flow

Visiting and Home PSBN helicopters (AGA-connected), drones (AGA or terrestrial-connected) and PSBN users from Countries A and B can communicate with each other in international agency-specific and international multi-agency communication groups for MCData and MCVideo.

5 Services and Architecture

5.1 Architecture Overview

MCX roaming is based on the existing regular 4/5G data roaming architecture (as defined in GSMA PRD IR.88). The same architecture is reused also by VoLTE roaming as a basis for the S8HR model.

As 4/5G data roaming is home routed it means that the Visited Public Land Mobile Network (VPLMN) is “a bit pipe” and all the service related intelligence such as PCRF, IMS core and MCX application server(s) are always located in the HPLMN. The main purpose of VPLMN is to provide a connectivity to the MCX service hosted by HPLMN.

An extension to the existing 4/5G data roaming architecture is the S10 interface running between MME in VPLMN and MME in HPLMN. It can be used to minimise the service interruption when the UE moves between these networks.

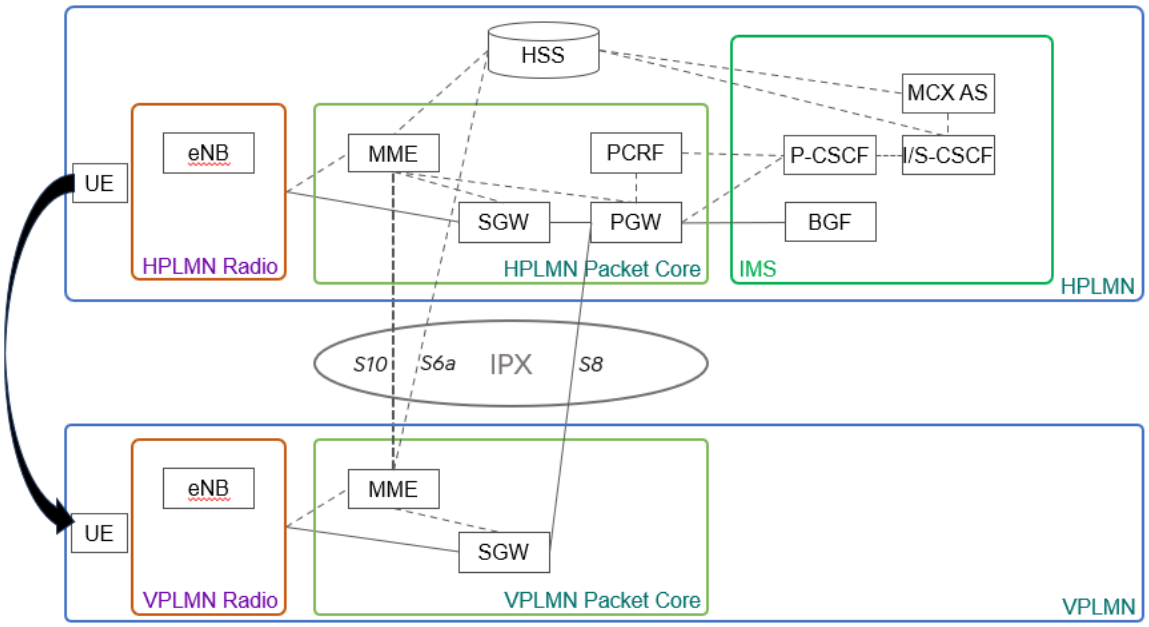


Figure 6: An MCX UE moves from HPLMN to VPLMN using the 4G/5G data roaming architecture

5.2 Potential Requirements

5.2.1 Wildfire

Foreseen functional and technical requirements:

- No action is needed from the end user point of view to get connectivity (seamless roaming),
- End users from country A are able to join existing talk groups or newly created talk groups from country B
- End user's UE from country A should be compatible with radio frequency spectrum from country B's mobile networks,
- Roaming to networks X,Y and Z with Quality of Service, Priority and Pre-emption,
- Seamless handover when roaming between operator X,Y and Z,
- Handover based on the best coverage or quality of service,
- Access to Home services hosted in country A
- Secured communications,
- MCX KPIs are met (low latency)

5.2.2 Police Chase

Foreseen functional and technical requirements:

- No action is needed from the end user point of view to get connectivity (seamless roaming)
- Seamless handover when roaming between different country networks
- End user's UE from country A should be compatible with the radio frequency spectrum of the cross country mobile networks when crossing different country borders
- Roaming to different country networks with Quality of Service, Priority and Pre-emption
- Handover based on the best coverage or quality of service
- Access to Home services hosted in country A
- Secured communications
- MCX KPIs are met (low latency)

5.2.3 Railways – Automatic Train Protection (ATP)

Getting connectivity to neighbour FRMCS Domain B shall be transparent to the application/end user (i.e., non-human user onboard ATP),

Non-human user onboard ATP from FRMCS Domain A in Country A shall be authorised to join newly created MCData one-to-one IP connectivity to trackside ATP from FRMCS Domain B in Country B,

UE used by non-human user onboard ATP from FRMCS Domain A in Country A shall be compatible with frequency bands of FRMCS Domain B in Country B,

The onboard ATP (ATP_OB) shall be able to connect simultaneously to both ATP_TS A_03 through FRMCS Domain A and to ATP_TS_B_01 through FRMCS Domain B for the transition time. This is required to ensure a "make-before-break" at application level.

QoS, priority and pre-emption shall be supported by both FRMCS Domain A in Country A and FRMCS Domain B in Country B,

QoS: Critical MCData KPIs shall be met:

- End-to-end latency is less than or equal to 500ms
- Reliability of 99.9%
- Speed limit is 500 kmph
- Data rate is less than 500kbps
- Service interruption is less than 150ms (TBC).

Confidentiality and integrity at MC layer are not required (supported by the application itself).

5.2.4 Mission Critical Cross Border Communications

Foreseen functional and technical requirements:

- No action is needed from the end user point of view to get connectivity (automatic and seamless roaming)
- PSBN users from Country A are able to join existing talk groups or newly created talk groups from Country B
- PSBN UEs from Country A should be compatible with the radio frequency spectrum from Country B
- Roaming to networks X, Y and Z with Quality of Service, Priority and Pre-emption
- Seamless handover when roaming between networks X, Y and Z
- Handover based on the best coverage or quality of service
- Access to Home services hosted in Country A
- Secured communications
- MCX KPIs are met (low latency)

5.3 Mandatory PSBN network capabilities

ORED ERAGE	SECURITY AND DATA PROTECTION/PRIVACY	CAPACITY	RELIABILITY	AVAILABILITY	RESILIENT INFRASTRUCTURE	STRICT RESOLU TIME
ork is ed to this ular onment *r for r ons or onments)*	Mission Critical Communications systems are not subject to accessibility risks, airtime billing or service issues that public subscription-based networks are used to.	Mission Critical Network is engineered to address peak usage. System sizing is designed for specific traffic needs and the existing workflows for user group communications.	Network reliability is based on high availability and a redundant architecture. Load balancing between core elements improves reliability and guarantees availability	from 98- 99,99% for the entire Network	Resilient PSBN Network to ensure availability, reliability, security and coverage to meet operational requirements. Consideration should be given to the necessary increase of batteries or alternative energy systems to meet the service requirements of the PSBN networks	From 2-4/h up to 8/12 hours reso time

Table 1: Mandatory PSBN Network Capabilities

5.4 Mandatory PSBN services features

QPP	PRIORITISATION AND PREEMPTION	ACCESS CLASS BARRING
Quality of Service (QoS) / Priority / Pre-emption	To apply to all network elements such as the radio access network, the core network and application servers	Critical communications users falling into higher classes in Access Class Barring (ACB) (10-14) shall be granted access immediately *(standards use ACB with classes from 0 to 14. When congested the network can refuse or delay the access to certain classes)*

Table 2: Mandatory PSBN services features

5.5 Miscellaneous Mandatory Requirements

5.5.1 Lawful interception

(To be completed)

5.6 Roaming Scenarios

Mission Critical Services such as fire, police and ambulance may need to move from their home country to another country or switch from one network operator to another in the same country. This is, in effect, roaming. The MCS devices used in the home network should be able to use the advanced capacity solutions and Quality of Service features available on the roamed network in a geographical area.

Foreseen functional and technical requirements:

- Multicast/broadcast architecture works in networks that use secure and full MVNO architecture model and international roaming scenarios.
- Mission critical QPP are supported and available on capacity enhancement features such as multicast/broadcast in the visited network.
- Network slices can be defined and configured across network components that have different PLMNs within a country or across different countries for guaranteeing capacity for mission critical users.
- The support of other relevant features that guarantee the support of mission critical service capacity as GSMA and 3GPP standards develop.

In the diagrams below, “ back EPC” and ”front EPC” indicate the EPC elements’ proximity to RAN (and only front core has interfaces to RAN). They are also referred as ”upper core” and ”lower core” respectively. Yet, both terminologies are not standard terms.

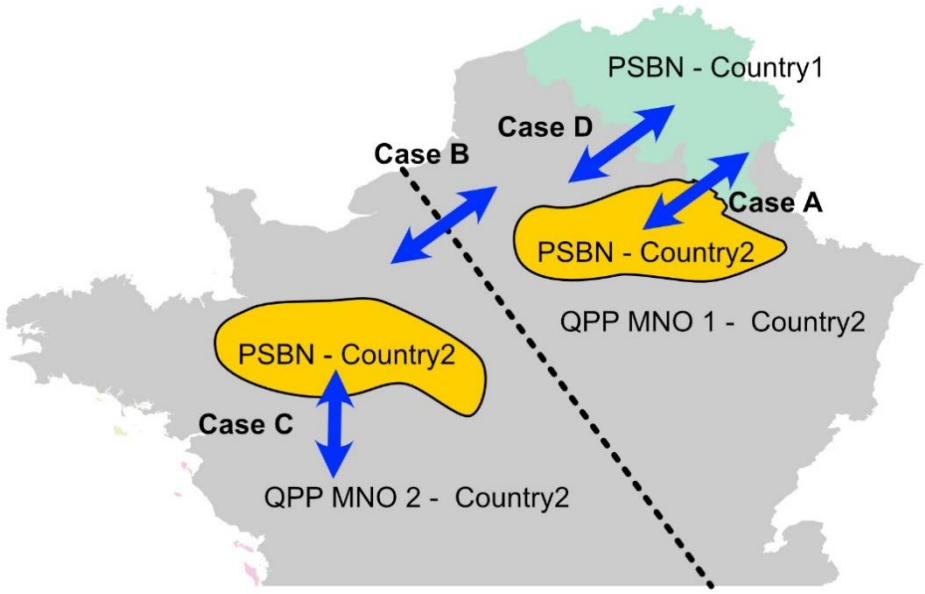


Figure 7: Roaming Scenarios

NOTE 1: Public safety broadband network (PSBN) is network generally owned by public safety network operator, specially designed for public safety users (policing, ambulance, fire etc.). PSBN has QPP enabled.

NOTE 2: QPP MNO is a public mobile network operator supporting 3GPP Quality of Service, Priority, and Pre-emption.

5.6.1 International roaming (Case A)

A user from PSBN of Country 1 crosses the border of Country 2 and connects to the PSBN of Country 2 or vice versa.

5.6.2 National roaming (Case B)

A user from PSBN of Country 2 crosses between two QPP enabled MNOs within the same country.

5.6.3 Private/Public network roaming (Case C)

In this case, an end-to-end PPDR network constitutes network components from at least two different network estates. The private network part, aka PSBN, is generally owned by a public safety network operator, acts as the home network for essential services users (policing, ambulance, fire etc.) and is not open to public use. This estate constitutes HSS, PGW, IMS, PCRF, MCS App servers and other components of a 4G network and has its own PLMN identity.

The other network part is often a public mobile network. This estate constitutes base stations, MMEs and SGWs of a 4G network. This network broadcasts different PLMN identities to cater to different QoS for public users and mission critical users thanks to MOCN configuration.

In this setup, if the PLMN identity broadcast for mission critical users is different to home PLMN identity of the PSBN network, it is working on a roaming architecture model. The broadcast PLMN identity gets the same parity of home PLMN (termed as EHPLMN - Equivalent Home PLMN) identity for mission critical users.

These two estates are linked by S8 (SGW-PGW) and S6a (MME-PCRF) roaming interfaces in LTE. Interface S10 can be optionally added to link MME of HPLMN and MME of VPLMN.

An example of this configuration is ESN – the British public safety network. The PLMN identity of PSBN is 234 71 and its partner MNO broadcasts PLMN identity of 234 32 for mission critical users and 234 30 for commercial users.

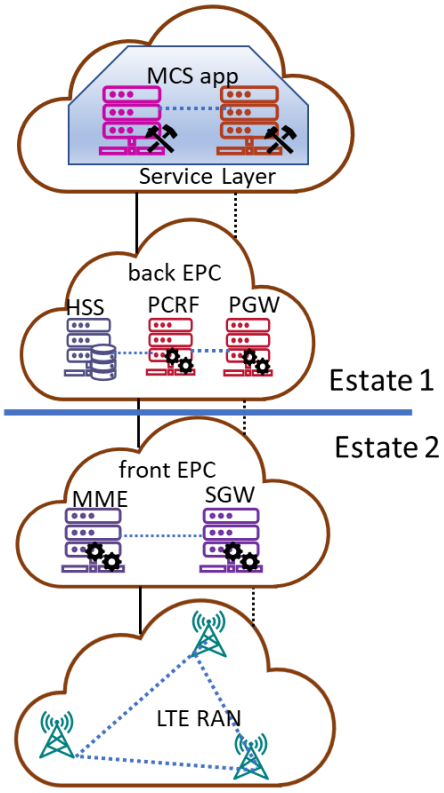


Figure 8: Private/public roaming network architecture (Case C)

Similar PLMN split also is applicable to 5G SA roaming architecture.

NOTE: If PLMN identities used by estates 1 and 2 are identical for mission critical users, this setup is not considered as a roaming architecture. An example is Finnish public safety network Virve 2.0 though it is a MOCN architecture like ESN.

Additionally, another scenario above is that mission critical users can also roam into the host MNO's PLMN only area if a base station does not broadcast mission critical network's EHPLMN and the configuration is enabled.

5.6.4 International roaming (Case D)

A user from PSBN of Country 1 crosses the border of Country 2 and connects to the MNO 1 of Country 2 where QPP are supported.

5.7 Mission Critical Communications traffic types

5.7.1 Wildfire

Primary Services:

- MCPTT
- VoLTE
- Short Data Service (MCData)
- Mission Critical Business Application (MCData)
- Non Mission Critical Business Application (OTT)

Secondary services

- MCVideo,
- SMS

5.7.2 Police Chase

Primary Services

- MCPTT
- VoLTE
- Short Data Service (MC Data)
- Mission Critical Business Application (MC Data)
- Non Mission Critical Business Application (OTT)

Secondary services

- MC Video
- SMS

5.7.3 Automatic Train Protection

Primary Services

- MCData one-to-one IP
- Functional Alias
- Resource management i.e., QoS and priority via N5/Rx interface

5.7.4 Mission Critical Cross Border Communications

Primary Services:

- MCPTT
- VoLTE
- MCVideo
- Short Data Service (MCData)
- Mission Critical Business Application (MCData)
- Non Mission Critical Business Application (OTT)

Secondary services:

- SMS

5.8 Deployment Options

5.8.1 4G Deployment

There are many possibilities for deployment options from one extreme of dedicated networks to the other extreme of fully shared network and options in between depending on the degree of separation between public users and mission critical users.

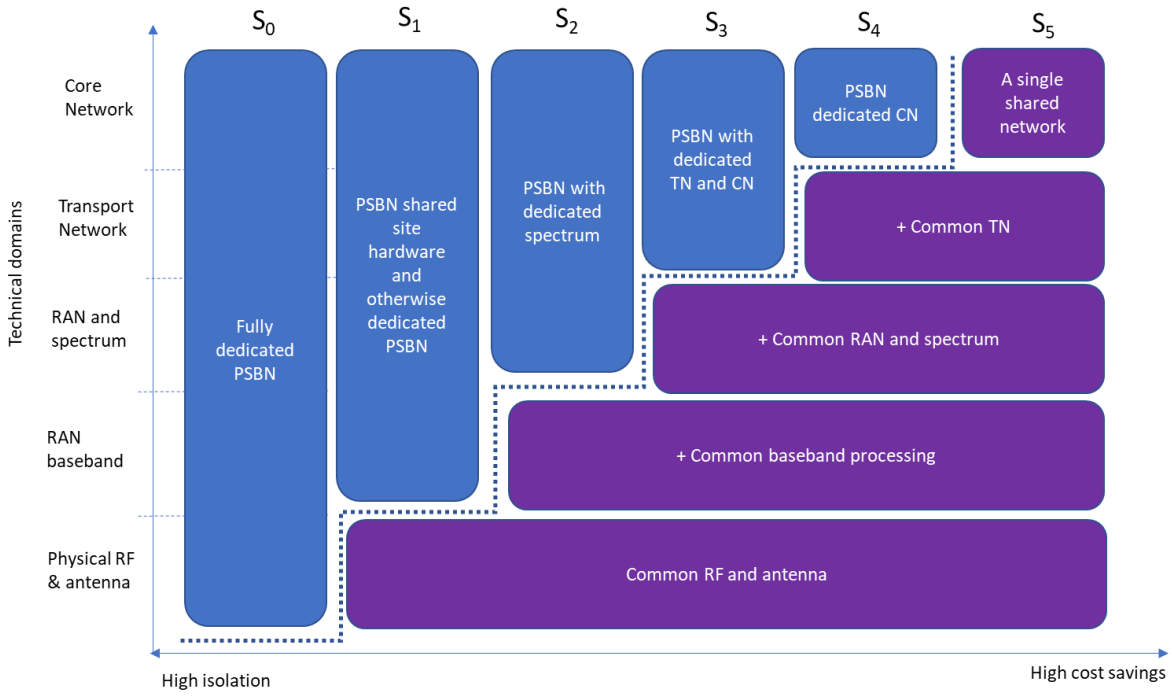


Figure 9: 4G deployment option map

Error! Reference source not found. shows the degree of PSBN's sharing of the network domain estates with public mobile networks to achieve cost savings and security. Six different network architectures, namely, S_0, S_1, S_2, S_3, S_4 and S_5 can be created. In the **Error! Reference source not found.**, the vertical blue boxes represent the dedicated part and horizontal purple boxes represent the shared part of an end-to-end public safety network.

In this section below, a few different network deployments are briefly explained. At one end is the option of a fully dedicated PSBN, and added are other hybrid PSBNs with varying options of shared infrastructures and at the other end is a fully shared PSBN, also known as Networks as a Service (NaaS) with an MNO).

PSBN owns its RAN and CN - Fully Dedicated PSBN Model

PSBN is built with its own dedicated RAN, spectrum, and CNs as shown in **Error! Reference source not found.**. An example is United Arab Emirates' public safety network called Professional Communication Corporation NEDAA, or SIRDEE, the national public safety network in Spain. No roaming interfaces are created within the network, and the coverage and services are tailored for the mission critical purposes.

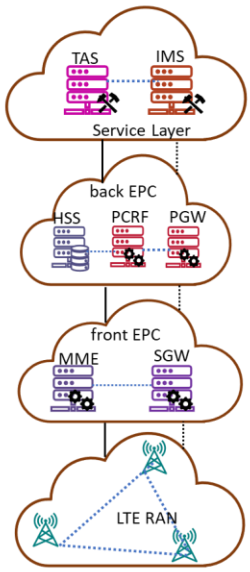


Figure 10: Fully Dedicated PSBN

PSBN owns its CN, has its own dedicated RAN in some area, and shared RAN with MNO(s) in other areas– Hybrid PSBN Model (Scenario 1)

PSBN is built with its own CN and dedicated RAN, spectrum, and extends its accessibility with shared RAN(s) of one or more MNOs in a country. A typical architecture diagram is shown in **Error! Reference source not found.**:

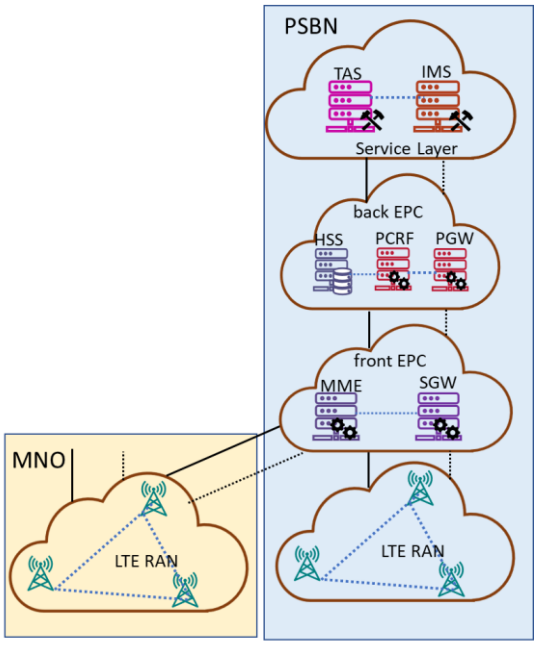
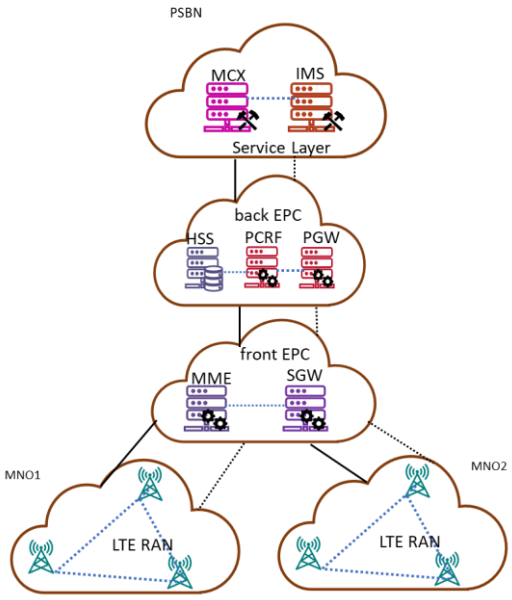


Figure 11: Hybrid PSBN Model (Scenario 1)

PSBN owns its CN but shares RAN with MNO(s) – Hybrid PSBN Model (Scenario 2)

PSBN is built with its own CN and shared RAN(s) with one or more MNOs in a country. A typical architecture diagram is shown in **Error! Reference source not found.**. An example is Virve 2 in Finland. No roaming interfaces are created within the network. RANs are shared



between commercial network and the public safety network by 3GPP defined MOCN configurations.

Figure 12: A PSBN architecture with dedicated CN and shared RAN(s)

PSBN owns a part of CN, but shares RAN and the other part of CN with MNOs

PSBN is built with CN split between itself and MNOs, and shared RAN(s) with one or more MNOs in a country. Typical architectures are shown in **Error! Reference source not found.**. Examples are ESN in UK and RRF in France. 3GPP standardised roaming interfaces (S8 and S6a) are created optionally between MNO(s) and PSBN if PLMN identities of the PSBN part and MNO parts are different. The roaming interface is between the front EPC and back EPC.

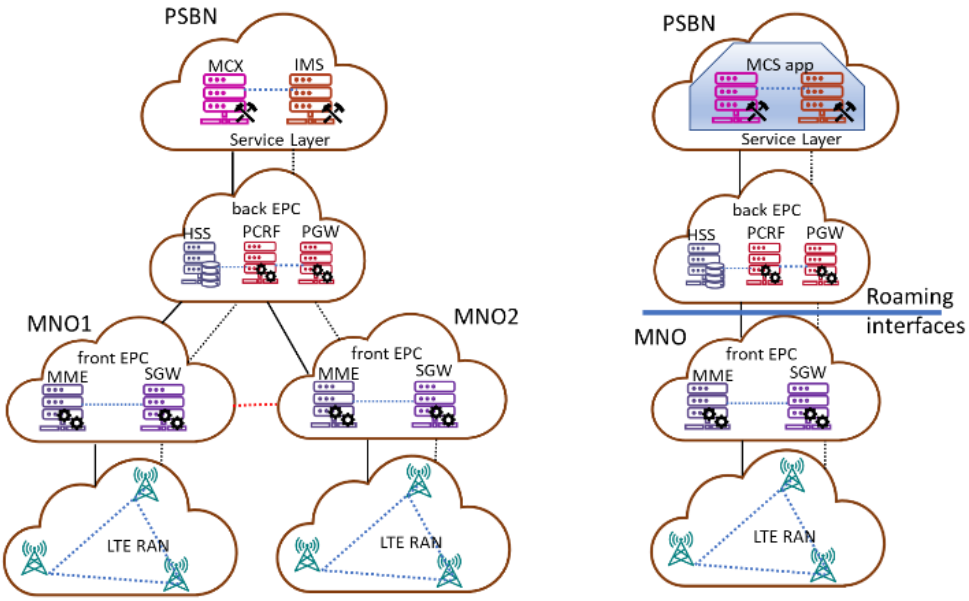


Figure 13: Variations of shared RAN(s) and dedicated CN with(out) roaming interfaces

PSBN owns MCS service layer, but share mobile network with MNOs

PSBN is built with shared RAN and CN with one or more MNOs in a country. A typical architecture is shown in Figure 14and have dedicated service layers such as MCS. The PSBN has no roaming interfces with MNOs.

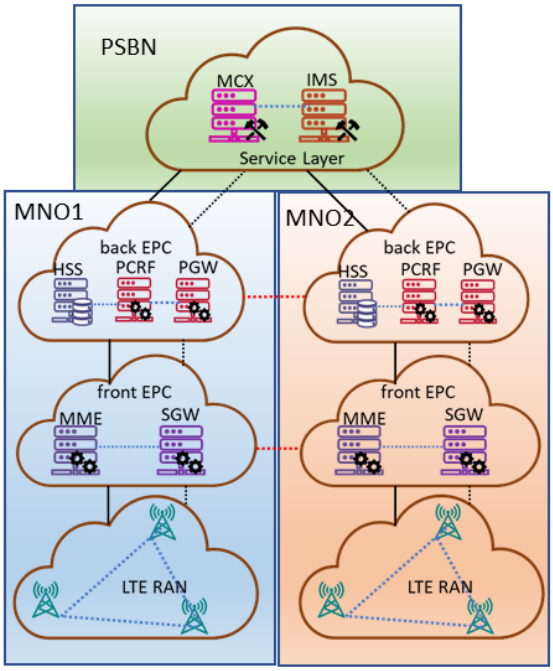


Figure 14: Shared mobile networks but with a dedicated MCS app network layer.

.

PSBN owns MCS service layer and HSS but shares the rest of the network with one or more MNOs

In this architecture model, PSBN owns only MCS service layer and HSS and shares the rest of the network with MNO(s) as shown in Figure 15.

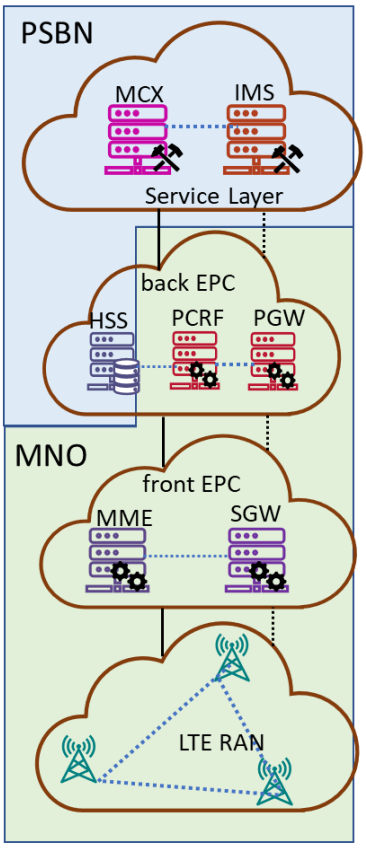


Figure 15: PSBN owns MCS service layer and HSS but shares the rest of the network with MNO(s)

MNOs providing public safety services.

A country does not build a dedicated PSBN but allows its MNO(s) to provide mission critical

communications services to its public safety and emergency service users. A typical architecture is

shown in **Error! Reference source not found.**.

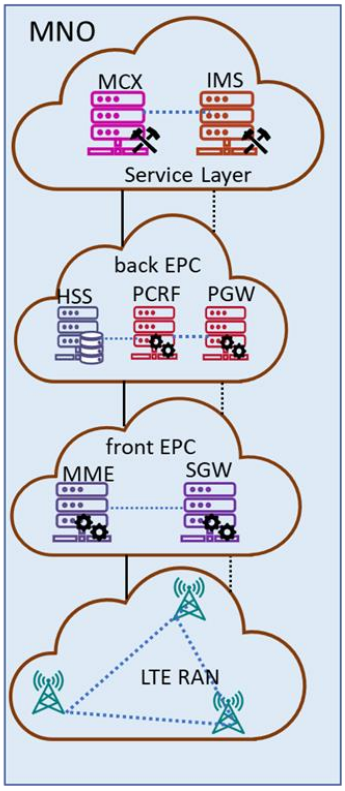


Figure 16: MNO(s) providing mission critical services: .

5.8.2 5G Deployment

As deployment options, most common adopted options are covered, as per standardisation that have been completed:

- 5G NSA Option 3
- 5G SA Option 2

Connectivity option	Core network	Master RAT	Secondary RAT	3GPP term	3GPP release
Option 3	EPC	LTE	NR	EN-DC	Rel. 15, Dec 2017
Option 2	5GC	NR	-	NR	Rel. 15, June 2018

Figure 17: 5G Deployment Options

5G NSA

5G NSA refers to the deployment where 5G is not used in Stand Alone mode, since it uses 5G components of only 5G Radio, i.e. 5G NR and the core network of 4G core, i.e. EPC core.

- 5G radio access technology (NR) and LTE are used simultaneously to provide radio access to users.
- This feature is referred to as “Dual Connectivity”, where architecture works in master-slave access node structure.

5G NSA deployment highlighted in **Error! Reference source not found.** can be implemented.

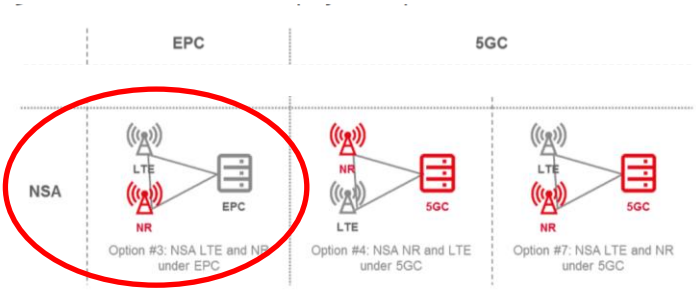


Figure 18: 5G NSA Deployment

5G NSA OPTION 3

In 5G NSA OPTION 3, Dual Connectivity refers to

- 4G access used as master node (EPC + 4G eNB master)
- 5G access used as secondary node (EPC + 5G en-gNB secondary)

Control plane goes through the master node whereas data plane is split across the master node and a secondary node and both LTE and NR are used for user data traffic (user plane).

Voice service is implemented as VoLTE since access to the network is provided via LTE control channels.

SMS service is implemented as it isfor LTE since access to the network is provided via the LTE control channel

5G SA Option 2

(To be completed)

5.9 Key Performances Indicators (KPIs)

The following KPIs are used for measuring the network performance including the Quality of Service.

5.9.1 General KPIs

KPI
LATENCY
JITTER
PACKET LOSS
THROUGHPUT
AVAILABILITY
DEFAULT/ DEDICATED BEARER (on Attach provides basic connectivity(/for specific QoS requirements)
GBR/Non-GBR/MBR/UE AMBR
QCI/5QI PRIORITY (Scheduling priority used for differentiating packet forwarding treatment between services with different QCI/5QIs)
PACKET ERROR RATE (upper bound for a rate of non-congestion related packet losses)
PACKET DELAY (upper bound for the time that a packet may be delayed between the UE and the Core network.)
ARP (Allocation/Retention Priority) (range of the ARP priority level is 1 to 15;1 being the highest priority)
PCI (Preemption Capability) / PVI (Preemption Vulnerability)

Table 3: General KPIs

5.9.2 KPI per type of Traffic (Value refer to domestic scenario)

KPI	Description	Definition	Value
KPI-1	MCPTT Access time	The time between when an MCPTT user request to speak and when this user gets a signal to start speaking, not including confirmation	<300ms
KPI-2	End-to-end Access time	The time between when an MCPTT user request to speak and when this user gets a signal to start speaking, including call establishment and acknowledgement	<1000ms
KPI-3	Mouth-to-ear latency	The time between an utterance by the transmitting user, and the playback of the utterance at the receiving user's speaker	<300ms
KPI-4	Late call entry time	The time to enter an ongoing MCPTT Group Call measured from the time that a user decides to monitor such an MCPTT Group Call, to the time when the MCPTT UE's speaker starts to play the audio.	<150ms or <350ms encrypted

Table 4: KPIs for MCPTT traffic

KPI	Description	Definition	Value
KPI-1	Urgent Transmission Delay	The delay in transmitting urgent real time video (after the request)	<2secs
KPI-2	Urgent End-to-end transmission delay	Time from transmitting MCVideo UE to receiving MCVideo UE or console for urgent real time video transmissions	<1 secs
KPI-3	Storing delay in MCVideo	Storing start from the time the user requests an MCVideo transmission. End to end shall not exceed 1 s plus the commencement delay (up to 2 s).	<= 2secs
KPI-4	Non Urgent Priority End-to-end transmission delay	Time from transmitted MCVideo UE to receiving MCVideo UE or console for non-urgent real time priority video transmissions s	<= 10 secs
KPI-5	Synchronization time	Synchronization between video and audio when played at the MCVideo receiving UE or console	<= 50 ms

Table 5: KPIs for MCVideo traffic

5.9.3 Standardised QoS Characteristics of MCS 5QIs

5QI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Averaging Window	Services
65	GBR	7	75 ms	10^{-2} 10^{-2}	2000 ms	Mission Critical user plane Push To Talk voice (E.g. MCPTT)
66	GBR	20	100 ms		2000 ms	Non-Mission-Critical user plane Push To Talk voice
67	GBR	15	100 ms	10^{-3}	2000 ms	Mission Critical Video user plane
69	Non-GBR	5	60 ms	10^{-6}		Mission Critical delay sensitive signaling (e.g. MCPTT signaling, MC Video signaling)
70	Non-GBR	44	200 ms	10^{-6}		Mission Critical Data (e.g. Www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)

Table 6: Standardized QoS characteristics of MCS 5QIs

6 Network Impact

6.1 MCX Service and associated Quality Parameters

An MCX VPLMN will be a VPLMN supporting the following MCX services:

- MCPTT
- MCVideo
- Short Data Service (MCData)
- Mission Critical Business Application (MCData)
- Non Mission Critical Business Application (OTT)
- VoLTE
- SMS

Those services are all based on data roaming (except SMSoNAS).

APN/DNN will be associated to those services. MC services' APNs are defined in the 3GPP TS 23.280 (subclause 5.2.7.0):

an MC services APN for the SIP-1 reference point,

an MC common core services APN for the HTTP-1 reference point

an MC identity management service APN for the CSC-1 reference point

1. The APN value of "IMS" is a well-known APN, whose PDN connection characteristics are defined in GSMA PRD IR.92 and GSMA PRD IR.88, and which is used in some deployments for operator IMS-based services e.g. Voice over LTE. This well-known APN can be used for the MC service APN if the SIP core belongs to the PLMN operator and both the PLMN operator and MC service provider have agreed which QoS aspects to utilise i.e. either the QoS aspects defined in subclause 5.2.7.2 of 3GPP TS 23.280 or the QoS aspects defined in GSMA PRD IR.92 and GSMA PRD IR.88.
2. The “IMS” APN for MCX services uses the default bearer QCI 5 for both VoLTE and MCX services. Therefore, mission critical QCI 69 cannot be used as default bearer. Furthermore, some data transfer and low priority signalling of MCX users may have to use QCI 5 default bearer.

Although 3GPP TS 23.179 and TS 23.280 allow the use of the well-known APN “IMS", TS 36.579-1 notes that, “handling IMS and MCX with one APN is theoretically possible but may have undesirable implications, e.g. VoLTE signalling could delay MCX signalling, therefore the assumption is that such implementations will be undesirable and unlikely.

MCPTT and MCData services are most likely be home-routed to HPLMN.

6.1.1 MCPTT

It is assumed that VPlMN is a PLMN supporting mission critical push to talk (MCPTT) services as specified by 3GPP TS 22.179, 3GPP TS 22.280, and 3GPP TS 23.379.

This document provides extra information for the VPLMN to support MCPTT services in a roaming relationship with a HPLMN that is a PLMN supporting MCPTT services.

It is assumed that MCPTT application level is totally controlled by HPLMN.

6.1.1.1 MCPTT roaming services

The following assumptions are made for MCPTT roaming:

1. MCPTT roaming services provided by VPLMN are Originating and Terminating Group Calls (including MCPTT emergency group calls) and Originating and Terminating Private Calls between two users (including MCPTT emergency private calls).
2. Origination and termination of the calls can be within VPLMN only, as well as between VPLMN and HPLMN.
3. Services referred to only relate to speech communications only.
4. The functional architecture is to support MC services over LTE, where MCPTT voice service in VPLMN uses E-UTRAN access based on the EPS architecture and Dual Connectivity access on 5G NSA architecture.
5. MCPTT calls are managed as Packet Switching Domain (e.g. VoLTE).
6. VPLMN has to be able to provide multiple parallel conversations for same group or same pair of users.

6.1.1.2 MCPTT Resource allocation

QoS settings/profile requested by the HPlMN should be in accordance with the Roaming Agreement. VPlMN controls QoS because VPlMN is always in charge of QoS parameters as its network is used to produce the service.

If a QoS profile is not explicitly described in the roaming agreement, then the default profile has to be implicitly considered and provided as described in “MCPTT Roaming information” of VPLMN GSMA PRD IR.21..

It is fundamental that HPlMN and VPlMN align on QoS parameter (for example, if HPLMN is requesting bearer setup with the PVI parameter value “off” and VPLMN uses a setting of “PVI value”on”, the connection setup will fail).

A minimum setting of QoS parameter shall be agreed by both parties representing HPLMN and VPLMN to avoid connection failures due to QoS parameters misalignment and agreed on the fallback setting to apply to the bearer dynamic downgrade. The table below defines the basic minimum QoS parameters that VPLMN shall support (Note: bilateral agreements may allow operators to negotiate other values).

QoS Parameters	MCPTT	MCX Signaling
QCI	65	69
ARP-PL (*)	2	1
ARP-PVI (**)	Enabled	Enabled
ARP-PCI)**)	Enabled	Enabled
MBR-UL	50 kbps	
MBR-DL	50 kbps	
GBR-UL	50 kbps	
GBR-DL	50 kbps	

Table 7: QoS parameters for MCPTT

(*) The use of ARP 1-8 traditionally reserved for home operator use applies to MCX operators in international roaming scenarios, according to specific International Roaming Agreement in place between parties (3GPP TS 23.203 6.1.7.3).

(**) The bearer request should not be denied based on PCI or PVI; instead, the VPLMN can change the requested PCI and/or PVI and accept the request. PVI downgrade is used to change the HPLMN Disabled request to Enabled in the VPLMN while PCI downgrade is used to change the HPLMN Enabled request to Disabled in the VPLMN, and vice versa for PVI/PCI upgrade (as per GSMA IR88 Annex E)

VPLMN has to be able to provide highest level of priority at Radio Access Network for MCPTT users by a prioritisation mechanism based on Quality of Service/Priority/Preemption/Access class baring, Quality of service Class identifier. VPLMN has to be able to assign different levels of Allocation and Retention Priority (ARP) to EPS bearers.

VPLMN has to be able to support different quality of service on the radio interface as per QCIs and 5QIs.

Resource allocation in a MCPTT call session request to the VPLMN is done using standardised QCI/5QI to QoS Characteristics. Non-standardised 5QI values may be also used (3GPP 23.179 and 23.280) in accordance with 3GPP TS 23.501.

QCI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Averaging Window	Services
65	GBR	0.7	75 ms	10^{-2}	2000 ms	Mission Critical user plane Push To Talk voice (E.g. MCPTT)
69	Non-GBR	0.5	60 ms	10^{-6}		Mission Critical delay sensitive signaling (e.g. MCPTT signaling, MC Video signaling)

Table 8: Standardised QCI

Value of 69 (Mission Critical delay sensitive signalling e.g., MCPTT signalling) is used on the default or a dedicated bearer and is used at PDN connection establishment.

Value of 65 (Mission Critical user plane Push To Talk voice) is used to setup a dedicated bearer for media traffic.

Considerations for the EPS bearers:

- The QCI value of 69 is used for the EPS bearer that transports SIP-1 reference point messaging (3GPP TS 23.203) and may also be used to transport floor control signalling.
- The QCI value 8 (as specified in 3GPP TS 23.203) or better shall be used for the EPS bearer that transports HTTP-1 reference point messaging. If QCI value 8 is not used for HTTP-1 transport, then caution should be exercised to ensure that a higher priority bearer (that is used for signalling) is not compromised by combining HTTP-1 traffic on this bearer (3GPP TS 23.203)
- The QCI value 65 (as specified in 3GPP TS 23.203) shall be used for the EPS bearer that transports MCPTT media and may also be used to transport floor control signalling.

VPLMN has to be able to apply the modification of the bearer priority, as well as to enable pre-emption of bearer wth lower priority (e.g., bearer modification applies to allocate resource to MCPTT emergency calls). Preemption of lower priority pre-emptible EPS bearers (for MCPTT or for other applications), in favor of the newly initiated MCPTT bearer may occur if the maximum number of bearers or maximum traffic capacity has been reached.

VPLMN has to be able to ensure that the MCPTT services always have access to a dedicated bearer for MCPTT, i.e., a pre-established session may be setup that includes a request for resources at the first MCPTT group affiliation. Other options might also be available (prearranged on-demand or chat call model). In pre-established sessions for MCPTT, resources can be pre-allocated at the session establishment or when the call actually starts. For pre-arranged on-demand models, resources are allocated at the call start (a SIP INVITE) and released at the call end (a SIP BYE), similar to VoLTE.

In chat call model, resources can be allocated at session establishment or when someone press the button to speak.

The ARP on the default bearer shall not be lower than the ARP assigned to the dedicated EPS bearer with the highest ARP priority.

The total number of simultaneous private calls is limited to 4 (3GPP TS 24.484) parallel private calls.

The total number of simultaneous group calls is limited to 255 (3GPP TS 24.483) parallel group calls. This total number may be smaller for roaming scenarios.

6.1.1.3 MCPTT Key Performance Indicators

VPLMN has to be able to ensure that performance indicators are preserved.

It is not expected that the level of performances in roaming will meet the same level as for domestic scenario.

The KPIs are referenced in section 4.9.2. KPI values and thresholds in roaming scenario shall be defined for validation of the service to go live and for quality of the service when QoS monitoring applies (see section 5.1.1.4).

VPLMN has to be able to guarantee MCPTT audio/voice quality is greater than or equal to 3.0 measured according to the ITU standard Perceptual Objective Listening Quality Assessment (POLQA) as defined in P.863.

Value 3.0 for audio/voice quality has to be considered as a safe value and as the lowest value in a congested network. Target value could be in the region of 4.0.

VPLMN has to be able to minimise private and group drop calls, as well as to manage drop calls within group calls, e.g., to keep the group communication ongoing even if one or some of the call legs are dropped.

6.1.1.4 Test of MCPTT Services and Quality of MCPTT services

In a roaming relationship, both HPLMN and VPLMN have to test MCPTT services, according to relevant IREG test book (IREG document to be provided): as an option a Subset of 3GPP TS 36.579 may be used for validating MCPTT services in roaming scenarios and expected level of performances indicator to be adjusted for roaming scenario.

After MCPTT has been made available/open as Outbound/Inbound roaming services, Quality of the Service can be monitored according to GSMA PRD IR.81 (IR81 voice section to be updated).

6.1.2 MCVideo

It is assumed that VPLMN is a PLMN supporting mission critical video (MCVideo) service as specified by 3GPP 3GPP TS 22.281, 3GPP TS 23.281, and 3GPP TS 22.280.

This document provides extra information for the VPLMN to support MCVideo service in a roaming relationship with a HPLMN that is a PLMN supporting MCVideo services.

It is also assumed that MCVideo application level is totally controlled by HPLMN.

6.1.2.1 MCVideo roaming services

MCVideo roaming services provided by VPLMN are Originating and Terminating Group Video Transmissions (including emergency video), and Originating and Terminating Private Video transmissions between 2 users (including emergency video). As part of video service, Video capture, Video streaming, Video encoding/decoding, Video storing are provided.

Origination and termination of video transmission can be within VPLMN only, as well as between VPLMN and HPLMN.

The functional architecture is to support MC services over LTE, where MCVideo service in VPLMN uses E-UTRAN access based on the EPC architecture and Dual Connectivity access on 5G NSA architecture.

VPLMN has to be able to ensure integrity, confidentiality and accuracy of the video information for stored video.

VPLMN has to be able to provide multiple parallel sessions for same group or same pair of users.

6.1.2.2 MCVideo Resource allocation

QoS settings/profile requested by the HPLMN should be in accordance with the Roaming Agreement. VPLMN controls QoS, because VPLMN is always in charge of QoS parameters as its network is used to produce the service.

If a QoS profile is not explicitly described during the roaming agreement definition, then default profile has to be implicitly considered and provided as “MCVideo Roaming information” of VLPLMN GSMA PRD IR.21.

It is fundamentally important that HPLMN and VPLMN align on QoS parameters (for example if HPLMN is requesting bearer setup with the PVI parameter value “off” and VPLMN uses a setting of “PVI=on”, the connection setup will fail).

A minimum setting of QoS parameters shall be agreed by both parties representing HPLMN and VPLMN to avoid connection failures due to QoS parameter misalignment and to agree on the fallback setting to apply to the bearer’s dynamic downgrade. The table below defines the basic minimum QoS parameters that VPLMN shall support (However, bilateral agreements may allow operators to negotiate other values).

QoS Parameters	MCVIDEO	MCX Signaling
QCI	67	69
ARP-PL (*)	3	1
ARP-PVI (**)	Enabled	Enabled
ARP-PCI)**)	Enabled	Enabled
MBR-UL	3.5 Mbps	
MBR-DL	3.5 Mbps	
GBR-UL	384 kbps	
GBR-DL	384 kbps	

Table 9: Roaming QOS values for MCVideo

(*) The use of ARP 1-8 traditionally reserved for home operator use applies to MCX operators in international roaming scenarios, according to specific International Roaming Agreement in place between parties (3GPP TS 23.203 6.1.7.3).

(**) The bearer request should not be denied based on PCI or PVI; instead, the VPLMN can change the requested PCI and/or PVI and accept the request. PVI downgrade is used to change the HPLMN Disabled request to Enabled in the VPLMN while PCI downgrade is used to change the HPLMN Enabled request to Disabled in the VPLMN, and vice versa for PVI/PCI upgrade (as given in GSMA PRD IR.88 Annex E).

VPLMN has to be able to provide appropriately higher level of priority at Radio Access Network for MCVideo users by a prioritisation mechanism based on Quality of Service/Priority/Preemption/, and Quality of service Class identifier.

VPLMN has to be able to assign different levels of Allocation and Retention Priority (ARP) to EPS bearers.

VPLMN has to be able to support different quality of service on the radio interface as per QCIs and 5CIs.

Resource allocation in a MCVideo call session request to the VPLMN is done using standardised QCI or 5QI to QoS Characteristics. . Non-standardised 5QI values may be also used (3GPP 23.179 and 23.280) in accordance with 3GPP TS 23.501.

QCI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Averaging Window	Services
67	GBR	1.5	100 ms	10^{-3}	2000 ms	Mission Critical Video user plane
69	Non-GBR	0.5	60 ms	10^{-6}		Mission Critical delay sensitive signaling (e.g. MCPTT signaling, MC Video signaling)

Table 10: Standardised QCIs for MCVideo

QCI Value of 67 (Mission Critical Video user plane- real time mode), QCI Value of 7, or QCI Value of 4 (Mission Critical Video user plane- non real time mode), and QCI value of 69 Mission Critical delay sensitive signalling (e.g., MC video signalling) are used to setup a dedicated bearer.

Considerations for the EPS bearer to the MC services PDN:

- The QCI value of 69 is used for the EPS bearer that transports SIP-1 reference point messaging (3GPP TS 23.203).

Considerations for the EPS bearer to the MC common core services PDN and MC identity management service PDN:

- The QCI value 8 (as specified in 3GPP TS 23.203 [8]) or better shall be used for the EPS bearer that transports HTTP-1 reference point messaging. If QCI value 8 is not used for HTTP-1 transport, then caution should be exercised to ensure that a higher priority bearer (that is used for signalling or media) is not compromised by combining HTTP-1 traffic on this bearer (3GPP TS 23.203).

VPLMN has to be able to apply modification of the bearer priority, as well as to enable pre-emption of bearer of lower priority (e.g. bearer modification applies to allocate resource to MCVideo emergency transmission). Preemption of lower priority pre-emptible EPS bearers (for MCVideo or for other applications), in favour of the newly initiated MCVideo EPS bearer, may occur if the maximum number of bearers or maximum traffic capacity has been reached.

6.1.2.3 MCVideo Key performance indicators

VPLMN has to be able to ensure that video performances indicators are preserved.

It is not expected that the level of performances in roaming will meet the same level as for domestic scenario.

Referenced KPI are set in section 4.9.2 KPI value and threshold in roaming scenario shall be defined for validation of the service to go live and for quality of the service when QoS monitoring applies(see section 5.1.2.4 of this document)

VPLMN has to be able to support video codec as per 3GPP TS 26.281.

VPLMN has to be able to minimise loss/ interruption of a video stream.

6.1.2.4 Test of MCVideo Services and Quality of MCVideo services

In a roaming relationship both HPLMN and VPLMN have to test MCVideo services, according to relevant IREG test book.

(IREG document to be provided): as an option a Subset of 3GPP TS 36.579 may be used for validating MCPTT services in roaming scenarios and expected level of performances indicator to be adjusted for roaming scenario).

After MCVideo have been made available or opened as Outbound/Inbound roaming services, Quality of the Service can be monitored according to IR81 PRD (IR81 video section to be updated).

6.1.3 MCData

It is assumed that VPLMN is a PLMN supporting mission critical data (MCData) services as specified by 3GPP TS 22.282. and, 3GPP TS 23.282.

This document provides extra information for the VPLMN to support MCData services in a roaming relationship with a HPLMN that is a PLMN supporting MCData services.

It is also assumed that MCData application level is totally controlled by HPLMN.

6.1.3.1 MCData roaming services

MCData service is totally managed by HPLMN and Home Routed. IP connectivity is provided by VPLMN.

6.1.3.2 MCData Resource allocation

QoS settings/profile requested by the HPLMN should be in accordance with the Roaming Agreement. VPLMN controls QoS because VPLMN is always in charge of QoS parameters and its network is used to produce the service.

If a QoS profile is not explicitly described during the roaming agreement definition, then default profile has to be implicitly considered and provided as “MCData Roaming information” of VLPLMN GSMA PRD IR.21..

It is fundamentally important that HPLMN and VPLMN align on QoS parameters (for example, if HPLMN is requesting bearer setup with the PVI parameter value “off” and VPLMN uses a setting of “PVI=on”, the connection setup will fail).

A minimum setting of QoS parameter shall be agreed by both parties representing HPLMN and VPLMN to avoid connection failure due to QoS parameters misalignment and to agree on the fallback setting to apply to the bearer dynamic downgrade. The table below defines the basic minimum QoS parameters that VPLMN shall support (However, bilateral agreements may allow operators to negotiate other values).

QoS Parameters	MCDATA	MCX Signaling
QCI	70	69
ARP-PL (*)	4	1
ARP-PVI (**)	Enabled	Enabled
ARP-PCI)**)	Enabled	Enabled
MBR-UL		
MBR-DL		
GBR-UL		
GBR-DL		

Table 11: QoS parameters for MCData

(*) The use of ARP 1-8 traditionally reserved for home operator use applies to MCX operators in international roaming scenarios, according to specific International Roaming Agreement in place between parties (3GPP TS 23.203 6.1.7.3).

(**) The bearer request should not be denied based on PCI or PVI; instead, the VPLMN can change the requested PCI and/or PVI and accept the request. PVI downgrade is used to change the HPLMN Disabled request to Enabled in the VPLMN while PCI downgrade is used to change the HPLMN Enabled request to Disabled in the VPLMN, and vice versa for PVI/PCI upgrade (as per GSMA IR88 Annex E)

VPLMN has to be able to provide appropriate level of priority at Radio Access Network for MCData users by a prioritisation mechanisms based on Quality of Service/Priority/Preemption and Quality of service Class identifier, as well as it has to be able to assign different levels of Allocation and Retention Priority (ARP) to EPS bearers.

VPLMN has to be able to support different quality of service on the radio interface as per QCIs and 5QIs.

Resource allocation in a MCData session request to the VPLMN is done using standardised QCI or 5QI QoS Characteristics. Non-standardised 5QI values may be also used (3GPP 23.179 and 23.280) in accordance with 3GPP TS 23.501.

QCI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Averaging Window	Services
69	Non-GBR	0.5	60 ms	10^{-6}		Mission Critical delay sensitive signaling (e.g. MCPTT signaling, MC Video signaling)
70	Non-GBR	5.5	200 ms	10^{-6}		Mission Critical Data (e.g. Www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)

Table 12: Standardised QCIs for MCData

QCI value of 70 (Mission Critical Data) is used to setup a dedicated bearer.

Considerations for the EPS bearer to the MC services PDN:

- The QCI value of 69 is used for the EPS bearer that transports SIP-1 reference point messaging (3GPP TS 23.203)

Considerations for the EPS bearer to the MC common core services PDN and MC identity management service PDN:

- The QCI value 8 (as specified in 3GPP TS 23.203]) or better shall be used for the EPS bearer that transports HTTP-1 reference point messaging. If QCI value 8 is not used for HTTP-1 transport, then caution should be exercised to ensure that a higher priority bearer (that is used for signalling or media) is not compromised by combining HTTP-1 traffic on this bearer (3GPP TS 23.203)

6.1.3.3 MCData Key performance indicators

IP Connectivity KPIs to be completed.

6.1.3.4 Test of MCData Services and Quality of MCData services

In a roaming relationship, both HPLMN and VPLMN have to test MCData services, according to relevant IREG test (IREG document to be provided): as an option a Subset of 3GPP TS 36.579 may be used for validating MCPTT services in roaming scenarios and expected level of performances indicator to be adjusted for roaming scenario).

After MCData have been made available or opened as Outbound/Inbound roaming services, Quality of the Service can be monitored according to GSMA PRD IR.81 (IR81 data session to be updated).

6.1.4 VOLTE and SMS

To support VoLTE and SMS, generic VoLTE roaming QoS recommendations listed in GSMA PRD IR.88 Annex E applies.

6.1.5 Non Mission Critical Business Application (OTT)

To be completed

6.1.6 Interoperability and Common requirements

Purpose of this section is to address interoperability aspects of Common Requirements and MCX services in roaming scenarios.

6.1.6.1 Application layer priorities

MCX Service priority requirements are mapped to priority levels and multiple pre-emptive priorities.

A pre-emption hierarchy for MCX Service Group transmissions and the permission to pre-empt other voice and video services in favour of MCX Service communications are managed by HPLMN.

6.1.6.2 Inter-MCX Service interworking

Following requirements are needed to be specified/confirmed for roaming scenarios (3GPP TS 22280-j10 8.2.2)

- When operating multiple MCX Services on the same network, radio resources shall be able to be utilised in an efficient manner for all MCX Services up to specific thresholds defined for each MCX Service and/or the combination of MCX Services. The radio resource allocation for each MCX Service and the combination of MCX Services shall be flexible based on demand, or allocated in a predefined manner.
- The network shall be able to assign radio resources so that resources assigned to each MCX Service, or the combination of all MCX Services stay below a threshold, subject to the agreement between the 3GPP network operator and the Mission Critical Organisation(s) (e.g., 3GPP network can be operated by Mission Critical Organisation(s), or 3GPP network is operated by commercial operator), for resources to be used for MCX Services without impacting other non-MCX Services.

6.2 Roaming partner agreement

MCX roaming services are provided by an MCX Visited Network to an MCX Home Network using an MCX roaming agreement.

Different approaches could be defined to build a MCX roaming agreement between the MCX Visited Network and the MCX Home Network, which are:

1. Use a bilateral relationship
2. Via a roaming hub, acting as an enabler between the MCX VPLMN and MCX HPLMN
3. Via another HPLMN already having a bilateral relationship with the MCX VPLMN

6.2.1 Bilateral Roaming Agreement

The bilateral agreement is the basic one.

It is a direct agreement between the MCX VPLMN and the MCX HPLMN.

New comers on the roaming market are likely to find it difficult to form bilateral MCX roaming agreements.

6.2.2 Via Roaming Hub

An alternative is to use a Roaming Hub, and to be able to implement MCX roaming between MCX VPLMN and MCX HPLMN.

All the contracts, tests, and billing will be managed by the Roaming Hub minimising the impact on the MCX VPLMN side.

The Roaming Hub will have to upgrade their systems in order to become MCX compliant.

An assumption is made that MCX services could be considered as data services for the Roaming Hub minimising the impact on Roaming Hub’ s systems.

Billing flows are cascaded by the Roaming Hub.

6.2.3 Via another HPLMN (Sponsor Roaming)

The MCX HPLMN can asks another MCX HPLMN (Sponsor) to reuse their MCX roaming agreements with their MCX VPLMNs.

A SIM applet will be used on the MCX user’s SIM to change user identity (using the Sponsor identity) when exchanging signalling/data with a MCX VPLMN.

The MCX VPLMN will accept this user and relay signalling/data to the sponsor.

The sponsor will adopt the original MCX user identities and send the traffic to the MCX HPLMN.

Billing flows will be cascaded by the sponsor.

6.3 Steering of Roaming (SoR)

Steering of Roaming (SoR) is a technology enabling the HPLMN to steer the roaming traffic to the preferred VPLMN based on diverse commercial and technical considerations

Considering the nature of Mission Critical communications, hybrid mode SoR (a combination of OTA and signalling based on the guidelines as defined in GSMA PRD IR.73) is recommended in order to optimise the time required to select and attach to a VPLMN.

Following are some key factors to consider as they relate to SoR for MCX:

The HPLMN may need to steer MCX and non-MCX subscribers differently. It is therefore recommended that the SoR solution is MCX-service-aware and ideally matching subscribed services of roaming users and VPLMN capabilities.

When VPLMNs in the visited country do not support MCX or the roaming agreements do not include MCX, then regular business as usual steering rules and methods must apply.

If there is a single MCX VPLMN in the visited country, the steering solution should direct roaming MCX users towards that MCX VPLMN whenever possible.

If the HPLMN has a roaming agreement with only one MCX VPLMN in the visited country and the MCX VPLMN is not available at the time of network selection, the HPLMN must decide whether to allow registration on a non-MCX VPLMN. Typically, in such scenarios, SoR must allow registration on a non-MCX VPLMN to ensure the roaming UE can enjoy access to basic non-MCX services, and MCX services are provided with commercial grade Quality of Service, if required. In this scenario, it is assumed that a periodic reselection mechanism will be used to periodically scan to search for the preferred MCX VPLMN. The reselection mechanism may rely upon SIM card files (such as the preferred PLMN list) or steering of roaming control information (SOR-CMCI) as defined in GSMA PRD IR.73 section 9.4.

Whenever an HPLMN has agreements with multiple MCX VPLMNs then SoR technology may be employed to direct traffic to one of the available MCX VPLMNs based on commercial and/or technical considerations.

It is worth noting that some level of service awareness is available in commercially available Steering of Roaming solutions (e.g., VoLTE, 5G, IoT). However, support of MCX awareness will have to be specifically developed to incorporate the recommendations in this document.

6.3.1 Steering of Roaming option 1 – Signalling rejection

SoR may be based on signalling, OTA or on a combination of both. Signalling based SoR typically rely on rejection of registration attempts from a non-preferred network to direct the roaming device to select one of the preferred networks. If this option is not carefully optimised, signaling rejections have the potential to increase the time to complete registration in the roaming network. Therefore, it is recommended to avoid signalling rejection for MCX roaming users whenever possible. However, if no MCX VPLMNs are available in a visted country signaling rejection SoR and regular/BAU (Business As Usual) SoR can be applied.

6.3.2 Steering of Roaming option 2 – Dynamic preferred PLMN

As mentioned in the fourth key factor in section 5.3, SoR may rely upon certain files stored in the SIM card and updated dynamically over the air (OTA) using various methods such as OTA, SMS in 2G, 3G, or 4G, or during the registration procedure in 5G SA.

The use of preferred PLMNs in SIM files is quite suitable for MCX roaming devices as it minimises the time that a roaming UE takes to select the preferred MCX VPLMN and to provide a method for roaming devices to perform reselection and choose a MCX-VPLMN when MCX-VPLMN has not been found during the initial registration.

6.4 Access Priority

Access priority mechanism could be configured on the Radio Access Network (RAN) in order to prioritise the radio access for MCX users.

6.4.1 Access Class

Access Class (AC) is employed to create access priority on RRC connection (radio connections) setup attempts of UEs. The Access Class is associated with a UE on a semi-permanent basis and is provisioned by HPLMN HSS and also configured in each SIM/USIM manually or over the air update.

ACs consist of sixteen enumerations from 0 to15. ACs enumerated from 0 to 9 are for commercial users and are randomly allocated to all UEs, are stored in the USIM. Additionally, UEs may belong to one or more of the five special ACs enumerated from 11 to 15 that are also stored in the USIM.

The ACs from 11 to 15 are allocated to specific high priority users as follows:

- Class 15 - PLMN Staff;
- Class 14 - Emergency Services;
- Class 13 - Public Utilities (e.g. water/gas suppliers);
- Class 12 - Security Services;
- Class 11 - For PLMN Use.

Access Classes are applicable in the networks as follows (3GPP TS 22.011):

- Classes 0 - 9 - Home and Visited PLMNs;
- Classes 11 and 15 - Home PLMN only if the Equivalent Home PLMN (EHPLMN) list is not present or any EHPLMN;
- Classes 12, 13, 14 - Home PLMN and visited PLMNs of home country only.

For this purpose, the home country is defined as the country of the MCC part of the IMSI.

Therefore, it can be concluded that Access Priority for mission critical services does not apply to UEs roaming internationally. They will be treated as UEs with normal priority (with ACs from 0 to 9) when they roam overseas.

Hence, the subsequent description of access priority and the Access Class Barring (ACB) is applicable only to national roaming within home country mobile networks that share the same Mobile Country Code (MCC).

AC is not a bearer related QoS attribute like QCI/5QI or ARP and applied merely to RRC connections between UE and MME.

Access Class can be used to control RRC Connection overload by barring low priority AC users' immediate access and allowing delayed network access when RRC Connection load exceeds a certain threshold.

It must be noted that Access Class Barring (ACB) is applied only to mobile originating RRC connection attempts with the establishment cause of MO signalling or MO data when UEs

are in idle mode. ACB does not bar handovers, and mobile terminated attempts, and does not stop ongoing traffic nor remove ongoing RRC connected UEs. If EUTRAN of the network supports a capability called Service Specific Access Control (SSAC), the network can selectively apply ACB for telephony services (MMTEL and Circuit Switched Fallback) for mobile originating session requests from idle mode and connected mode. An additional control known as "Access Class 10" is also signalled over the radio interface to the UE. This indicates whether or not network access for emergency calls is allowed for UEs with access classes 0 to 9 or without an IMSI. For UEs with access classes 11 to 15, emergency calls are not allowed if both "Access Class 10" and the relevant Access Class (11 to 15) are barred. Otherwise, emergency calls are allowed.

Access Class Barring mechanism can help prioritise roaming emergency services traffic users within a country if such users are assigned Access Class 14 and the networks allow Access Class 14 to make RRC connection attempts during congestion.

If a mobile network is hosting visiting mission critical communication users from a public safety network abroad, the hosting mobile network should disable Access Class Barring feature to its home subscriber users in the area where visiting international mission critical users are.

This is because international mission critical users with special Access Class are considered normal Access Class users while they are roaming internationally and can be denied or delayed access to the hosting network during network congestion if the Access Class Barring is active for local users.

In summary, the effectiveness of the access-priority-based control also known as Access Class Barring is limited because:

1. This applies only to mobile originated connections from idle UEs in HPLMN or EHPLMN and its home country networks, and other traffic are not affected.
2. It depends entirely on the UEs' compliance to 3GPP procedures. i.e., rogue UEs that do not comply with 3GPP procedures of ACB can cause congestion.
3. Already active connections can still cause congestion with their communications.
4. Mobile terminating connections are not barred based on ACs and can still cause congestion in the networks.
5. It is also vulnerable to Denial-of-Service attacks during congestion utilising the above gaps in ACB by hostile elements.
6. Not all the radio access network providers may implement/ may have plan for implementing special access classification for MCX.

6.5 Seamless mobility

6.5.1 Overview

Seamless mobility is uninterrupted user experience of communication services when the user moves from one serving cell to another. The duration of a temporary loss of network connection should be short enough for any service in use to have a seamless mobility experience.

Handing over an active connection from the core network of PLMN A (e.g. HPLMN) to the core network of PLMN B (e.g. a VPLMN) will cause a minor temporary interruption to the connection. This can be due to, for example, long geographical distance (in hundreds of kilometres) between the locations of core network functions, such as MME orchestrating the inter-PLMN handover, and the possibility of required inter-PLMN functions not being connected via the most optimal IP connection.

Additionally, a use case can also impose a connection interruption. For example, a police chase crossing a country border at a speed of 200kmph will cause a temporary connection interruption to an MCPTT call during a handover procedure. Therefore, achieving a perfectly seamless handover to an MCPTT call may not be a realistic target in all the international roaming deployment scenarios. The prospect of seamless handover in these scenarios can be validated by pilot test projects run in the real world, for example, as part of EU's 5G NETC (Northern European Transport Corridor) project.

The following section describes the model for seamless mobility in the context of the cross-border MCX service. The handover model is the long-term target model.

In the interim, there also exists several preliminary solutions which do not achieve the full seamless mobility as such but still offer significant reduction of the delay incurred during the regular roaming handover. These solutions could be potentially deployed faster and/or cheaper than the long-term target of seamless mobility.

The interim solutions can fulfil the requirements of some use cases but may not fulfil those of the most demanding use cases such as a police chase. The solutions are described in the following sections.

Error! Reference source not found. shows the summary of the solutions:

Description	Target PLMN is EPLMN	No EPLMN	Voice impact	Data impact	Implementation effort
UE is in idle mode					
Cell Selection at PLMN border (no neighbor cell information provided to UE)	UE picks target PLMN after 9s	UE picks target PLMN cell after **~60s**	No calls can be received or initiated during the PLMN change period	No data can be exchanged during the PLMN change period	low
Cell ReSelection at PLMN border (neighbor cell information (EARFCN aka	UE picks target PLMN instantly **200ms** after reading SIBs	UE does not pick target PLMN cell if serving PLMN cell is available. If any Serving PLMN cell is not	No calls can be received or initiated during the PLMN change period	No data can be exchanged during the PLMN change period	Medium

frequency channel) provided to UE)		available, UE picks a target PLMN cell after **~60s**			
UE is in connected Mode					
Cell Selection at PLMN border (no neighbour cell information provided to UE)	UE drops the connection and enters idle mode. Then UE picks target PLMN within **2s.**	UE drops the connection and enters idle mode. Then UE picks target PLMN cell after ~**60s**	The ongoing call get dropped. User has to initiate the call again	No data can be exchanged during the PLMN change period. A prolonged delay (varies) can drop application layer data connection	low
ReDirect: serving PLMN cell redirect to a target PLMN frequency	UE picks target PLMN within **200ms**	UE does not pick target PLMN cell if serving PLMN cell is available. If any serving PLMN cell is not available, UE picks a target PLMN cell after **~60s**	The ongoing call gets dropped	No data can be exchanged during the PLMN change period. A prolonged delay (varies) can drop application layer data connection	Medium
Handover	UE is instructed from network to pick a target PLMN cell	Not applicable as the network instructs the UE to use the target PLMN network	No impact due to seamless mobility	No impact due to seamless mobility	High

Table 13: Summary of solutions

Error! Reference source not found. describes the requirements to implement each solution.

Note: for seamless mobility, the proposed solution is required to have overlapping coverage of the serving PLMN and target PLMN at the border.

Solution	Requirements
Idle mode	
Cell Selection	MME configuration: target PLMN as ePLMN in NAS message
Cell ReSelection	MME configuration: target PLMN as ePLMN in NAS message Target Cell as neighbour cell
Connected mode	

Cell Selection	MME configuration: target PLMN as ePLMN in NAS message
ReDirect	MME configuration: target PLMN as ePLMN in NAS message eNodeB Configuration: target frequency, event threshold
Handover	MME configuration: target PLMN as ePLMN in NAS message and in HORL (Handover Restriction List) S10 Interface connectivity between source PLMN and target PLMN DNS connectivity between source PLMN and Target PLMN DNS configuration of the TAI eNodeB configuration: set the target Cell as neighbour, deactivate the X2 handover, and set the offset attribute GTP FW configuration: if the packet inspection is activated

Table 14: the basic requirements of the proposed solutions

6.5.2 Inter PLMN Mobility

Inter PLMN mobility requires a differentiation of the RRC States: RRC Idle or RRC connected. For each RRC state, different mobility scenarios can be manifested.

Note: in order to enable the seamless mobility easily it is recommended to have specific IMSI range for the MCX users.

6.5.2.1 Mobility scenarios in RRC IDLE

In RRC IDLE state, UE has no established RRC connection to the registered network. The processes and actions are UE driven.

6.5.2.1.1 Cell Selection

When UE camps on a cell and the cell becomes “unsuitable” (S criterion < 0), it enters the Cell Selection mode. the UE starts searching for alternative cells.

- Case 1: If target PLMN is in the list of the EPLMN, the decoding of SIB messages immediately leads to the attach message. The UE directly picks that cell, tries to connect and succeeds.
- Case 2: If target PLMN is not in the list of EPLMN, the UE continues scanning all RATs of available PLMNs. After an additional ~51s, the only available cell is picked. Target PLMN is selected only as the last resort, if no serving PLMN is available on any frequency and RAT.

The better option is to add the target PLMN to the EPLMN list in NAS message as part of the MME configuration.

6.5.2.1.2 Cell Reselection

In this case, target PLMN eNodeB cells are defined as neighbour cells in a serving PLMN eNodeB cell. In this cell reselection scenario, the signal power of serving PLMN cell is smoothly degraded until the criteria for reselection is met. The UE attempts to select the target PLMN neighbour cell starting with reading SIB1.

- Case 1: If target cell's PLMN is in the list of EPLMN, the cell is picked immediately after decoding SIB1 messages.
- Case 2: If target cell's PLMN is not in the list of EPLMN, SIB is decoded, but UE does not try to attach to this cell. UE remains in the serving PLMN's cell.

To allow this cell reselection in idle mode, the target eNodeB shall be added as a neighbour to source eNodeB and to MME configuration while the target PLMN is also added as EPLMN.

6.5.2.2 Mobility scenarios in RRC connected mode

In RRC connected mode, the UE has an established RRC connection with the registered network. The call processing is controlled by network's signaling.

6.5.2.2.1 Cell Selection

If UE is in RRC connected mode and loses serving cell, it will adopt the state of Radio Link Failure.

In that phase, the UE enters PLMN and Cell Selection mode. The UE starts searching for an alternative cell and selects a suitable cell in the target PLMN. There are two cases to this process:

- Case 1: If the target cell's PLMN is an EPLMN, and after 2 seconds the serving PLMN becomes unavailable the roaming procedure as described above for cell selection in RRC idle mode applies and
  TAU/TAU Reject with the cause of "implicitly detached" is signaled due to the roaming policy,
  Attach/Attach Accept is applied and a new IP address is assigned to the UE.
- Case 2: If the target cell is not in the list of EPLMN, the UE picks the target cell after about 60s or even longer when crossing borders. It highly depends on available RATs and the PLMN(s), which must be scanned, listed and sorted according to the priority order by the UE with number of base stations or MME. This process can be improved by providing a priority list including allowed / not allowed RATs and PLMNs to UE as the list is shorter.

6.5.2.2.2 Redirect

This feature requires configuring the target cell as a neighbour in the source network and redirecting event trigger threshold. The target frequency must be defined. Redirect can be configured with or without neighbour cell measurements. The procedure is as follows:

UE is served by a cell in RRC connected mode. When UE reaches the serving cell boarder it reports "Event A2" (Serving cell's coverage measurements becomes worse than a set threshold). As a result, the serving PLMN network triggers the redirect process.

Technically, it is an RRC connection release redirecting to a target frequency.

When the UE receives the RRC connection release it enters RRC idle mode, selects the given target frequency and attempts to get access to a new cell in the target PLMN.

This means that a “Redirect” always enforces the UE to enter PLMN and join the Cell Selection process with the aim of speeding up the PLMN search procedure by redirecting to the right carrier in a given PLMN.

Serving PLMN sends “RRC Connection Release” including target PLMN target frequency. UE enters idle mode, selects a target PLMN cell and reads SIBs.

- If the target cell is EPLMN, UE starts decoding SIB at the target frequency and immediately selects a cell in the target frequency after 200ms. The UE does not need to scan for other cells as this cell is suited and available immediately.
- If no EPLMN is configured, the network redirects UE to a target frequency. UE starts to decode target cell’s SIB message but does not try to attach to that cell. Then the UE again reads SIB of a HPLMN cell and connects back to HPLMN. Network starts to redirect to a target cell. This process continues until either a serving PLMN cell’s coverage gets stronger again (above threshold) or serving PLMN loses service (out of coverage) to the UE.

6.5.2.2.3 Handover

As UE moves away from serving network coverage, the connection continues in a target network. In this solution, the handover to the target network is triggered from the source network based on the reports of continuous UE’s RRC connected mode measurements of the neighbour cells. The serving cell makes the decision to move the connection to target network according to local configuration as shown in **Error! Reference source not found.**.

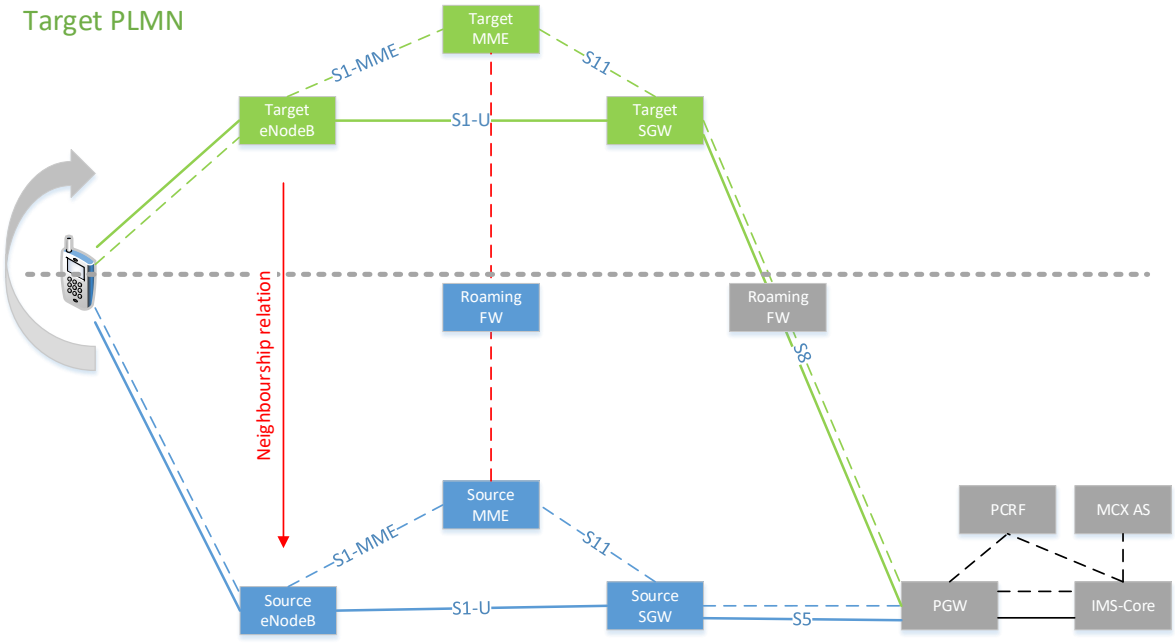


Figure 19: Seamless Mobility handover architecture

Error! Reference source not found. shows the architecture of seamless mobility in 4G network scenario where the source PLMN (in blue) and the target PLMN (in green) are not the same as the HPLMN (in gray).

In order to achieve the inter-PLMN handover, the following changes need to be considered:

- MMEs in source PLMN (it can be either a HPLMN or a VPLMN) and target PLMN (another VPLMN) need to be connected through S10 Interface where both source PLMN and target PLMN can be VPLMNs.
- The target eNodeB needs to be configured as a neighbour in source eNodeB and X2 (eNodeB to eNodeB) Handover needs to be deactivated.
- MME shall restrict the handover using the EPLMN configuration for a selected IMSI range of the MCX users.
- If the inspection is activated in IPX Firewall, the S10 Interface needs to be routed through IPX Firewall in order to allocate a tunnel identity and accept the “modify bearer request” signaling later.
- The target DNS shall be configured in order to resolve the target Cell’s Tracking Area Identity (TAI) to the target MME. The TAI shall be configured in target DNS generally in order to give access to entries from the source DNS.

Error! Reference source not found. shows the Inter-PLMN handover message flow:

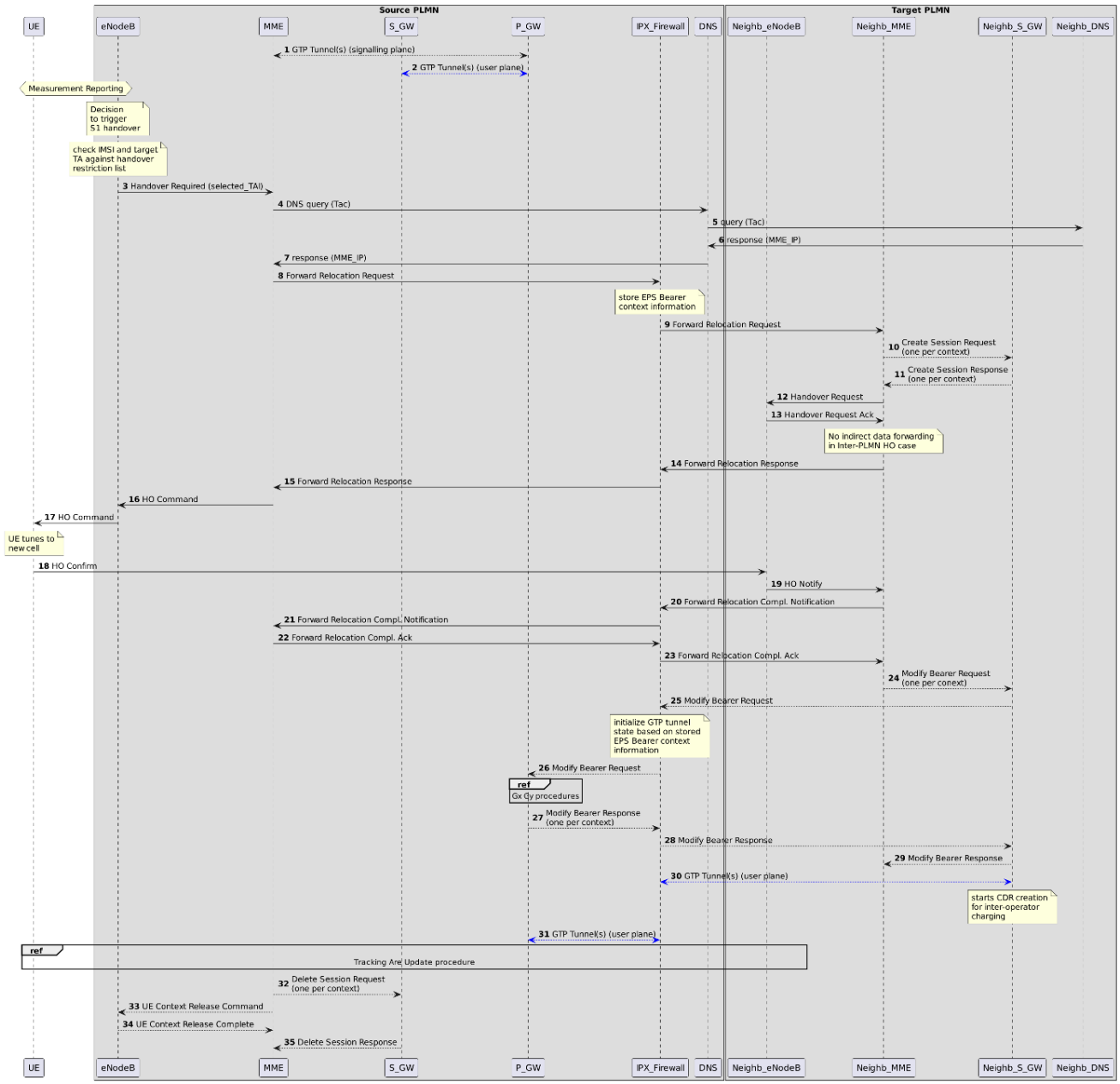


Figure 20: Inter-PLMN Handover message flow

The source eNodeB evaluates the measurement reports from the UE against the handover criteria. To allow handover towards the neighbour PLMN and trigger S1 handover, a required message with the selected TAI is sent.

The source MME tries to resolve the selected TAI from the DNS in order to get the target MME’s IP address.

Once the handover is confirmed, the UE triggers “Tracking Area Update” procedure as the MME has been changed.

The 3GPP 23.401 provides more information about the messages in this procedure.

Main challenges to handover processes are:

1. **Lawful interception:** This will not be possible since SIP signaling encryption in (IMS or SIP core) have to be enabled in public safety networks.
2. **ANR (Automatic Neighbour Relation) feature:** ANR function in the network is responsible for creating a handover relations between candidate cells according to the UEs' reported cell measurements. eNodeB can instruct the UEs what frequencies shall be scanned. In boarder scenarios, if the target network uses the same frequencies as the source network, then the UE reports the target network in its cell measurements and the eNodeB adds the reported cells as candidates for inter-PLMN handover even if this location is not desired for inter-PLMN handover. In this case, the operator cannnot control as to what area the Inter-PLMN handover is allowed and all the attributes of the handover relations such as offsets which are most important attributes in order to control the handover trigger areas and to avoid big traffic shift to the target operator.

Error! Reference source not found. shows a scenario where the decision has been made to allow the handover only in a specific area (indicated by "Handover required") though the handover is possible in two areas ("Handover required" and "Handover not required") according to ANR feature measurements.

Figure 21: An example of handover requirements in a geographical context

1. **Network architecture:** In many networks, the MMEs are configured as a pool. During the initial attach the UE gets a serving MME, which could not be located in the same

data centre or in the same geographical region, as PGW due to the pool configuration of MMEs. In this case, the S10 interface and S8 interface get passed through two different IPX Firewall instances if the IPX Firewall is collocated with MME pool or PGW. If the IPX Firewall has activated the inspection then the "Modify Bearer Request" received over S8 interface gets rejected as the Firewall instance has no information about the tunnel because it has not received "Create Bearer Request" or "Forward Relocation Request" before. **Error! Reference source not found.** shows this scenario where the serving MME and an IPX Firewall instance A are located in Location A whereas its assigned PGW and another IPX Firewall instance B are in Location B. The S10 interface is served by IPX Firewall instance A whereas S8 interface is served by IPX Firewall Instance B. In case of no synchronisation between the two instances, the handover fails.

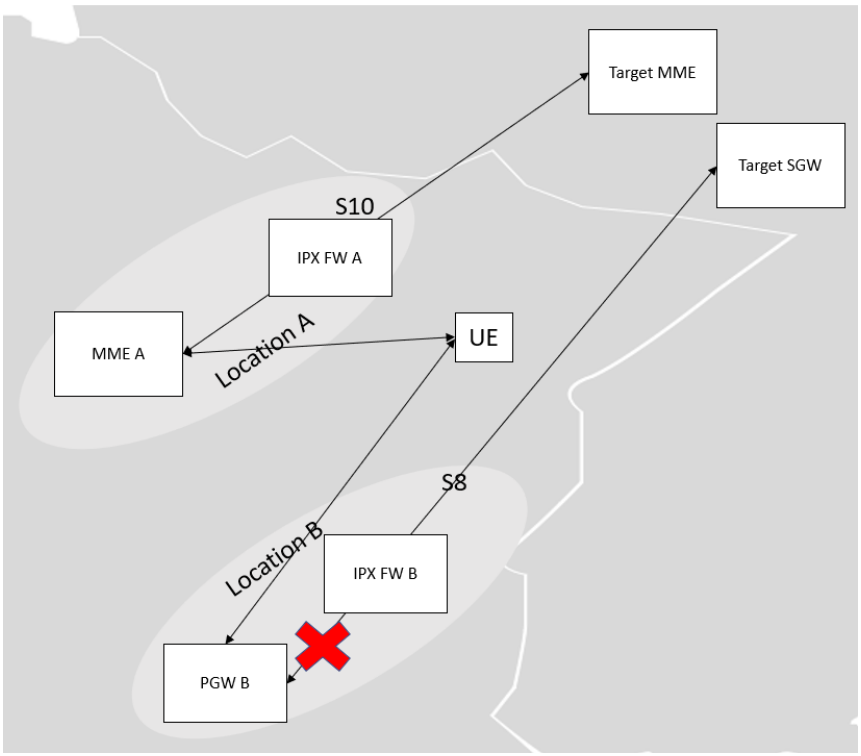


Figure 22: Network architecture change

1. **Steering of Roaming:** Once a UE moves into a different network (HPLMN to VPLMN or vice versa), a tracking area update is triggered and it in turn leads to a new location area update to the HPLMN. According to the roaming agreement and the steering of roaming, the connection could be rejected by dropping the session. The 3GPP TS 29.272 rel. 17.4 gives a solution to add a new flag in the location area update to specify this scenario.

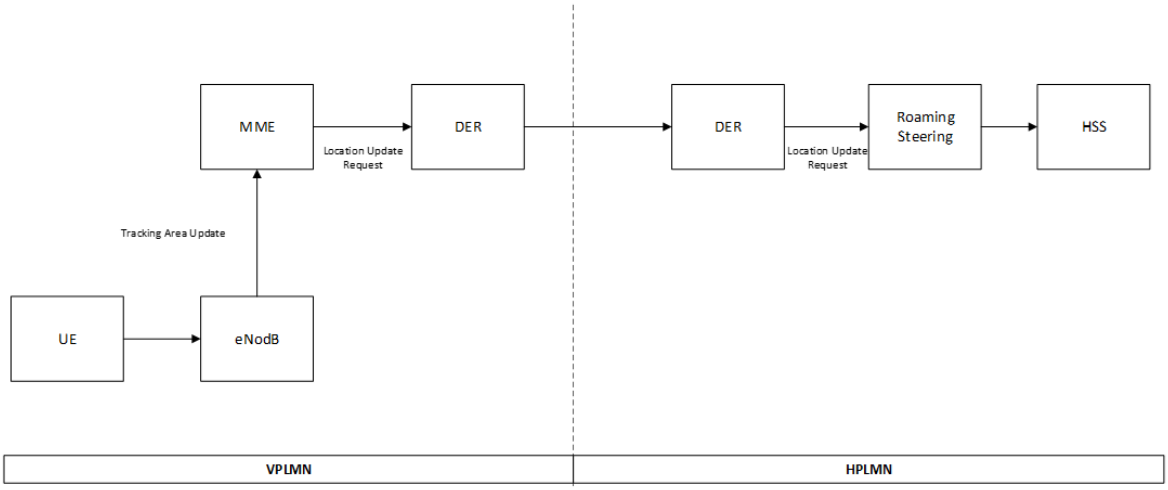


Figure 23: steering of Roaming

6.6 IPX usage

IPX providers will manage all the flows exchanged between the MCX actors (VPLMN, HPLMN, Hub etc.) for

- 4G signalling
- 5G signalling
- 4G/5G roaming data

Only 5G SA signalling and 5G SA Roaming data control will be encrypted (using https N32 interface).

6.7 Roaming configuration

In order to define the impact on the roaming networks, GSMA has defined a roaming data base (RAEX GSMA PRD IR.21), containing all data configurations to implement a roaming agreement for commercial networks.

MCX roaming agreement will need new data configuration for:

- the MCX HPLMN
    - MCC/MNC and TADIG code
    - 4G signalling
    - 5G signalling
    - 4G/5G roaming Data (IP addresses/ranges)
    - MCX services supported by the HPLMN

- the MCX VPLMN
    - MCX services supported by the VPLMN
    - 4G QoS definition (QCI)
    - 5G QoS definition (5QI)

Configuration for VoLTE and SMS are already defined in GSMA PRD IR.21.

6.8 Slicing

Only applicable to 5G SA (TBA)

7 Wholesale Billing

To be completed by WAS for future version of PRD

8 Legal and regulatory obligations

To be defined

9 Roaming Service Level Agreement

To be completed by WAS for future version of PRD

10 Existing PRD amendment

This section identifies any amendment to be included in existing PRD in order to cover mission critical communication services' use cases. Process to capture changes (i.e. CR, pCR) are to be identified.

10.1 IREG TEST BOOK

IREG document to be provided. Subset of 3GPP TS 36.579 may be used and expected level of performances indicator to be adjusted for roaming scenario.

10.2 GSMA PRD IR81

IR81 to include MCX Quality of Service monitoring (IR81 voice section to be updated).

10.3 GSMA PRD IR.21

IR 21 to include MCX data configuration

10.4 GSMA PRD IR.73

Support of MCX awareness specifically will have to be developed to incorporate the recommendations in this white paper.GSMA PRD IR.88

to be completed

10.5 GSMA PRD IR.34

to be completed

10.6 GSMA PRD NG.113

to be completed

10.7 GSMA PRD BA.51

to be completed

10.8 OTHERS

to be completed

Annex A Gaps identified

A.1 Technology gaps

a) There is no roaming architecture defined for eMBMS in 3GPP specifications and therefore, eMBMS cannot work for roaming users if VPLMN has eMBMS for mission critical services.
b) Access Class Barring (ACB) does not work in international roaming scenarios. Home networks may have to disable to avoid visiting public safety users being barred as they will be treated as normal priority users in congestion.
c) Implementation challenges to local breakout MCPTT roaming call scenarios (due to the challenges MCPTT calls will be home-routed and are not ideal for certain scenarios, e.g. wildfire use case in section 3.1).
d) Full seamless mobility may not be possible with existing architecture implementations.

Annex B User Requirements – Network Impacts Mapping

User Requirement	Use Case	Network Impact
End users from country A are able to join existing talk groups or newly created talk groups from country B	Wildfire Police Chase Mission Critical Cross Border Communications	Network impact provided (5.1.1.1, 5.1.2.1)
End user's UE from country A should be compatible with radio frequency spectrum from country B's mobile networks	Wildfire Police Chase Mission Critical Cross Border Communications	Network impact provided (5.7)
Roaming to networks X,Y and Z with Quality of Service, Priority and Pre-emption	Wildfire Police Chase Mission Critical Cross Border Communications	Network impact provided (5.1.1.2, 5.1.2.2, 5.1.3,2)
Seamless handover when roaming between operator X,Y and Z	Wildfire Police Chase Mission Critical Cross Border Communications	Network impact provided (5.5)
Handover based on the best coverage or quality of service	Wildfire Police Chase Mission Critical Cross Border Communications	Network impact provided (5.5)
Access to Home services hosted in country A	Wildfire Police Chase Mission Critical Cross Border Communications	MCX Application level is totally controlled by HPLMN
Secured communications	Wildfire Police Chase Mission Critical Cross Border Communications	Security mechanisms at IP level (Transport and routing) under the control of the VPLMN Security mechanisms at application level under the control of the Mission Critical/Public Safety agencies
MCX KPIs are met (low latency)	Wildfire Police Chase Mission Critical Cross	Network impact provided (5.1.1.3, 5.1.2.3,5.1.3.3)

	Border Communications	
Getting connectivity to neighbour FRMCS Domain B shall be transparent to the application/end user (i.e., non-human user onboard ATP)	Railways - Automatic Train Protection	Network Impact to be further analyzed
Non-human user onboard ATP from FRMCS Domain A in Country A shall be authorized to join newly created MCData one-to-one IP connectivity to trackside ATP from FRMCS Domain B in Country B	Railways - Automatic Train Protection	Network Impact to be further analyzed
UE used by non-human user onboard ATP from FRMCS Domain A in Country A shall be compatible with frequency bands of FRMCS Domain B in Country B	Railways - Automatic Train Protection	Network Impact to be further analyzed
The onboard ATP (ATP_OB) shall be able to connect simultaneously to both ATP_TS A_03 through FRMCS Domain A and to ATP_TS_B_01 through FRMCS Domain B for the transition time. This is required to ensure a “make-before-break” at application level	Railways - Automatic Train Protection	Network Impact to be further analyzed
QoS, priority and pre-emption shall be supported by both FRMCS Domain A in Country A and FRMCS Domain B in Country B	Railways - Automatic Train Protection	Network Impact to be further analyzed
QoS: Critical MCData KPIs shall be met: End-to-end latency is less than or equal to 500ms	Railways - Automatic Train Protection	Network Impact to be further analyzed
QoS: Critical MCData KPIs shall be met Reliability of 99.9%	Railways - Automatic Train Protection	Network Impact to be further analyzed
QoS: Critical MCData KPIs shall be met Speed limit is 500 kmph	Railways - Automatic Train Protection	Network Impact to be further analyzed
QoS: Critical MCData KPIs shall be met Data rate is less than 500kbps	Railways - Automatic Train Protection	Network Impact to be further analyzed
QoS: Critical MCData KPIs shall be met Service interruption is less than 150ms (TBC)	Railways - Automatic Train Protection	Network Impact to be further analyzed

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	27/01/2025	Mission Critical Communications Roaming Guidelines	ISIG-NG	Manuela Montagna, Hutchinson

Other Information

Type	Description
Document Owner	ISAG-NG
Editor / Company	Manuela.Montagna@ckhiod.com

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com.

Your comments or suggestions & questions are always welcome.