

5GS Roaming Guidelines
Version 3.0
17 November 2020

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2020 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction 4
1.1 Overview 4
1.2 Scope 4
2 Definition of Terms and Acronyms 5
2.1 Acronyms 5
2.2 Terms 7
2.3 Document Cross-References 7
2.4 Conventions 8
3 Architecture 8
3.1 Architecture Models 8
3.2 Roaming Interfaces 11
4 Technical Requirements and Recommendations for Interfaces 12
4.1 General requirements for Inter-PMN interfaces 12
4.1.1 Transport Protocol – TCP / IP 12
4.1.2 Serialization Protocol – JSON 12
4.1.3 Interface Definition Language – OpenAPI 12
4.1.4 Application Protocol – HTTP/2 12
4.2 Inter PLMN (N32) Interface 12
4.2.1 IPX HTTP Proxy 14
4.2.2 N9 Interface between VPMN and HPMN UPF 15
4.2.3 Procedures 15
4.2.4 GTP-U 16
4.3 Requirements Related to Service Based Architecture 16
5 Technical Requirements and Recommendations for Interworking and Co-Existence with E-UTRAN and EPC 17
5.1 Interworking Scenarios 17
5.2 Co-existence Scenarios 18
5.3 Inter-RAT Handover 19
5.4 Handover and Access Restriction between 5GC and EPC 19
5.4.2 Handover and Access Restriction between 5GC and Untrusted Non-3GPP Access 20
6 Technical Requirements and Recommendations for Services 20
6.1 Network Slicing 20
6.1.1 UE Support of Network Slicing when Roaming 20
6.1.2 5GC Support of Network Slicing when Roaming 21
6.2 Voice, Video, and Messaging 22
6.2.1 Short Message Service (SMS) over NAS 22
6.2.2 IMS Voice Roaming Architecture 23
6.3 Location Support 25
7 Other Technical Requirements and Recommendations 25
7.1 Access Control 25
7.1.1 Access Control in the VPMN 26

7.1.2 Access Control in the HPMN 26
7.2 IP Addressing 27
7.2.1 UE Addressing 27
7.2.2 PDU Session Type Accepted by the Network 27
7.2.3 5GC Network Function Addressing 28
7.3 DNN for IMS based services 28
7.3.1 Introduction 28
7.3.2 IMS well-known DNN 28
7.3.3 DNN for Home Operator Services 29
7.4 Emergency PDU Session 30
7.5 Emergency Services Fallback 30
7.6 Security 30
7.6.1 Fundamentals 31
7.6.2 5G Roaming Security Architecture Overview 32
7.6.3 5G Roaming Control Plane Security 32
7.6.4 5G Roaming User Plane Security 34
7.6.5 Key Management for 5G Roaming Security 35
7.6.6 Protection Policy Agreement and Exchange 36
7.6.7 Preparatory Steps per 5G Roaming Relation 37
7.6.8 Error Handling 37
7.6.9 Issue Tracking and Incident Handling 37
7.6.10 Risks from Interworking with Different Technology Generations and Signaling Protocols 37
7.7 Steering of Roaming in 5GS 39
8 Technical Requirements for QoS support 39
8.1 5G QoS Model 40
8.2 5G QoS Profile 40
8.3 QoS control 41
8.3.1 Procedures Involving QoS Control 41
8.3.2 Requirements for the VPLMN 43
8.3.3 Requirements for the HPLMN 44
8.3.4 QoS Control for IMS APN in the N9HR Architecture 44
8.3.5 Support of QoS by the IPX 45
8.3.6 Enforcement of QoS by the VPLMN 45
9 Testing Framework 46
Annex A Guidelines for Proposed Basic QoS Parameters for N9HR Roaming Scenario 47
Annex B Document Management 48
B.1 Document History 48
Other Information 48

1 Introduction

1.1 Overview

This document aims to provide a standardised view on how 5G System (5GS) networks making use of the 5G Core (5GC) can interconnect and/or interwork when users roam onto a network different to their HPMN (Home Public Mobile Network). This will be applicable when NR (New Radio) radio bearers are used, connected to a 5GC, and both UE (user equipment) and VPMN (visited PMN) have matching capabilities. The main focus is to describe 5GC, NR and interworking with EPS during roaming.

References are made to 3GPP specifications covering the 5GS, as well as other GSMA NG PRD's, such as GSMA PRD IR.88 [3] where EPC (Evolved Packet Core) interworking is specified for roaming purposes, using E-UTRAN (LTE only or LTE as master node and 5G NR as secondary node).

1.2 Scope

This PRD presents material about 5GS Roaming where the 5GC, using the SBA (Service Based Architecture) is used by the HPMN and the VPMN. The document addresses aspects that are new for 5GS roaming in general using NR mainly.

In the roaming case, the HPMN can have deployed 5GC with EPC interworking (5GC/EPC interworking) support as specified in clause 4.3.2 in 3GPP TS 23.501 [1]. If both HPLMN and VPLMN support 5GC/EPC interworking, then also idle and active mode mobility between EPC and 5GC can be supported between the roaming partners, assuming a suitable roaming agreement.

The HPMN can also have deployed two separate cores without 5GC/EPC interworking (denoted in the following as separate 5GC and EPC).

The Table X below lists the possible roaming scenarios when the HPMN supports 5GC with EPC interworking or supports separate 5GC and EPC. In addition, and for completeness, the table, lists possible roaming scenarios when the HPMN has EPC only as covered in GSMA PRD IR.88 [3].

	HPMN 5GC has EPC Interworking	**HPMN has EPC only**	**HPMN has separate 5GC and EPC**
VPMN has 5GC only	5GS roaming*	No roaming specified	5GS roaming*
VPMN has EPC only	EPC roaming using 5GS and EPC Interworking #	EPC roaming**	EPC roaming**
VPMN has separate 5GC and EPC	5GS roaming* or EPC roaming using 5GS and EPC Interworking #	EPC roaming**	5GS roaming* or EPC roaming**
VPMN 5GC has EPC Interworking	5GS roaming* or EPC roaming using 5GC and EPC Interworking #	EPC roaming**	5GS roaming* or EPC roaming**

* in scope of this PRD

** in GSMA PRD IR.88 [3]

5GC supports interworking with EPC as per 3GPP TS 23.501 [1] Section 4.3

The PRD describes the N32 interface between the HPMN and VPMN, and the services that are carried over it, as illustrated in the Architecture Model Interfaces (Section 2.2.)

This PRD is covering Voice and SMS (Short Message Service) aspects when roaming; see also GSMA PRD NG.114 [21].

Note: This version of the PRD only covers 5GS roaming over 3GPP (3rd Generation Partnership Project) access and NR connected to 5GC. WLAN access to 5GC will be covered in GSMA PRD NG.115 [30].

2 Definition of Terms and Acronyms

2.1 Acronyms

Acronym	Description
3GPP	3rd Generation Partnership Project
5GC	5G Core Network
5GS	5G System
AF	Application Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
APN	Access Point Name
CA	Certification Authority
CN	Core Network
CP	Control Plane
DDoS	Distributed Denial of Service
DEA	Diameter Edge Agent
DNN	Data Network Name
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
DRA	Diameter Routing Agent
EN-DC	E-UTRA-NR Dual Connectivity
Elte	Evolved LTE
EPC	Evolved Packet Core
EPS	Evolved Packet System (Core)
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FQDN	Fully Qualified Domain Name
GFBR	Guaranteed Flow Bit Rate
GERAN	GSM/Edge Radio Access Network
GMLC	Gateway Mobile Location Center
GPRS	General Packet Radio Service
GRX	Global Roaming Exchange
GTP	GPRS Tunnelling Protocol
HPMN	Home Public Mobile Network
HR	Home Routed
HSS	Home Subscriber Server
HTTP	Hyper-Text Transfer Protocol
IE	Information Element
IMEI	International Mobile Equipment Identifier
IMEISV	IMEI Software Version

Acronym	Description
IMSI	International Mobile Subscriber Identity
IKE	Internet Key Exchange
IP-CAN	IP Connectivity Access Network
IPUPS	Inter-PLMN User Plane Security
IPX	Internet packet Exchange
LA	Location Area
LBO	Local Break Out
LMF	Location Management Function (5G)
LTE	Long Term Evolution (Radio)
MAP	Mobile Application Part (protocol)
MBR	Maximum Bit Rate
MME	Mobility Management Entity
MIoT	Mobile Internet of Things
NE	Network Element
NEF	Network Exposure Function
NF	Network Function
NR	New Radio (5G)
NR CGI	New Radion (5G) Cell Global Identifier
NRF	Network Repository Function
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
OCS	Online Charging System
PCF	Policy Control Function
PDR	Packet Detection Rule
PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
PFCP	Packet Forwarding Control Protocol
PGW	PDN (Packet Data Network) Gateway
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMIP	Proxy Mobile IP
PRD	Permanent Reference Document
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
SA NR	Standalone New Radio
SBA	Service Based Architecture
SBI	Service Based Interface (5G)
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SGW	Serving Gateway
SUCI	Subscription Concealed Identifier
SUPI	Subscriber Permanent Identifier
TA	Tracking Area
TAU	Tracking Area Update
TLS	Transport Layer Security
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
VPMN	Visited Public Mobile Network
XCAP	XML Configuration Access Protocol
XML	eXtensible Markup Language

Acronym	Description
YAML	YAML Ain't Markup Language

2.2 Terms

Term	Description
Data Off	See GSMA PRD IR.92 [9]
Data Off Enabled Service	See GSMA PRD IR.92 [9]
Network Element	Any active component on the network that implements certain functionality that is involved in sending, receiving, processing, storing, or creating data packets. Network elements are connected to networks. In the mobile network, components such as MME, SGW, PGW, HSS, and GTP Firewalls, as well as routers and gateways are considered network elements.
Network Function	A network function can be implemented either as a network element on dedicated hardware, as a software instance running on dedicated hardware, or as a virtualised function instantiated on an appropriate platform, e.g. on a cloud infrastructure
Unsolicited downlink IP packet	An IP packet is an unsolicited downlink IP packet if: - the IP packet is sent towards the UE IP address; and - the IP packet is not related to an IP packet previously sent by the UE.
Well-known APN	An APN whose value has a defined specific string of characters

2.3 Document Cross-References

Ref	Document Number	Title
1	3GPP TS 23.501	System Architecture for the 5G System; Stage 2
2	3GPP TS 23.502	Procedures for the 5G System, Stage 2
3	GSMA PRD IR.88	LTE and EPC Roaming Guidelines
4	GSMA PRD IR.33	GPRS Roaming Guidelines
5	GSMA PRD IR.34	Guidelines for IPX Provider networks
6	GSMA PRD IR.40	Guidelines for IPv4 Addressing and AS Numbering for GPRS Network Infrastructure and Mobile Terminal
7	GSMA PRD IR.51	IMS Profile for Voice, Video and SMS over untrusted Wi-Fi access
8	GSMA PRD IR.67	DNS/ENUM Guidelines for Service Providers and GRX / IPX Service Providers
9	GSMA PRD IR.92	IMS Profile for Voice and SMS
10	3GPP TS 29.573	5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3
11	3GPP TS 29.503	5G System; Unified Data Management Services; Stage 3
12	3GPP TS 29.518	5G System; Access and Mobility Management Services
13	3GPP TS 29.509	5G System; Authentication Server Services; Stage 3
14	3GPP TS 29.502	5G System; Session Management Services; Stage 3
15	3GPP TS 29.513	5G System; Policy and Charging Control signalling flows and QoS parameter mapping
16	3GPP TS 29.510	5G System; NF Repository Services; Stage 3
17	3GPP TS 29.531	5G System; Network Slice Selection Services; Stage 3
18	3GPP TS 29.281	General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) (Release 16)
19	3GPP TS 33.501	Security architectures and procedures for 5G System
20	3GPP TS 29.500	Technical Realization of Service Based Architecture; Stage 3
21	GSMA PRD NG.114	IMS Profile for Voice, Video and SMS over 5GS
22	IETF RFC 2119	Key words for use in RFCs to Indicate Requirement Levels

Ref	Document Number	Title
23	IETF RFC 793	Transmission Control Protocol
24	IETF RFC 8259	The JavaScript Object Notation (JSON) Data Interchange Format
25	OpenAPI	OpenAPI 3.0.0 Specification", https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md
26	IETF RFC 7540	Hypertext Transfer Protocol Version 2 (HTTP/2)
27	GSMA PRD NG.116	Generic Network Slice Template
28	3GPP TS 24.501	Non-Access-Stratum (NAS) Protocol for 5G System (5GS); Stage 3
29	3GPP TS 23.003	Numbering, Addressing and Identification
30	GSMA PRD NG.115	VoWiFi over Untrusted WLAN Access to 5GC
31	GSMA PRD IR.73	Steering of Roaming Guidelines
32	GSMA PRD IR.77	IP Backbone Security Req. For Service and Inter-Operator IP backbone Providers
33	GSMA PRD FS.17	Security Accreditation Scheme - Consolidated Security Requirements
34	GSMA PRD FS.19	Diameter Interconnect Security
35	GSMA PRD FS.20	GPRS Tunnelling Protocol (GTP) Security
36	GSMA PRD FS.21	Interconnect Signalling Security Recommendations
37	GSMA PRD FS.34	Key Management for 4G and 5G Inter-PLMN Security
38	GSMA PRD IR.65	IMS Roaming Guidelines
39	3GPP TS 33.127	Lawful Interception (LI) Architecture and Functions
40	3GPP TS 29.571	5G System; Common Data Types for Service Based Interfaces; Stage 3
41	GSMA PRD FS.36	5G Interconnect Security
42	3GPP TS 33.885	Study on security aspects for LTE support of Vehicle-to-Everything (V2X) services
43	IETF RFC 7516	JSON Web Encryption (JWE)
44	GSMA PRD FS.11	SS7 Interconnect Security Monitoring Guidelines
45	GSMA PRD NG.120	MIoT Location in Roaming
46	GSMA PRD TD.201	Common Billing and Charging Processes
47	3GPP TS 29.303	Domain Name System Procedures
48	3GPP TS 23.122	Non-Access-Stratum (NAS) Functions related to Mobile Station (MS) in idle mode
49	GSMA PRD FS.37	GTP-U Security
50	3GPP TS 29.244	Interface between the Control Plane and the User Plane Nodes; Stage 3 (Release 16)
51	3GPP TS 26.114	Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS)

2.4 Conventions

“The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, and “optional” in this document are to be interpreted as described in IETF RFC 2119 **Error! Reference source not found.**.”

3 Architecture

3.1 Architecture Models

The following diagrams are produced based on the roaming reference architectures found in 3GPP TS 23.501 [1] covering:

- 5G System Roaming architecture – Local Breakout (LBO)

- Service Based Interface representation
- Reference point representation
- 5G System Roaming architecture – Home Routed (HR)
- Service Based Interface representation
- Reference point representation

Which of the Network Functions that are used by VPMN and HPMN depends on whether local-break out (LBO) or home-routed (HR) architecture are used, as depicted in the following figures.

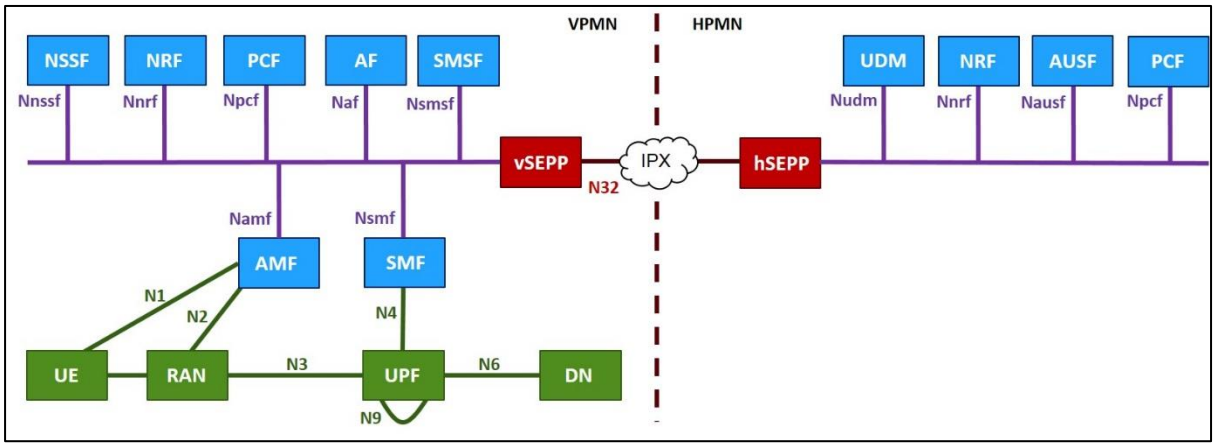


Figure 1 5G System Roaming architecture – Service Based Interface Representation (LBO)

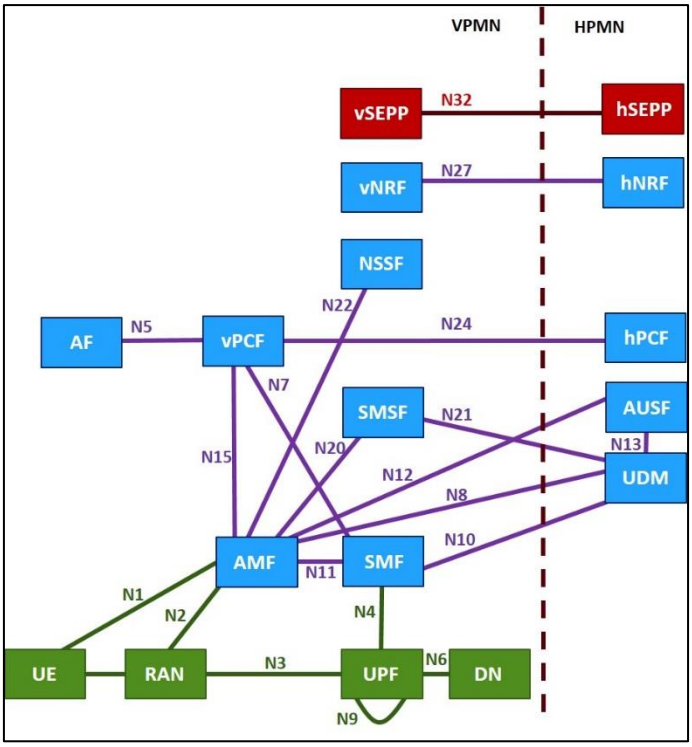


Figure 2 5G System Roaming architecture – Reference point Representation (LBO)

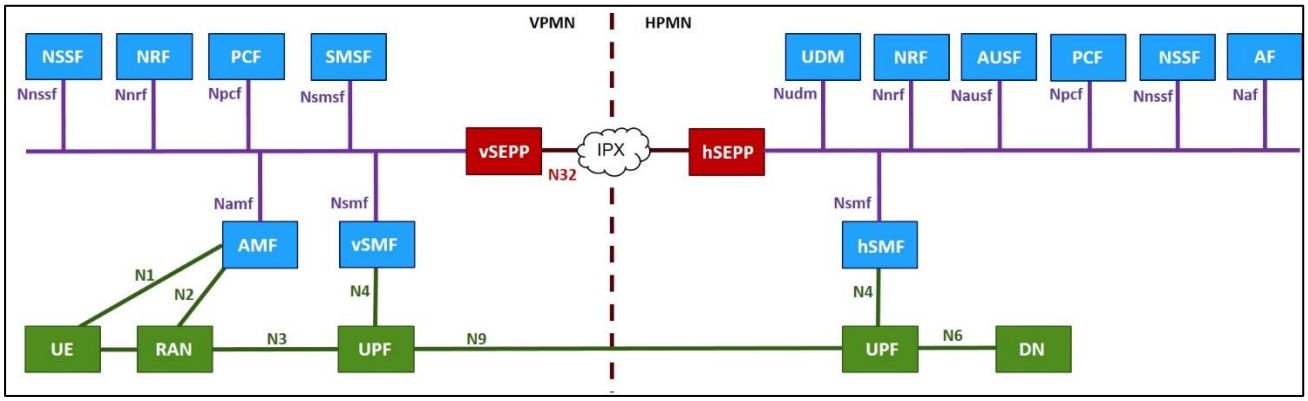


Figure 3 5G System Roaming architecture – Service Based Interface Representation (HR)

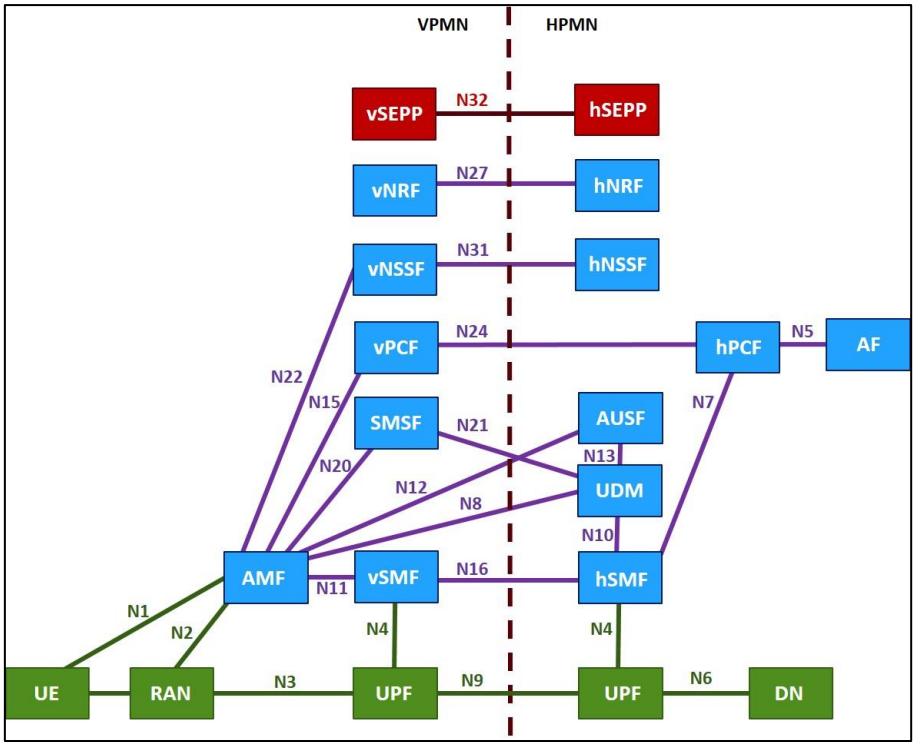


Figure 4 5G System Roaming architecture – Reference point Representation (HR)

The SEPP (Security Edge Protection Proxy) is part of the roaming security architecture and described in section 6.5.2.

3.2 Roaming Interfaces

The following Inter-PLMN interfaces in Reference Point representation are relevant for 5GC roaming; and the associated services are defined by 3GPP as follows:

Network Functions	Ref Point ID	Service Definition	Used for LBO, HR, or LBO & HR
AMF – UDM	N8	3GPP TS 29.503 [11] and 3GPP TS 29.518 [12]	LBO & HR
SMF – UDM	N10	3GPP TS 29.503 [11]	LBO
AMF – AUSF	N12	3GPP TS 29.509 [13]	LBO & HR
vSMF – hSMF	N16	3GPP TS 29.502 [14]	HR
SMSF – UDM	N21	3GPP TS 29.503 [11]	LBO & HR
vPCF – hPCF	N24	3GPP TS 29.513 [15]	LBO & HR
vNRF – hNRF	N27	3GPP TS 29.510 [16]	LBO & HR
vNSSF – hNSSF	N31	3GPP TS 29.531 [17]	LBO & HR
SEPP – SEPP	N32-c N32-f	3GPP TS 29.573 [10]	LBO & HR
vUPF – hUPF	N9	3GPP TS 29.281 [18] This is the User Plane interface so not part of the 5GC Service Based Architecture control plane solution	HR

Table 1 Relevant inter-PMN interfaces for 5GC roaming

Note: The services will all traverse over the N32 interface between SEPP functions as specified by 3GPP TS 29.573 [10]. The N9 user-plane interface does not traverse between SEPP functions.

4 Technical Requirements and Recommendations for Interfaces

4.1 General requirements for Inter-PMN interfaces

Requirements relating to IP addressing and routing for PMN's using the 5G Core and Service Based Architecture are addressed in this PRD. Where not specified in this PRD, the requirements for IP addressing and routing specified in GSMA PRD IR.33 [4], GSMA PRD IR.34 [5], GSMA PRD IR.40 [6], and GSMA PRD IR.67 [8] will apply.

The GRX/IPX (Global Roaming Exchange/Internet Packet Exchange) environment is considered as trusted, and is addressed in GSMA PRD IR.34 [5]. However, additional security functions will be specified in this PRD.

4.1.1 Transport Protocol – TCP / IP

The Transmission Control Protocol as described in IETF RFC 793 [23] shall be used as transport protocol for the HTTP/2 connection, as specified in 3GPP TS.23.501 [1]

4.1.2 Serialization Protocol – JSON

The JavaScript Object Notation (JSON) format as described in IETF RFC 8259 [24] shall be used as serialization protocol, as specified in [1] for the Service Based Interfaces.

4.1.3 Interface Definition Language – OpenAPI

OpenAPI 3.0.0 [24] shall be used as the Interface Definition Language for the Service Based Interfaces.

4.1.4 Application Protocol – HTTP/2

HTTP/2 as described in IETF RFC 7540 [26] shall be used in the Service Based Interfaces. The Service Based Interfaces used in the 5G Core are further specified in 3GPP TS 29.500 [20].

Further detail on HTTP/2 routing across PLMNs can be found in 3GPP TS 29.500 [20].

Further detail on URI Structure can be found in TS.29.501, Section 4.4.

4.2 Inter PLMN (N32) Interface

The Inter-PLMN specification 3GPP TS 29.573 [10] has been produced by 3GPP to specify the protocol definitions and message flows, and also the APIs for the procedures on the PLMN (Public Land Mobile Network) interconnection interface (i.e. N32)

As stated in 3GPP TS 29.573 [10] the N32 interface is used between the SEPPs of a VPLMN and a HPLMN in roaming scenarios. Furthermore, 3GPP has specified N32 to be considered as two separate interfaces: N32-c and N32-f.

N32-c is the Control Plane interface between the SEPPs for performing the initial handshake and negotiating the parameters to be applied for the actual N32 message forwarding. See section 4.2.2 of 3GPP TS 29.573 [10].

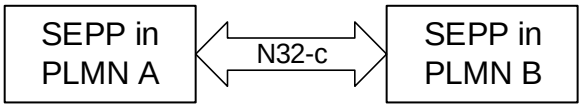


Figure 5 N32-c Interface

Once the initial HTTP/2 handshake is completed the N32-c connection is torn down. This connection is End-to-End between SEPPs and does not involve IPX to intercept the HTTP/2 connection; although the IPX may be involved for IP level routing.

N32-f is the Forwarding interface between the SEPPs, that is used for forwarding the communication between the Network Function (NF) service consumer and the NF service producer after applying the application level security protection. See section 4.2.3 of 3GPP TS 29.573 [10].

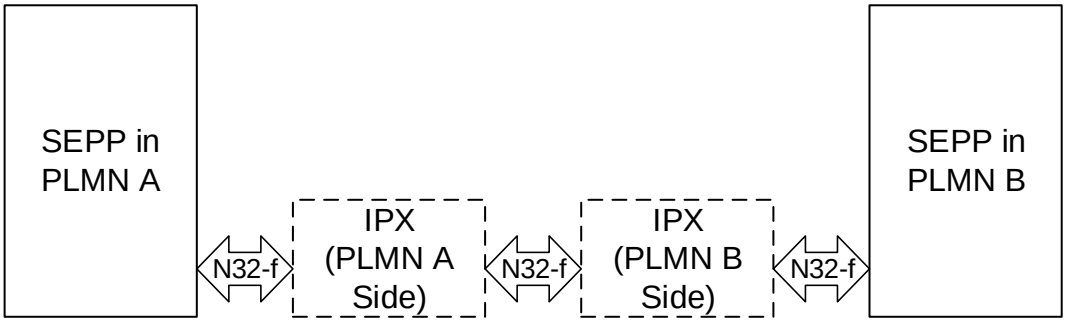


Figure 6 N32-f Interface

N32-f can provide Application Level Security (ALS) as specified in 3GPP TS 33.501 [19] between SEPPs, if negotiated using N32-c. ALS provides the following protection functionalities: -

- Message protection of the information exchanged between NF service consumer and producer
- Forwarding of the application layer protected message from a SEPP in one PLMN to another PLMN by way of using IPX providers on the path. The IPX providers on the path may involve the insertion of content modification instructions which the receiving SEPP applies after verifying the integrity of such modification instructions.

The HTTP/2 connection used on N32-f is long lived; and when a SEPP establishes a connection towards another PLMN via IPX, the HTTP/2 connection from a SEPP terminates at the next hop IPX.

N32-f makes use of the HTTP/2 connection management requirements specified in 3GPP TS 29.500 [20]. Confidentiality protection shall apply to all IE's for the JOSE protected message forwarding procedure, such that hop-by-hop security between SEPP and the IPXs should be established using an IPSec or TLS VPN.

If an IPX is not in the path between SEPPs, then an IPSec of Transport Layer Security, TLS VPN will be established directly.

Note: N32-f shall use "http" connections generated by a SEPP, and not "https"

4.2.1 IPX HTTP Proxy

The SEPP will act as a non-transparent Proxy for the NF's when service based interfaces are used across PLMNs, however inside IPX service providers, an HTTP proxy may also be used to modify information elements (IE's) inside the HTTP/2 request and response messages.

Acting in a similar manner to the IPX Diameter Proxy used in EPC roaming, the HTTP/2 Proxy can be used for inspection of messages, and modification of parameters.

Figure 7 illustrates the End to End HTTP/2 Service Based Architecture where HTTP Proxy functions are implemented by the PLMN and IPX. It shows both consumer's SEPP (cSEPP) and producer's SEPP (pSEPP). The cSEPP resides in the PLMN where the service consumer NF is located. The pSEPP resides in the PLMN where the service producer NF is located.

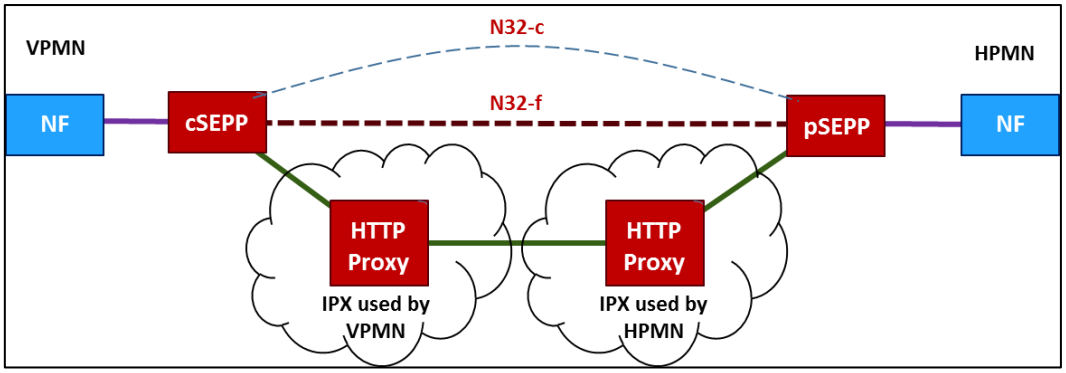


Figure 7 End to end HTTP/2 Roaming Architecture

The SEPP in a PLMN shall contain operator-controlled policy that specifies which IE's can be modified by the IPX provider directly related to the particular SEPP. For example, 'SUPI, Subscriber Permanent Identifier' or 'location data'.

As stated in 3GPP TS 33.501 [19], each PLMN shall agree the modification policy with the IPX provider that has a relationship with, prior to establishment of an N32 connection. Each modification policy applies to one individual relation between PLMN-operator and IPX provider. In order to cover the complete N32 connection both involved roaming partners shall exchange their modification policies. Both complementary modification policies shall comprise of the overall modification policy for this specific N32 connection.

Note1: In order to validate modifications for messages received on the N32-f interface, the operator's roaming partners will have to know the overall modification policy.

Note2: Modification includes removal and addition of new IE. IEs therefore may not be present in the rewritten message.

The IEs that the IPX is allowed to modify shall be specified in a list giving an enumeration of JSON paths within the JSON object created by the SEPP. Wildcards may be used to specify paths.

This policy shall be specific per roaming partner and per IPX provider that is used for the specific roaming partner.

The modification policy shall reside in the SEPP.

For each roaming partner, the SEPP shall be able to store a policy for sending in addition to one for receiving.

The following basic validation rules shall always be applied irrespective of the policy exchanged between two roaming partners:

IE's requiring encryption shall not be inserted at a different location in the JSON object

4.2.2 N9 Interface between VPMN and HPMN UPF

The UPF (User Plane Function) selection methodology is specified in 3GPP TS 23.501 [1]. For the Local Break Out (LBO) deployment scenario, both the SMF (Session Management Function) and all UPF(s) for the PDU (Protocol Data Unit) Sessions are under the control of the VPLMN. The Home Routed (HR) scenario makes use of both SMF's and UPF's in the VPLMN and HPLMN. In this case the SMF in the HPLMN selects the UPF(s) in the HPLMN, and the SMF in the VPLMN selects the UPF(s) in the VPLMN. Thus, the N9 reference point for user plane traffic is only applicable to the HR scenario, as seen in Figures 3 & 4.

The use of a UPF in the VPLMN enables VPLMN charging, VPLMN LI and minimizes the impact on the HPLMN of the UE mobility within the VPLMN (e.g. for scenarios where SSC mode 1 applies).

Different simultaneous PDU Sessions from a UE may use different modes: Home Routed and LBO. The HPLMN can control via subscription data per DNN (Data Network Name) and per S-NSSAI (Single Network Slice Selection Assistance Information) whether a PDU Session is to be set-up in HR or in LBO mode.

4.2.3 Procedures

As noted in 3GPP TS 23.501 [1] - In the case of PDU Sessions per Home Routed deployment:

- NAS Session Management terminates in the SMF in the VPLMN.
- The SMF in the VPLMN forwards to the SMF in the HPLMN SM related information

- The SMF in the HPLMN receives the SUPI of the UE from the SMF in the VPLMN during the PDU Session Establishment procedure
- The SMF in the HPLMN is responsible to check the UE request with regard to the user subscription and to possibly reject the UE request in the case of mismatch. The SMF in the HPLMN obtains the subscription data directly from the HPLMN UDM (Unified Data Management)
- The SMF in the HPLMN may send QoS requirements associated with a PDU Session to the SMF in the VPLMN. This may happen during the PDU Session Establishment procedure and after the PDU Session is established. The interface between SMF in the HPLMN and SMF in the VPLMN is also able to carry (N9) User Plane forwarding information exchanged between the SMF in the HPLMN and the SMF in the VPLMN. The SMF in the VPLMN may check QoS requests from the SMF in the HPLMN with respect to roaming agreements.

In the HR roaming case, the AMF (Access and Mobility Management Function) selects a SMF (Session Management Function) in the VPLMN and a SMF in the HPLMN as described in 3GPP TS 23.502 [2] clause 4.3.2.2.3.3, and provides the identifier of the selected SMF in the HPLMN to the selected SMF in the VPLMN.

Conversely, in roaming with LBO, the AMF selects a SMF in the VPLMN as described in 3GPP TS 23.502 [2] clause 4.3.2.2.3.2. In this case, when handling a PDU Session Establishment Request message, the SMF in the VPLMN may reject the N11 message (related with the PDU Session Establishment Request message) with a proper N11 cause. This triggers the AMF to select both a new SMF in the VPLMN and a SMF in the HPLMN in order to handle the PDU Session using home routed roaming.

4.2.4 GTP-U

The N9 interface makes use of the GPRS Tunnelling Protocol, GTP version 1 for the User Plane. The UPF's inside the PLMNs making use of the Home-Routed solution architecture is compliant to 3GPP TS 29.281 [18] Release 16 together with the Inter-PLMN User Plane Security (IPUPS) functionality for 5G Roaming User Plane Security. More details of the IPUPS can be found in section 7.6.4.

4.3 Requirements Related to Service Based Architecture

3GPP has defined four communication models for consumers and producers, grouped into direct communication and indirect communication, see Annex E.1 of 3GPP Release 16 TS 23.501 [1] and Table 2.

Communication between consumer and producer	**Service discovery and request routing**	**Communication model**
Direct communication	No NRF or SCP; direct routing	A
	Discovery using NRF services; no SCP; direct routing	B
Indirect communication	Discovery using NRF services; selection for specific instance from the Set can be delegated to	C

	SCP. Routing via SCP	
	Discovery and associated selection delegated to an SCP using discovery and selection parameters in service request; routing via SCP	D

Table 2 Communication models

Direct communication refers to the communication between network functions (NFs) or NF services without using a Service Communication Proxy (SCP) and indirect communication refers to the communication between NFs or NF services via an SCP.

Every control plane message in inter-PLMN signaling is sent via SEPPs as described in section **Error! Reference source not found.**. Consumers in the VPMN interact with producers in the HPMN. In order to avoid configuration of all relevant HPMN NFs in the VPMN as in communication model A, it is recommended that both VPMN and HPMN support discovery and selection of NFs using Network Repository Functions (NRF), i.e. visited NRF (V-NRF) in the VPMN and home NRF (H-NRF) in the HPMN.

> **Note**: The recommendation on NRF is applicable to all consumers in VPMN that interact with produces in the HPMN. Interactions between consumers and producers within VPMN or within the HPMN are out of scope.

HPMN and VPMN can have different preferences regarding communication models. The decision whether to select communication model B, C or D or any combination thereof is up to each PMN.

5 Technical Requirements and Recommendations for Interworking and Co-Existence with E-UTRAN and EPC

5.1 Interworking Scenarios

3GPP has specified interworking that allows 5GC network functions to support interfaces to an EPC. In particular, UDM+HSS (Home Subscriber Server) supports S6a, and SMF+PGW-C and UPF+PGW-U support S8-C and S8-U respectively. The diagram shown in Figure 8 illustrates the Home-routed roaming architecture for interworking between 5GS EPC/E-UTRAN making use of the interfaces to the EPC.

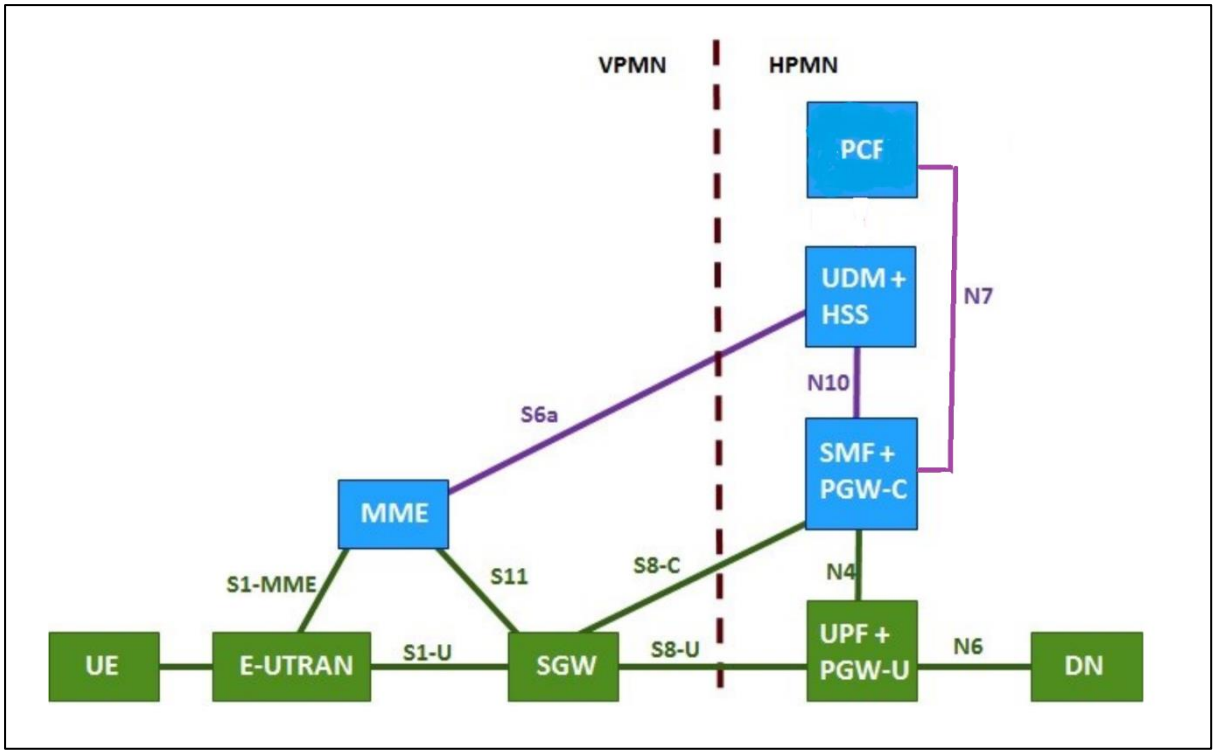


Figure 8 Home-routed roaming architecture for interworking between 5GS EPC/E-UTRAN

A 5GC in the HPMN that supports this interworking architecture, is therefore able to support 4G network roaming to an EPC based VPLMN. This type of EPC roaming will also be used initially when 5GC networks are deployed. EPC related functionality has to be supported in the Home PCF. This type of EPC roaming can be with and without 'E-UTRAN New Radio – Dual Connectivity' in the VPMN. See GSMA PRD IR.88 [3] for details.

Note: Support of split control and user plane functions in the VPLMN SGW is not required.

3GPP has specified interworking that allows the AMF in the VPMN to interact with the MME in the VPMN using the N26 interface for both idle and connected mode mobility as specified in 3GPP TS 23.502 [2]. The AMF may use the Domain Name System (DNS) communications interface to find an MME using the standard DNS procedures and protocol as specified in 3GPP TS 29.303 [47]. To support the legacy EPC core network entity (i.e. MME) to discover and communicate with the AMF, the information about the AMF should be published and available in the DNS system, see clause 5.21.2.1 in 3GPP TS 23.501 [1].

To support the MME in the VPMN to discover and select the SMF+PGW-C in the HPMN, the PGW-C information about the SMF+PGW-C should be published and available in the DNS system, see also clause 2.2 in GSMA PRD IR.88 [3].

5.2 Co-existence Scenarios

It is anticipated that both 5GS (using 5GC) roaming and LTE roaming using EPC, as well as 3G/2G roaming using a circuit switched and mobile packet core will be provided at the same time between two PMNs.

This section describes the roaming scenarios where 5GC is used and the UE supports the radio access technology and frequency band of the VPMN, 3G and 2G co-existence is outside of the scope of this PRD.

As stated in 3GPP TS.23.501 [1] Section 5.17, deployments based on different 3GPP architecture options (i.e. EPC based or 5GC based) and UEs with different capabilities (EPC NAS and 5GC NAS) may coexist at the same time within one PLMN.

It is assumed that a UE that is capable of supporting 5GC NAS procedures may also be capable of supporting EPC NAS (i.e. the NAS procedures defined in 3GPP TS 24.301]) to operate in legacy EPC networks when roaming.

The UE will use EPC NAS or 5GC NAS procedures depending on the core network by which it is served

5.3 Inter-RAT Handover

Handover attempts to NR connected to 5GC from 4G LTE will occur, with active data sessions at risk of disruption if a roaming agreement exists for 4G, but not for 5G between PMN's. The MME can prevent such handover attempts by including RAT and Core Network Type restrictions in the Handover Restriction List to E-UTRAN (see also section **Error! Reference source not found.**). There is also the possibility that a 5G roaming agreement exists, and not 4G roaming; e.g., in IoT use cases or with specific 5G, QoS criteria are used that cannot be met in 4G. The AMF can prevent such handover attempts by including RAT (Radio Access Technology) and Core Network Type restrictions in the Mobility Restriction List to NG-RAN.

> **Note**: Handover procedures between 5GS and EPS using the N26 interfaces are specified in 3GPP TS.23.502 [2], Section 4.11.1.2.

5.4 Handover and Access Restriction between 5GC and EPC

Interworking between EPC and 5GC been specified by 3GPP in 3GPP TS 23.501 [1] with system interworking, covering *Handover* specified in 3GPP TS 23.502, Section 4.11.2 [2].

5.4.1.1 Mobility Restriction for 5GC from HSS

The UE's subscription in the HSS may include access restriction for NR in 5GS and restriction for Core Network Type (5GC). If so, the HSS provides these restrictions to the MME. The MME may also, based on local policy, locally restrict accesses. The MME includes these restrictions in the Handover Restriction List to the E-UTRAN. The MME and E-UTRAN use these restrictions to determine if mobility of the UE to 5GC or NR connected to 5GC should be permitted. This way a UE roaming in a VPLMN that utilises 5GC will not be permitted to handover to NR connected to 5GC.

5.4.1.2 Mobility Restriction for EPC from UDM

The UE's subscription in the UDM may include access restriction for E-UTRAN in EPS and restriction for Core Network Type (EPC). If so, the UDM provides these restrictions to the AMF. AMF may also, based on local policy, locally restrict accesses. The AMF includes these restrictions in the Mobility Restriction List to the NG-RAN. The AMF and NG-RAN use these restrictions to determine if mobility of the UE to EPS or E-UTRAN connected to EPC

should be permitted. This way a UE roaming in a VPLMN that utilises EPC will not be permitted to handover to E-UTRAN connected to EPC.

5.4.2 Handover and Access Restriction between 5GC and Untrusted Non-3GPP Access

[Editor's Note: Placeholder for future content]

6 Technical Requirements and Recommendations for Services

6.1 Network Slicing

A 5GS UE and 5GC must support network slicing. When a UE registers to the VPLMN, it can include a Requested NSSAI, which contains up to eight S-NSSAIs. The UE subscription information must contain one or more S-NSSAI's. The UE subscription information must contain at least one default S-NSSAI to be used when the UE performs initial registration and includes no S-NSSAI value in the Requested NSSAI. Network slicing and the use of S-NSSAI is described in section 5.15 of 3GPP TS 23.501 [1].

Standardized Service Slice Types (SST) values are specified in Table 5.15.2.2-1 of 3GPP TS 23.501 [1].

The GSMA PRD NG.116 [27] defines the Generic (Network) Slice Template (GST) and how it can be used to define a variety of NEtwork Slice Types (NESTs). The GST provides a template including a set of slice attributes that can characterise a network slice. The GST can be filled with values that create a NEST, which is a set of attributes which satisfy a particular (set of) use case(s) that may be supported by the NEST. NG.116 [27] also defines NESTs with the minimum set of the attributes which map to the standardised S-NSSAIs specified in 3GPP TS 23.501 [1].

6.1.1 UE Support of Network Slicing when Roaming

As stated in Section 5.15.6 of 3GPP TS 23.501 [1], if the UE only uses S-NSSAI with standard values, then the same S-NSSAI values can be used in the VPLMN as in the HPLMN for the network slices serving the UE. Based on local VPLMN policy or if the VPLMN and the HPLMN have an agreement to support S-NSSAI with non-standard values in the VPLMN, the AMF or the NSSF of the VPLMN maps the Subscribed S-NSSAI values (provided by the HPLMN) to the respective S-NSSAI values to be used in the VPLMN. This mapping is performed during the initial registration procedure, and the AMF informs the UE about the mapped S-NSSAI values in the Mapping of Allowed NSSAI.

A UE may be configured by:

- VPLMN with the Configured NSSAI for the serving PLMN: applies to the VPLMN only, and/or
- HPLMN with the Default Configured NSSAI: applies to any serving PLMN for which no specific Configured NSSAI has been provided to the UE.

The Default Configured NSSAI, if it is configured in the UE, is used by the UE in a PLMN only if the UE has no Configured NSSAI for this serving PLMN.

The Configured NSSAI for the serving PLMN includes the S-NSSAI values which can be used in the VPLMN and may be associated with mapping of each S-NSSAI of the Configured NSSAI to one or more corresponding HPLMN S-NSSAI values, see section 5.15.4.1.1 of 3GPP TS 23.501 [1].

A roaming UE provides the Requested NSSAI in the Registration procedure based on:

- Allowed NSSAI, if received in previous registration in this VPLMN
- Default Configured NSSAI if available, and if no Configured NSSAI for the serving PLMN is available
- Configured NSSAI for the serving PLMN, if available
- S-NSSAIs for established PDN connections or for active PDU sessions, if applicable
- URSP rules or UE Local Configuration, if available: the UE uses applicable URSP rules or the UE Local Configuration to ensure that the S-NSSAIs included in the Requested NSSAI are not in conflict with the URSP rules or with the UE Local Configuration.

The AMF sends the following in the Registration response to the roaming UE, which stores the received information:

- Allowed NSSAI
- Mapping Of Allowed NSSAI (Optional)
- Configured NSSAI for the Serving PLMN (Optional)
- Mapping of Configured NSSAI (Optional)
- Rejected S-NSSAIs (Optional)

The UE behaviour regarding mapped values is stated in section 5.15.4 of 3GPP TS 23.501 [1]. The VPLMN can map S-NSSAI values provided by different HPLMNs into the same S-NSSAI value used in the VPLMN.

The UE can include S-NSSAI(s) during registration and PDU session establishment procedure as specified in section 5.15.5 of 3GPP TS 23.501 [1].

6.1.2 5GC Support of Network Slicing when Roaming

Every operator deploying 5GS will deploy network slices fitting its business. These may be network slices using S-NSSAI with standard or non-standard values.

All or a subset of these network slices may be supported for inbound and outbound roamers, and one or more slices may be dedicated to the support of inbound roamers. There are technical and commercial steps that are required to implement 5GS roaming for network slices. The technical guidelines are covered by this document and the commercial requirements, charging models and agreements can be found in GSMA WAS PRDs (in development). Guidance on billing and charging (BCE) processes are available in GSMA

PRD TD.201 [46]. Successful completion of all network, device and billing related steps is required to support network slice roaming.

A fundamental aspect of the roaming support in the 5GS is the definition in serving PLMN of a mapping between the HPLMN S-NSSAI value and VPLMN S-NSSAI value. This mapping is based on the agreement between the roaming partners of what NEST is associated to a S-NSSAI of the HPLMN. In the case of GSMA-defined NEST, the NEST is defined in GSMA PRD NG.116 [27].

The UDM in the HPLMN contains the Subscribed S-NSSAI(s) inside the Subscription Information. When roaming, the UDM must provide to the VPLMN only the S-NSSAI(s) that the HPLMN allows for the UE in the VPLMN.

When the UDM provides/updates the Subscribed S-NSSAI(s) to the serving PLMN AMF, e.g. during registration procedure, the AMF determines by itself or through interaction with the NSSF:

- Configured NSSAI for the serving PLMN and, if needed, the mapping to the Subscribed S-NSSAI(s)
- Allowed NSSAI and, if needed, the mapping to the Subscribed S-NSSAI(s).
- Rejected S-NSSAIs

In addition, the AMF determines

- Pending S-NSSAIs requiring network-slice specific authentication and authorization as described in section 5.15.10 of 3GPP Release 16 3GPP TS 23.501 [1].

The serving AMF then provides/updates the UE with the above information. The NSSF may also provide restricted S-NSSAI per TA. This information is only used by the AMF to construct the UE RA, as per section 5.15.4.1.1 of 3GPP TS 23.501 [1].

It is recommended that the S-NSSAI for eMBB [SST value 1] be supported globally for roaming as a globally available network slice, and be present in Subscribed S-NSSAIs in UDM for subscriptions using e.g. Internet access and IMS services. Other S-NSSAIs can be provided as Subscribed NSSAI if required.

6.2 Voice, Video, and Messaging

It is recommended that IMS voice, video and messaging services are on the same network slice, irrespective of whether using single IMS registration or dual IMS registration, see also GSMA PRD NG.114 [21].

> **Note**: In case of dual IMS registration, this recommendation avoids multiple IMS registrations on different network slices for these services.

It is recommended for roaming to make use of the S-NSSAI with eMBB SST value 1 exclusively. GSMA PRD NG.114 [21] provides the guidelines on the IMS profile for voice, video and messaging over 5GS.

6.2.1 Short Message Service (SMS) over NAS

SMS over NAS is a means to provide C-Plane based SMS over NR. SMS over NAS is defined in 3GPP TS 23.501 [1].

When SMS over NAS is provided for roaming, existing roaming interfaces will be used for SMS transport. The reference point N21 is used between the SMSF in the VPMN and the UDM in the HPMN.

6.2.2 IMS Voice Roaming Architecture

6.2.2.1 General

During the registration procedure in 5GS, the voice domain selection in the UE takes place as specified in section 5.16.3.5 of 3GPP TS 23.501 [1].

Details on IMS Roaming over 5GS can be found in GSMA PRD IR.65 [38].

6.2.2.2 IMS Voice Roaming Architecture N9HR

To support IMS roaming using N9 Home Routed (N9HR, refer to GSMA PRD IR.65 [38]), both the SMF/UPF and the Proxy-Call Session Control Function (P-CSCF) must be located in the HPMN. The same IMS voice roaming architecture using N9HR is used in case of IMS voice support over NR connected to 5GC and in case of EPS Fallback.

To select the correct SMF in the HPMN, the HPMN operator must not allow its IMS Voice subscribers to use VPMN addressing. See Section 7.3.2 for detailed discussion related to SMF selection and a "well-known" DNN usage related to IMS Voice Roaming.

For the VPMN and HPMN to enable N9HR IMS roaming, the following conditions must be fulfilled in 5GC and NG-RAN. Conditions in IMS are not listed:

1. The VPMN must support the following capabilities:

   - IMS well-known DNN;
   - QoS flow with 5QI=5 for SIP signalling;
   - QoS flow with 5QI=1 for voice media; in case of EPS Fallback, the request to establish the QoS flow with 5QI=1 is rejected by the gNB.
   - if videocall is supported, then QoS flow with 5QI=2 (or non-GBR 5QI);
   - Indication from AMF to the UE “IMS VoPS (Support Indicator) = supported” if the VPMN has a roaming agreement that covers support of IMS voice with the HPMN as specified in clause 5.16.3.2 of 3GPP TS 23.501 [1];

   Note1: As specified in 3GPP TS 23.501 [1], "IMS VoPS" indicator can reflect the roaming agreement which is intended to support IMS voice only in EPS, while excluding the case of IMS voice via NR connected to 5GC.

   - Indication from AMF to the UDM "Homogeneous Support of IMS Voice over PS" based on the conditions specified in 3GPP TS 23.501[1].

- Lawful interception of IMS voice calls and SMS as per 3GPP TS 33.127 [39], and data retention.

Note2: Lawful interception of IMS service is also needed in case of EPS Fallback.

- To support IMS emergency calls for inbound roamers, the VPMN must support anonymous emergency calls over IMS as described in GSMA PRD NG.114 [21].

Note3: N9HR requires support for anonymous emergency calls over IMS.

2. The HPMN must support

- IMS well-known DNN
- QoS flow with 5QI=5 for SIP signalling;
- QoS flow with 5QI=1 for voice media;
- If videocall is supported, then QoS flow with 5QI=2 (or non-GBR 5QI);

As ARP settings are exclusively related to the VPMN service prioritization strategy and may change from one VPMN to another, HPMN should agree with VPMN on a right Priority Level (PL) value to set on QoS flow with 5QI=5 in order to ensure that its sessions will be handled with the right priority.

In addition, in order to enable N9HR IMS voice roaming, local regulatory requirements in the VPMN need to be fulfilled.

6.2.2.3 Terminating Access Domain Selection

Terminating Access Domain Selection (T-ADS) optimizes routing of MT calls so that they can be successfully delivered to the UE irrespective of whether or not the UE is camping in an area with IMS Voice over PS supported. For IMS voice roaming using N9HR, if an HPMN requires T-ADS for its outbound roaming subscribers, then both the HPMN and VPMN must provide the needed functionality as described section 5.16.3.3 in 3GPP TS 23.501 [1].

6.2.2.4 IMS Voice Roaming Restriction

IMS voice roaming restriction allows the HPMN to restrict IMS voice roaming per subscriber and / or per VPMN by excluding the IMS well-known DNN from the subscriber data sent from UDM to the AMF in the VPMN, unless HPMN intends to provide non-voice IMS services in the VPMN. If the AMF does not receive the IMS well-known DNN in the subscriber data, then the AMF:

- Is recommended to set the indication “IMS VoPS (Support Indicator) = not supported” to the UE at Registration as described in section 5.16.3.2 of 3GPP TS 23.501 [1]; and
- Rejects an attempt by the UE to establish a PDU session to the IMS well-known DNN with #33 "requested service option not subscribed" as described in section 6.4.1.4.3 of 3GPP TS 24.501 [28].

Note1: The AMF provides the “IMS VoPS (Support Indicator) = supported” to the UE if the VPMN has a roaming agreement that covers support of IMS voice with the HPMN as specified in clause 5.16.3.2 of 3GPP TS 23.501 [1].

Note2: HPMN is not required to delete the IMS well-known DNN from the subscription profile when HPMN understands that IMS voice cannot be provided for the corresponding customer in the registering VPMN. The AMF of the VPMN needs to provide the adequate “IMS VoPS (Supported Indicator)” value reflecting the IMS voice roaming agreement.

6.3 Location Support

GSMA PRD NG.120 [45] presents the technical alternatives to locate objects in roaming.

Location in 5G networks is based on the GMLC/AMF/LMF architecture as described in the figure hereafter (applies to MIoT), using potentially different interfaces to retrieve location in roaming.

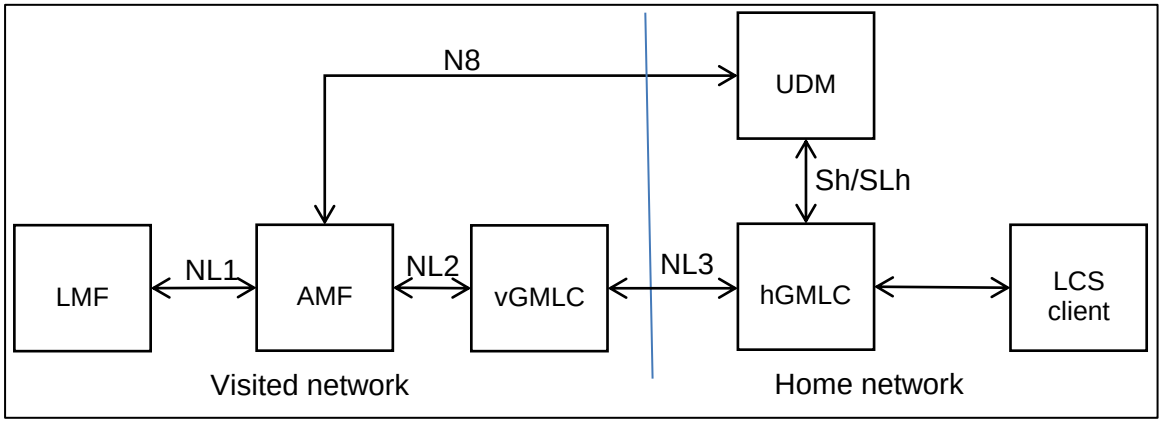


Figure 9 Location Support

In order to retrieve the location information, 2 different HTTPs signalling messages could be used:

- N8: ProvideLocationInfo
- NL2/NL3: ProvidePositioningInfo (LCS architecture related to MT-LR procedure)

Based on those signalling messages, three solutions could be proposed in 5G (similar to 4G) to retrieve the Cell-Id and the associated geographical coordinate. The solution complexity and accuracy could vary depending on visited network implementation:

- Cell-Id: the visited AMF will provide the Cell-Id (NR CGI) to the home GMLC
- Cell geographical coordinate: the visited AMF will provide the geographical coordinate (latitude, longitude) of the cell to the home GMLC
- Object geographical coordinate: the visited AMF (via the LMF) will provide the geographical coordinates (latitude, longitude) of the object to the home GMLC

7 Other Technical Requirements and Recommendations

7.1 Access Control

Without an explicit roaming agreement from the HPMN, the VPMN must block the access of inbound roamers onto their 5G-NR access network. This is compulsory to ensure roamers will not experience any service disruption because the necessary technical requirements have not been implemented and tested within the HPMN.

7.1.1 Access Control in the VPMN

The AMF in the VPMN shall implement the same sort of access control feature that exists in EPC MME. One mechanism to achieve this, is based on the MCC and MNC range information inside of the Subscription Concealed Identifier, SUCI (based on IMSI). Using this mechanism, the subscriber is either rejected (with the appropriate reject cause as defined in 3GPP TS 24.501 [28]) or allowed to register.

- Cause #15 (no suitable cells in Tracking Area) if the VPMN already has a Roaming Agreement with the HPMN covering other Radio Access Technologies (RATs), it forces the UE to reselect another RAT in the same PMN
- Cause #11 (PLMN Not Allowed) if the VPMN has no roaming agreement with the HPMN. It forces the UE to perform a PMN reselection. UE shall store the PMN identity in the "forbidden PLMN list" in the USIM (Universal Subscriber Identity Module) and the UE shall no more attempt to select this PMN. Cause #13 may also be used (to avoid permanent storage of PMN in the Forbidden PMN file in the USIM).

IMS Voice over PS Session support indication shall be sent to a roaming UE, only if there is an IMS voice roaming agreement between the HPMN and VPMN in place.

7.1.2 Access Control in the HPMN

If the VPMN does not implement the requirements in the previous section, then the HPMN can implement its own access control feature in the UDM to protect its subscribers.

If the HPMN already has a Roaming Agreement with the VPMN covering other RAT access technologies then the reject indication sent by the UDM back to the AMF in the Nudm_UECM_Registration response HTTP status code “403 Forbidden”, will contain the additional error information in the response body, “ProblemDetails” element. The “ProblemDetails” Data type will use the “cause” attribute – RAT_NOT_ALLOWED. Figure 10 below illustrates the AMF registration service operation.

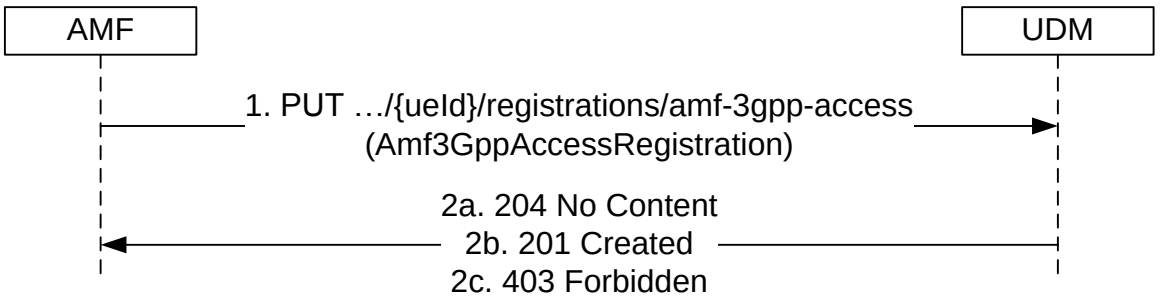


Figure 10 AMF registering for 3GPP access [10] Section 5.3.2.2.2

The AMF must then map the RAT_NOT_ALLOWED cause from the UDM into the cause #15 (no suitable cells in Tracking Area) to send to the UE. The AMF should not map RAT_NOT_ALLOWED into cause #12 (Tracking area not allowed) or #13 (Roaming not allowed in this tracking area) or #11 (PLMN not allowed.)

7.2 IP Addressing

The 5GS has significant differences to GPRS (2G), 3G and LTE (4G) networks that push the drive to use of IPv6 as much as possible. Reasons such as: -

- Integration with broadband [fixed] network and control planes
- Use of non-3GPP access, and more small cell endpoints
- Network slices across Access and Core networks
- Hosting of functions with NFV / cloud-based infrastructure
- Support of Edge Computing and 3rd party access
- Massive IoT volumes for UE

Network operators could have insufficient IPv4 resources, thus the 5G UE and 5G network must support the use of IPv6 as the PDU session type. For the purpose of supporting the service or feature provided through the DN that requires native IPv4 connectivity, use of IPv4 and IPv4v6 should be considered.

7.2.1 UE Addressing

7.2.1.1 General

Every 5G capable UE using the IPv4, IPv6, or IPv4v6 is allocated one or more IP addresses. One per PDU session as a minimum.

Section 5.8.2.2 of 3GPP TS 23.501 [1] provides information on UE IP Address Management. IPv4, IPv6 and IPv4v6 session types are allowed. Other non-IP PDU Session types, i.e. Ethernet and Unstructured, are also allowed. PDU Session Type is based on the request sent by UE and the support and any policy in the network, where SMF decides whether to accept, partially accept, or decline the request from UE.

7.2.1.2 PDU Session Type Requested by UE

UE must request the PDU Session Type as specified in section 5.8.2.2.1 of 3GPP TS 23.501 [1].

7.2.2 PDU Session Type Accepted by the Network

SMF must select the PDU Session Type to be used as specified in section 5.8.2.2 of 3GPP TS 23.501 [1], based on UE's request, DNN configuration, local policy at SMF, and/or IP version supported by the DNN.

For Home Routed Roaming, the PDU Session Type is decided by HPMN, i.e. by the H-SMF, as the VPMN, i.e. V-SMF, will only transparently forward the requested PDU Session Type to the HPMN, and the decision of the accepted PDU Session Type is solely dependent on the policy at HPMN.

For Local Breakout Roaming, the PDU Session Type is decided by VPMN, (i.e. by the SMF in VPMN serving the inbound roamer), and operators must negotiate the PDU Session Type to be accepted. It is recommended that the PDU Session "IPv6" to be supported at minimum for the reason described in Section 6.2. Other PDU Session Types may be supported for the purpose of supporting legacy services based on bilateral negotiation between the VPMN and HPMN.

7.2.3 5GC Network Function Addressing

The 5GC supports a PDU Connectivity Service, i.e. a service that provides the exchange of PDUs between a UE and a data network identified by a DNN. The PDU Connectivity Service is supported via PDU Sessions that are established upon request from the UE.

Section 5.6.1 of 3GPP 23.501 [1] states that the following PDU Session types are defined: IPv4, IPv6, IPv4v6, Ethernet, Unstructured.

It is recommended that routing across PLMN NF services make use of IPv6 only.

7.2.3.1 Fully Qualified Domain Names (FQDNs)

Section 6.1.4.3 of 3GPP TS 29.500 [20] specifies how HTTP/2 request messages are routed between PLMNs, where the correct target NF service should be reached. Where the target URI authority designates an origin server not in the same PLMN as the client, the "authority" HTTP/2 pseudo-header shall contain the FQDN including the PLMN ID.

The format of the FQDN of the target NF service is specified in 3GPP TS 23.003 [28] Section 28.5. For HTTP/2 request messages to a NF service in different PLMN, the FQDN of the target NF shall have the Home Domain as the trailing part – i.e.

- 5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

7.3 DNN for IMS based services

7.3.1 Introduction

IMS well-known DNN and a DNN for related Home Operator Services are defined below. For more details on when these DNNs are used over 5GS, see GSMA PRD NG.114 [21] (for Voice/Video and messaging over 5GS).

7.3.2 IMS well-known DNN

7.3.2.1 Definition

The Network Identifier (NI) part of the DNN must be set to "IMS". The Operator Identifier (OI) part of the full DNN must be blank as it is automatically derived and appended to the NI part by the VPMN and its value depends on the PMN whose SMF the UE is anchored to.

7.3.2.2 SMF Discovery and Selection

The PDU Session to the IMS well-known DNN utilises an V-SMF in VPMN and an H-SMF in HPMN when using N9HR roaming. Therefore, when enabling IMS voice roaming for a subscriber, the following subscription settings must be taken into account for the IMS well-known DNN:

- The barring on "All Packet Oriented Services" (“ALL_PACKET_SERVICES” in 3GPP TS 29.571 [40] is not active
- The barring on "Packet Oriented Services from access points that are within the HPMN" (“ROAMER_ACCESS_HPLMN_AP” in 3GPP TS 29.571 [40]) is not active.
- LBO Roaming information in the UDM is set to not allowed.

Note: The term ‘access point’ is used to indicate the H-SMF located in HPMN that is accessed to establisn a PDU Session specified by a particular DNN.

The SMF discovery and selection is described in section 6.3.2 of 3GPP TS 23.501 [1].

7.3.2.3 Inter-PLMN Roaming Hand Over

If the PDU session to the IMS well-known APN is maintained after moving from one PLMN to another, because an inter-PLMN roaming agreement is in place, then the SMF in the HPMN (H-SMF) must disconnect the PDU session to the IMS well-known APN unless the inter-PLMN roaming agreement in place allows this PDU session to continue.

7.3.3 DNN for Home Operator Services

7.3.3.1 Definition

The Network Identifier (NI) part of the DNN is undefined and must be set by the Home Operator. The requirements for the value of the NI are as follows:

- must be compliant to 3GPP TS 23.003 [28] section 9.1.2;
- must resolve to an SMF in the HPMN; and
- must not use the same value as the IMS well-known APN (as defined in Section 7.3.2.1).

Home operators can choose to reuse an DNN for already deployed services (e.g. Internet access, WAP, MMS, etc.) or choose a new, specific DNN for the DNN for Home Operator Services. See also GSMA PRD IR.88 [3].

If using a new/specific DNN, then the value "hos" (case insensitive) is recommended.

The Operator Identifier part of the full DNN should be blank as it is automatically derived and appended to the NI part by the VPMN.

7.3.3.2 SMF Discovery and Selection

The DNN for Home Operator Services utilises a V-SMF in VPMN and an H-SMF in HPMN. Therefore, when enabling IMS roaming for a subscriber, the following subscription settings must be taken into account for the DNN for Home Operator Services:

- The bar on "All Packet Oriented Services" is not active
- LBO Roaming Information in the UDM is set to not allowed.

7.3.3.3 Inter-PLMN roaming hand over

If the PDU session to the DNN for Home Operator Services is maintained after moving from one PLMN to another, because an inter-PLMN roaming agreement is in place, then the SMF in the HPMN does not need to disconnect the PDU session to the DNN for Home Operator Services unless the inter-PLMN roaming agreement in place enforces this PDU Session to discontinue.

The SMF discovery and selection is described in section 6.3.2 of 3GPP TS 23.501 [1].

7.3.3.4 Data Off related functionality

3GPP PS Data Off and 3GPP PS Data off Exempt Services have been defined in GSMA PRD NG.114 [21]. This section applies when the UE has activated 3GPP PS Data Off.

The home network supporting 3GPP PS Data Off, as defined in 3GPP Release TS 23.501 [1], must only send IP packets for services that are configured as 3GPP PS Data Off Exempt Services.

> **Note**: IPv6 Router Advertisement IP packets are an essential part of the UE IP address configuration. Although these packets do not belong to any specific 3GPP Data Off Exempt Services, they are still sent over the PDN connection.

7.4 Emergency PDU Session

An emergency PDU session is established to an SMF within the VPMN when the UE wants to initiate an emergency call/session due to it detecting the dialling of a recognised emergency code and if the AMF has indicated support for emergency services. Any DNN included by the UE as part of the emergency request is ignored by the network. This is further detailed in 3GPP TS 23.167 [X], Annex H. The emergency PDU session must not be used for any other type of traffic than emergency calls/sessions. Also, the DNN used for emergency calls/sessions must be unique within the VPMN, and so must not be any of the well-known DNNs or any other internal ones than what is used for emergency. Whilst the 3GPP specifications do not provide any particular DNN value, the value of "sos" is recommended herein. The DNN for emergency calls/sessions must not be part of the allowed DNN list in the subscription. Either the DNN or the SMF address used for emergency calls/sessions must be configured to the AMF.

7.5 Emergency Services Fallback

If the AMF has indicated support for emergency services using fallback, and the UE wants to initiate an emergency call/session due to it detecting the dialling of a recognised emergency code, the Emergency Services Fallback procedure is initiated by the UE as specified in 3GPP TS 23.501 [1] and 3GPP TS 23.502 [2]. The AMF receives a service request for emergency from the UE and triggers a request for Emergency Services Fallback towards NG-RAN. The NG-RAN initiates handover or redirection to E-UTRAN connected to EPS.

7.6 Security

Ensuring adequate security levels is not just a matter of deploying the right technology in the right place. It is critical that proper procedures are adequately defined and continuously adhered to throughout the entire security chain, particularly at an operational level. Security cannot be achieved by just one stakeholder in a network, it requires that every single stakeholder fulfils their part of the requirements.

Due to interconnect and roaming, the inner PLMN is exposed to other networks. Consequently, measures to securely allow partners to interconnect in a controlled way have to be deployed, without revealing confidential information or facilitating fraud/abuse. Furthermore, the mobile ecosystem is changing. There is an increasing demand on security by the public and by regulators. With the 5G standard, 3GPP addresses these demands by introducing new security controls and secure inter-operator communication, all of which are introduced in this document and in particular in this section.

This section covers all aspects relevant for deploying and operating 5G roaming securely. Aspects, such as security controls at the network edge, secure communication, key management and protection policy exchange are covered.

PLMN operators and IPX Providers are advised to adhere to the recommendations which are given in this section.

7.6.1 Fundamentals

Security requires a comprehensive approach. There is the need for all PLMN operators and IPX Providers to:

- Have a secure network design that isolates all parts of the network that need not to be reached from the outside;
- Secure all entry points into their networks at the edge;
- Deploy secure communication between PLMNs;
- Introduce, apply and maintain security procedures.

A secure network design guarantees that the impact of a failure or an attack is limited, as it cannot spread to other parts of the network. As a concrete measure, PLMN operators should only expose the network functions to the IPX Network that are to be reachable by partners. More on network design and fundamental network security aspects can be found in the binding GSMA PRD IR.77 [32].

At the network edge, all entry points should be configured securely, all incoming traffic should be validated and discarded if unwanted. Security is to be applied on all layers. It is good security practice to filter traffic on IP level and to perform DoS (denial of service) protection at the border gateway (BG) as the outermost device, followed by a firewall that filters on transport and application layer. For signalling traffic, this firewall is the SEPP. For user plane traffic, it is the UPF/UP gateway. For fundamentals on network edge security on network layer and transport layer, the reader is referred to the binding GSMA PRD IR.77 [32]. Application layer aspects of 5G are covered in this document and in GSMA PRD FS.21 [36], an overview of and an introduction into signalling security is provided.

Secure communication for 5GS between PLMNs is defined by N32 security and N9 security, as specified by 3GPP in TS 33.501 [19], and in this section.

A variety of security procedures for preparing roaming agreements, deploying and configuring network equipment, maintaining roaming connections and network equipment, dealing with faults, attacks and software upgrades are to be introduced and applied. The binding GSMA PRD IR.77 [32] covers general aspects and this document deals with the specifics of 5G roaming security, in particular Protection Policy definition, agreement and exchange and cryptographic key exchange.

The documents referenced above are applicable and important to the same extent as this section is applicable and important to PLMN operators and IPX Providers.

7.6.2 5G Roaming Security Architecture Overview

5G roaming security architecture consists of the Security Edge Protection Proxies (SEPPs) that communicate over the N32 interface and the respective Protection Policies for the SEPPs. The Security Edge Protection Proxy (SEPP) has been introduced in 3GPP TS 33.501 [19] 5GS security architecture. Details to the interface between 2 SEPPS via Inter PLMN N32 interface are provided in clause 3.2. Operators manually provision SEPPs with a Protection Policy based on bilateral agreements as elaborated in detail in clause 6.5.6. Protection policies can be validated via N32-c, which is protected by TLS.

In summary, the SEPP is a non-transparent proxy to allow secure communication between service-consuming and a service-producing NFs in different PLMNs. The SEPPs sitting at the perimeter of each network and enforce via N32 interface the protection policies ensuring integrity and confidentiality protection for those elements to be protected and defining, which parts are allowed to be modified by an IPX provider sitting between the SEPPs.

The functionality of the SEPP includes message filtering and policing on inter-PLMN control plane interfaces as well as topology hiding. In addition the SEPP can provide Application Level Security (ALS) by PRINS (PRotocol for N32 INterconnect Security) on all HTTP messages before they are sent externally over the roaming interface.

The SEPP applies its functionality to every Control Plane message in inter-PLMN signalling, acting as a service relay between the actual Service Producer and the actual Service Consumer. For both Service Producer and Consumer, the result of the service relaying is equivalent to a direct service interaction.

The IPX HTTP Proxy is out of scope in 3GPP. It allows the IPX service provider to modify information elements received by the SEPP in a controlled way. For details see clause 3.2.1.

7.6.3 5G Roaming Control Plane Security

In support of 5G roaming, operators will need to filter and control their exchange of HTTP/2 messages with the SEPPs of their roaming partners. In addition to the TCP/TLS/IP lower layer filter actions as in section 6.5, the 5G roaming filter and control actions especially refer to application layer security (ALS as defined in 3GPP TS 33.501 [19]) controls and cross-layer checks like:

- To validate if the 5G roaming control information received via the N32 interface in one or more JSON objects is allowed, correct and plausible for this end-user
- Idem, to check if the 5G roaming control information in one or more JSON objects is allowed, correct and plausible to be received from this home or visiting network

To verify if information in a JSON object matches with the IP address on the IP layer by performing cross-layer information checking.

These checks and supplementary balancing actions (like throttling and traffic policies) are only possible by the SEPP to decide if the HTTP/2 message can be forwarded to the final destination in the receiving network, or not.

In addition, to investigate the authenticity of the sending roaming partner, to validate and screen the control actions of the messages via the API interface.

The filtering actions are recommended to work on the basis of a “White-List” principle (i.e. only pass messages that meet given conditions) similarly as specified for LTE with the Diameter firewall guidelines in GSMA PRD FS.19 [34] Annex B.

Please note that the subsequent sections only provide high-level introduction to the security aspects of the ALS signalling application protocols. Further details can be found in:

GSMA PRD FS.17 [33] with detailed guidelines for both the HTTP/2 security aspects and the JSON security aspects
GSMA PRD FS.21 [36] with proposed sets of RFI/RFQ requirements for the 5GS functional elements and the related implementation and testing aspects.

7.6.3.1 HTTP/2 Security

For topology hiding, the SEPP supports TLS wildcard certificate for its domain name and generation of telescopic FQDN based on an FQDN obtained from the received N32-f message, as defined in 3GPP TS 33.501 [19], clause 13.1.

The SEPP rewrites the FQDN from the received HTTP/2 message with a telescopic FQDN and forwards the modified HTTP/2 message to the target NF inside the PLMN. The details of how SEPPs uses the telescopic FQDN to establish a TLS connection between a NF and the SEPP is defined in 3GPP TS 33.501 [19], clause 13.1, 3GPP TS 29.573 [10], clause C.2.2 and GSMA PRD FS.21 [36], clause 3.8.1.

For the HTTP/2 message protection, the SEPP (referred to as cSEPP) reformats the HTTP/2 message to produce the input to JSON Web Encryption (JWE), as specified by clause 13.2.4.3 of 3GPP TS 33.501 [19]. The SEPP applies JWE to protect the reformatted

message and encapsulates the resulting JWE object into a HTTP/2 message (as the body of the message).

The HTTP/2 message over the N32-f interface may be routed via the two IPX nodes. These IPX nodes may modify messages according to the modification policy, and creates a JSON Web Signature (JWS) object, as specified by clause 13.2.4.5.2 of 3GPP TS 33.501 [19]. Other details can be found in GSMA PRD FS.21 [36], clause 3.8.1 and GSMA PRD FS.36 [41], clause 3.4.1

7.6.3.2 JSON Security

The SEPP reformats an HTTP message received from an internal NF into two temporary JSON objects that will be input to JWE. The SEPP uses JSON Web Encryption (JWE) as specified in IETF RFC 7516 [43] for the protection of reformatted HTTP messages between the SEPPs.

The IPX providers create modifiedDataToIntegrityProtect JSON object, as described in clause 13.2.4.5.1 of 3GPP TS 33.501 [19], as input to JWS to create a JWS object. The IPX providers apply the modifications described in the JSON patch, and appends the generated JWS object to the payload in the HTTP message and then sends the message to the receiving SEPP.

The receiving SEPP decrypts the JWE ciphertext, and checks the integrity and authenticity of the clear text and the encrypted text in the HTTP message. The receiving SEPP, next verifies the IPX provider updates, if included, by verifying the JWS signatures. It then checks whether the modifications performed by the IPX provider were permitted by the respective modification policies. If this is the case, the receiving SEPP creates a new HTTP message. At last, the receiving SEPP verifies that the PLMN-ID contained in the incoming N32-f message matches the PLMN-ID in the related N32-f context. Other details can be found in GSMA PRD FS.21 [36], clause 3.8.2

7.6.3.3 API Security

[Editor’s Note: This content is pending.]

7.6.4 5G Roaming User Plane Security

In support of 5G roaming, operators will need to filter and control their exchange of GTP-U messages over the N9 reference point with their roaming partners.

In the 5GS security architecture the Inter-PLMN User Plane Security (IPUPS) functionality within UPF correlates user plane sessions over the N9 reference point with SMF control plane sessions and drop invalid user plane sessions if there is no match.

Operators can deploy either UPFs supporting the IPUPS functionality or the IPUPS as a separate Network Function from the UPF, at the border of their network to protect their network from invalid inter PLMN N9 traffic in home routed roaming scenarios. Figure 11 depicts the home routed roaming architecture where a UPF is inserted in the UP path for the IPUPS functionality.

Figure 11 Roaming Home Routing Scenario - In Serviced Based Interface Presentation

The IPUPS interacts with the SMF on the N4 interface. During the establishment of a Packet Forwarding Control Protocol (PFCP) session between a UPF and SMF on the N4 interface, the UPF indicates to the SMF whether it has an IPUPS enabled. Once the PFCP sessions are established with the UPF on the N4 interface, the SMF (Control Plane) provisions into the User Plane (for later use by the lookup actions by the IPUPS feature) using Packet Detection Rule (PDR) declarations that define how user plane sessions are identified.

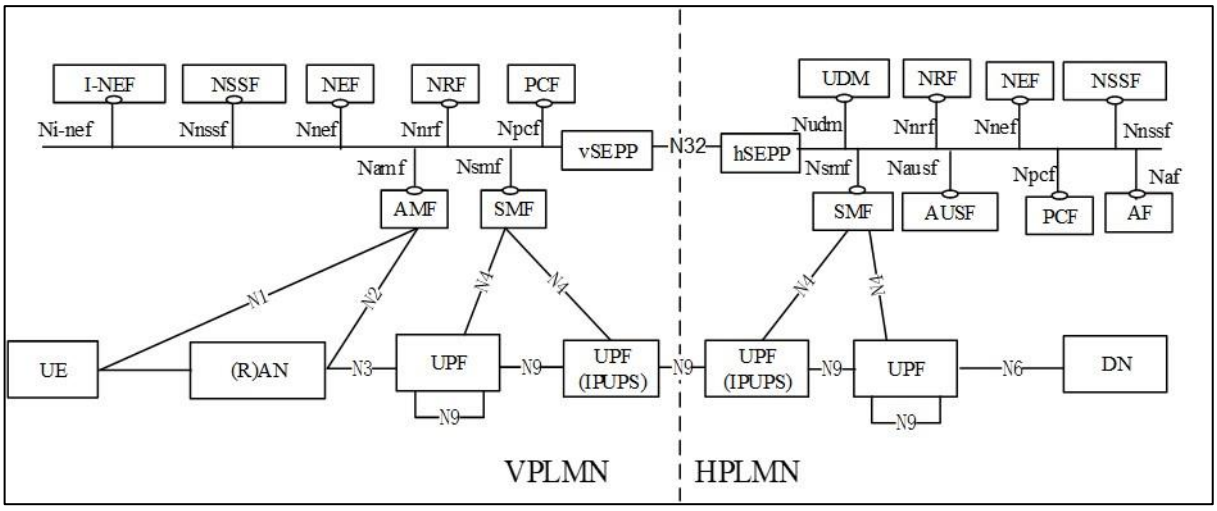
The IPUPS functionality within UPF correlates the received user plane sessions by lookup with the provisioned PDR. The IPUPS drops user plane sessions that do not have corresponding PDR provisioned. More details of the Packet Forwarding Model can be found in 3GPP TS 29.244 [50].

3GPP TS 23.501 [1] and TS 33.501 [19] specify further details of the IPUPS functionality and please be referred to GSMA PRD FS.37 [49] for more guidance of the GTP-U/GTP-C tunnel correlation solutions for 3G/4G and 5G.

In addition, relevant aspects may be considered as specified in GSMA PRD IR.88 [3] section 6.5.1 for LTE.

7.6.5 Key Management for 5G Roaming Security

5G inter-PLMN roaming security (as defined in 3GPP TS 33.501 [19]) requires cryptographic



keys to achieve peer authentication, message integrity and confidential communication. These cryptographic keys need to be managed and exchanged between stakeholders involved in roaming.

Key management in the context of this document refers to the process and technology used by mobile network operators (MNOs) and IPX providers to exchange their certificates, and how the trust relations are established between interconnect partners.

It is required that every MNO uses at least one Root Certification Authority (CA). The reason for this is, that there is no single global CA which could be considered as trusted for all MNOs located in different geopolitical regions. A dedicated Public Key Infrastructure (PKI) for signalling security is required. It is required that every MNO independently operates a PKI including a Root CA, and that it uses this PKI to issue certificates for its own network elements and servers, as well as for the IPX providers that it has a contractual relationship with. It is further required that the policies and procedures governing the operation of the PKI, including the issuance and revocation of certificates, has been documented by each MNO.

Issuer certificates are exchanged manually on a bilateral basis. This requires staff involvement.

> **Note**: Manual exchange of certificates is just an initial procedure for early 5G roaming agreements. An automated solution is under development, which will replace the manual procedures in due course.

As anybody could create an issuer certificate containing an identifier and a public key, there is a need to verify that a particular certificate actually belongs to a particular entity. This verification requires the use of a separate communication channel, i.e. not the one used to transport the issuer certificate.

By default, MNOs should run its own roaming operations and deploy a SEPP. They are responsible for performing the procedures described in this section. Depending on the service offering of IPX providers and on the agreements between MNOs and IPX providers, some of the inter-PLMN security functionality may be operated by the IPX provider on behalf of the MNO. In such a case, responsibilities move from the MNO to the IPX provider. The IPX provider will then have to perform the steps described in this section.

As defined in 3GPP TS 33.501 [19], MNOs issue certificates for their serving IPX providers. The corresponding keys, belonging to the IPX provider, are to be used by the IPX provider when it modifies the signalling messages on transit. Depending on the roaming relation between two MNOs, the IPX Provider needs to attach the corresponding certificate to the modified 5G signalling message, so that the receiving MNO can validate the modification against the Root CA certificate of the sending MNO.

In short, certificate management consists of:

1. Issuing a certificate with the MNO’s own PKI for each SEPP
2. Share the Issuer certificate with all roaming partners through another channel than the IPX network
3. Validate through a separate channel, i.e. by phone, the correctness of the received issuer certificate by validating the certificate’s fingerprint

4. Install the received issuer certificates from peer MNOs in the SEPP and bind them to the respective peer operator's SEPP configuration.

Certificate management needs to be done correctly and carefully to ensure that the certificates belong to the entity they claim they belong to and to ensure that the security controls are effective as GSMA PRD FS.34 [37] specifies. GSMA PRD FS.34 [37] describes in detail the prerequisites for the certificate management, the caveats and the steps of the certificate management, and it also provides background information on certificates, Certification Authorities (CA) and other related aspects. Following the guidelines in GSMA PRD FS.34 [37] is a requirement for 5G roaming.

7.6.6 Protection Policy Agreement and Exchange

- Technical descriptions on creating and handling protection policies.
- Create/handle Modification Policy
- Create/handle Encryption Policy
- Technical aspects of exchanging policies
- Technical aspects of keeping policies up-to-date

7.6.7 Preparatory Steps per 5G Roaming Relation

- Agree on and exchange protection policies and keys as described above.
- Section covers the procedures and organisational framework to follow the technical guidelines in the previous two subsections.
- Establish communication channels to easily deploy policy and key updates.

7.6.8 Error Handling

For 5G roaming, the SEPP handles the security errors in the following cases:

Errors in verifying the integrity protection of the N32-f message: if the receiving SEPP is not able to verify the integrity protection of the message, the receiving SEPP responds an error signalling message to the initiating SEPP with an appropriate status code (as specified in 3GPP TS 29.573 [10]).

Errors in decrypting the JWE ciphertext in the N32-f message: if the receiving SEPP is not able to decrypt the JWE ciphertext in the N32-f message, the receiving SEPP responds an error signalling message to the initiating SEPP with an appropriate status code (as specified in 3GPP TS 29.573 [10]).

Errors in checking integrity of the JSON object in the N32-f message: if the receiving SEPP fails to check the integrity of the JSON object in the N32-f message, the receiving SEPP responds an error signalling message to the initiating SEPP with an appropriate status code (as specified in 3GPP TS 29.573 [10]).

Errors in verifying the JWS signatures added by the intermediaries (i.e. IPX provider): if the receiving SEPP fails to verify the JWS signatures added by the intermediaries, the receiving

SEPP responds an error signalling message to the initiating SEPP with an appropriate status code (as specified in 3GPP TS 29.573 [10]).

Errors in verifying the PLMN-ID contained in the N32-f message: if the receiving SEPP verifies that the PLMN-ID contained in the incoming N32-f message mismatch the PLMN-ID in the related N32-f context, the receiving SEPP responds an error signalling message to the sending SEPP with "403 Forbidden" status code with the application specific cause set as "PLMNID_MISMATCH" (as specified in 3GPP TS 29.573 [10]).

7.6.9 Issue Tracking and Incident Handling

- Forward issues to involved partners.
- Agree on machine readable data structure of issues raised towards stakeholders.
- Agree on procedures for issue tracking and how to establish them across stakeholders.

7.6.10 Risks from Interworking with Different Technology Generations and Signaling Protocols

The security to end-users highly depends on the concatenation of all the technical elements involved for the communication including the protection capabilities supported by the device, the type of radio technology and the type of signaling.

A well-known attack strategy is downgrading attacks (or bidding down attacks) with the aim that the device connects to an older mobile system with less secure protection capabilities. In particular, these attacks are targeting weaknesses or imperfections in the interworking solutions between different signaling protocols.

The specifics of the 5G, LTE (4G), 3G and 2G use cases are outlined in detail in GSMA PRD FS.21 [36] for the following roaming scenarios:

a. 5G SA scenario
b. 5G NSA and native LTE scenarios
c. 5GC with EPC interworking scenario
d. Native 2G and 3G scenarios.

As an illustration, Figure 12 shows in more detail the mobile roaming scenarios a and b with the best protection capability. This is with end-to-end supported confidentiality protection (on top of authentication and integrity protection) by means of either a Digital Signature (DESS Phase 2) or HTTP/2 per security perimeter segment. The diagram shows that confidentiality protection can only be supported for a 5G UE when the device is end-to-end controlled either by:

- The 5G SA scenario with end-to-end HTTP/2 signaling support between SEPPs via the N32 interface as specified in GSMA PRD FS.36 [41].

- The 5G NSA scenario with end-to-end DESS Phase 2 enhanced Diameter signaling support between the DEA/SigFW border elements of the EPC networks as specified in GSMA PRD FS.19 [34].

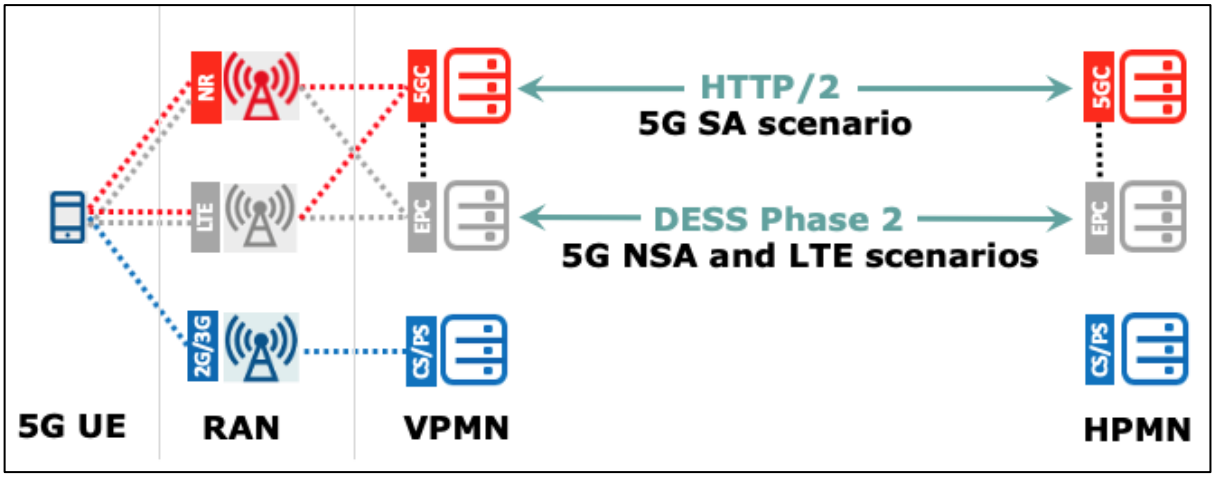


Figure 12 Confidentiality Protected Roaming Scenarios

Note1: Typically, SS7 is used for the 2G and 3G roaming scenarios. However, for 3G PS, Diameter may also be used via the S6d interface.

The less protected of the roaming scenarios apply when the roaming traffic is exchanged via either the standard Diameter signaling (without the DESS enhancements) or via SS7 signaling. This is illustrated in Figure 13, and applies for the following roaming scenarios with a 5G UE:

- The 5G NSA scenario with the standard Diameter support between the DEA/SigFW border elements of the EPC networks as specified in GSMA PRD FS.19 [34] or by means of the SS7 signaling as specified in GSMA PRD FS.11 [44].
- When the 5G UE is paging in 2G or 3G because then the roaming is being supported via SS7 signalling as specified in GSMA PRD FS.11 [44].

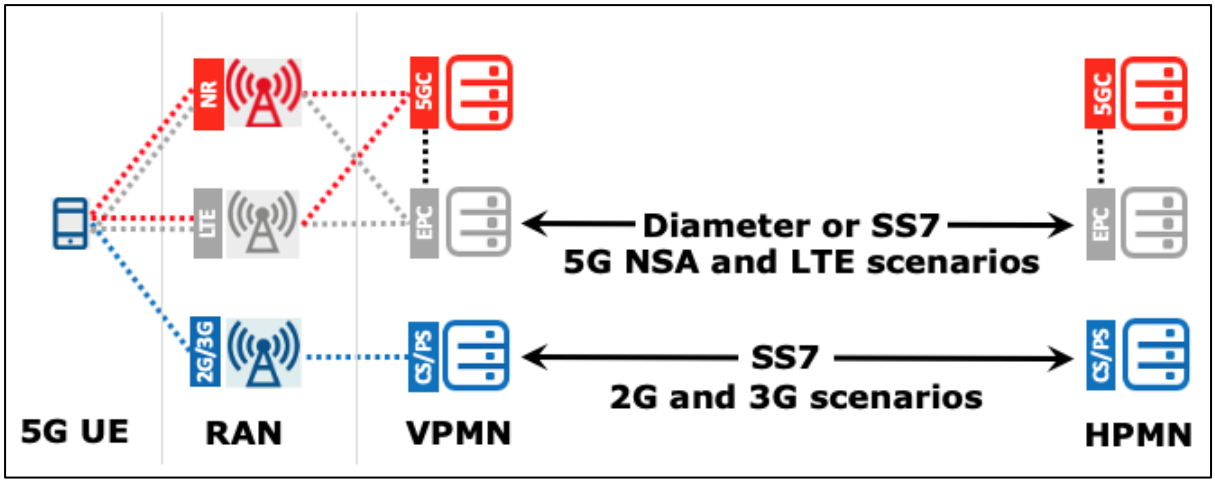


Figure 13 Least Protected Roaming Traffic Scenarios

Note2: Typically, SS7 is used for the 2G and 3G roaming scenarios. However, for 3G PS Diameter may also be used via the S6d interface.

Please be referred to GSMA PRD FS.21 [36] for a complete overview of the other scenarios and the security impact that is exposed via the network signaling by the parallelism of technologies like 2G, 3G, 4G and 5G in combination with the coexistence of SS7, Diameter and HTTP/2 signaling protocol suites.

7.7 Steering of Roaming in 5GS

3GPP defined a solution to enable the Steering of Roaming when using NR connected to 5GC, see 3GPP TS 23.501 [1] and Annex C of 3GPP TS 23.122 [48]. See also GSMA PRD IR.73 [31].

8 Technical Requirements for QoS support

This section covers the functionality needed in the VPLMN and in the HPLMN in order to support QoS procedures for 5GS roaming.

Support of QoS procedures whilst roaming has several aspects:

1. Ensuring that an outbound roamer will be given the expected level of QoS for the service the outbound roamer is using, within the limits of the roaming agreement.
2. Ensuring that the QoS parameters of an inbound roamer are within the limits of the roaming agreement.
3. Enforcement of the actual QoS by the VPLMN.

8.1 5G QoS Model

The 5G QoS model is based on QoS Flows. The 5G QoS model supports both QoS Flows that require guaranteed flow bit rate (GBR QoS Flows) and QoS Flows that do not require guaranteed flow bit rate (Non-GBR QoS Flows).

According to section 5.7 of 3GPP TS 23.501 [1], any QoS Flow is characterised by

- a QoS profile;

- one or more QoS rule(s) and optionally, for non-standardized 5QI and/or Reflective QoS control, QoS Flow level QoS parameters associated with these QoS rule(s); and
- one or more uplink (UL) and downlink (DL) Packet Detection Rule(s) (PDR).

Within the 5GS, a QoS Flow associated with the default QoS rule is required to be established at PDU Session establishment and remains established throughout the lifetime of the PDU Session. This QoS Flow should be a Non-GBR QoS Flow.

8.2 5G QoS Profile

A QoS Flow may either be 'GBR' or 'Non-GBR'. The QoS profile of a QoS Flow is sent to the (R)AN and it contains the QoS parameters as described below:

- For each QoS Flow, the QoS profile includes the QoS parameters:
  - 5G QoS Identifier (5QI); it is a scalar that is used as a reference to a specific QoS forwarding behaviour (e.g. packet loss rate, packet delay budget) to be provided to a 5G QoS Flow.
  - Allocation and Retention Priority (ARP): this is a set of 3 parameters used to decide whether a QoS flow establishment / modification / handover can be accepted or needs to be rejected in the case of resource limitations. It may be also used to decide which existing QoS Flow to pre-empt during resource limitations. ARP is composed of:
    - ARP Priority Level (PL): relative importance of a QoS Flow (range from 1 to 15 with 1 being the highest priority);
    - ARP pre-emption Capability (PCI): ability of a QoS Flow with higher ARP PL to get resources that were already assigned to another QoS Flow with a lower ARP priority level; and
    - ARP Pre-emption Vulnerability (PVI): possibility of QoS Flow resource pre-emption by another QoS flow having higher ARP PL and ARP PCI. PVI should be set appropriately to minimize the risk of a release of this QoS Flow.
- For each Non-GBR QoS Flow only, the QoS profile can also include the QoS parameter:
  - Reflective QoS Attribute (RQA).
- For each GBR QoS Flow only, the QoS profile also includes the QoS parameters:
  - Guaranteed Flow Bit Rate (GFBR) - UL and DL: denotes the bit rate that is guaranteed to be provided by the network to the QoS Flow over the Averaging Time;
  - Maximum Flow Bit Rate (MFBR) - UL and DL: limits the bit rate to the highest bit rate that is expected by the QoS Flow;
- In the case of a GBR QoS Flow only, the QoS profile can also include one or more of the QoS parameters:

- Notification control;
- Maximum Packet Loss Rate - UL and DL.

Each PDU Session of a UE is associated with per Session Aggregate Maximum Bit Rate (Session-AMBR). Session-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows for a specific PDU Session.

Each UE is associated with per UE Aggregate Maximum Bit Rate (UE-AMBR). UE-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows of a UE for all established PDU sessions.

The standardized 5QI to QoS characteristics mapping can be found in section 5.7.4 of 3GPP TS 23.501 [1].

8.3 QoS control

In general, any QoS settings requested by the HPLMN should be in accordance with the Roaming Agreement. However, in order to protect its network against unwanted resource usage, the VPLMN, through its V-SMF, must control, and enforce, the negotiated QoS.

8.3.1 Procedures Involving QoS Control

QoS control is required due to UE or at H-SMF initiated procedures that result in the QoS Flow establishment/modification/deletion, regardless of the triggers behind these procedures.

It is up to the HPLMN to implement a PCC infrastructure which is mandatory if the HPLMN provides services requiring dynamic/non-dynamic QoS control. For instance, voice requires guaranteed bit rates and hence require the SMF to setup a Guaranteed Bit Rate (GBR) QoS Flow requested by the PCF.

In this scenario and according to 3GPP, the entire PCC infrastructure remains inside the HPLMN. See the architecture diagram below.

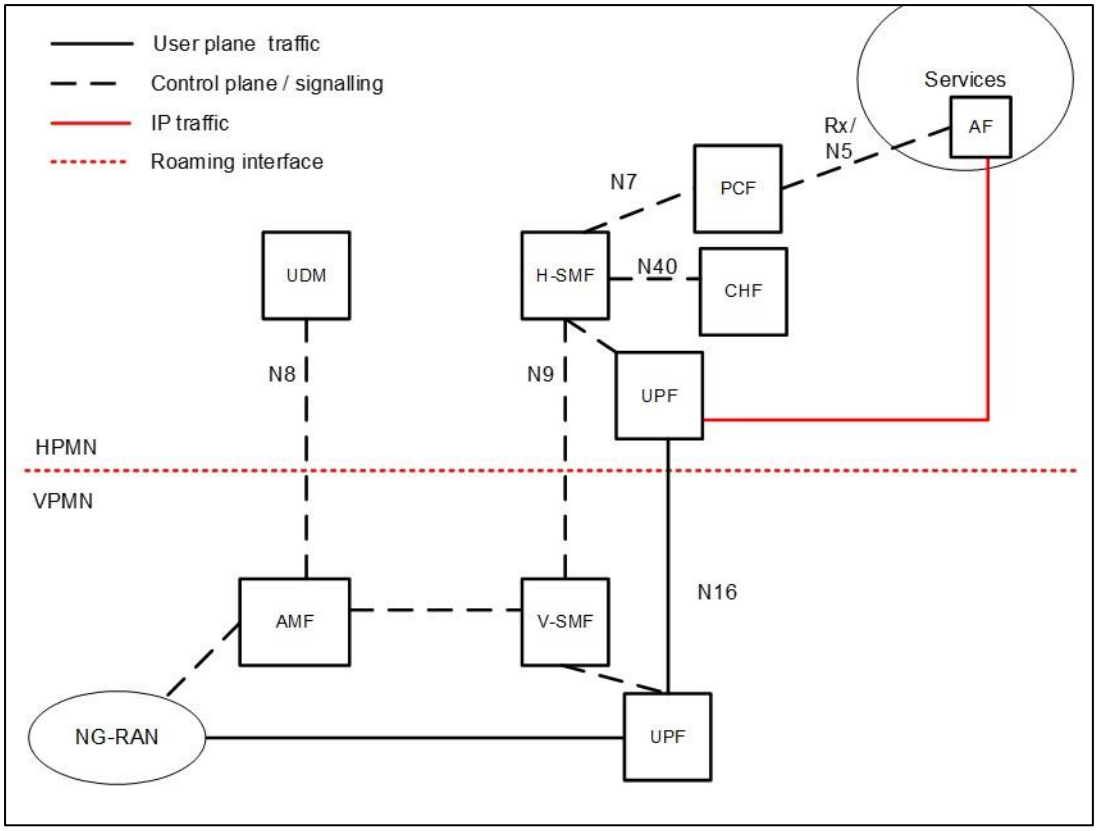


Figure 14 PCC Architecture with Home Routed Architecture

Within the above architecture, and for home routed traffic, the following must be fulfilled:

1. The VPLMN must support the relevant QoS control procedures.
2. The VPLMN and the HPLMN must be able to ensure that QoS parameters of roamers are within the limits of the roaming agreement.
3. The VPLMN must enforce the QoS.

If QoS differentiation requires only the use of the default QoS flow (and no dedicated QoS flow), the H-SMF may modify the QoS parameters of the default QoS flow within the limits of the roaming agreement.

If services which require dynamic QoS and/or service specific QoS are deployed and the QoS of the default QoS flow is not sufficient, the VPLMN must support PDU session modification procedures, initiated by the H-SMF based on HPLMN decision or in response to PCF initiated policy association modification:

- to establish new dedicated QoS flow(s) - this procedure is invoked by the H-SMF if for example the QoS of the already established QoS flows cannot support the new requested service; or

- to modify one or several of the QoS parameters exchanged between the UE and the network related to existing QoS Flows.

8.3.2 Requirements for the VPLMN

Control of QoS parameters within the VPLMN V-SMF requires:

- QoS profile definition within the Roaming Agreement; and
- the V-SMF checks any QoS parameters sent by the H-SMF during a PDU session establishment and during a PDU session modification to ensure they comply to the Roaming agreement.

A roaming QoS profile in V-SMF is defined by:

- a list of allowed 5QI (GBR and non-GBR);
- a remapping Matrix for non-GBR 5QI (including 5QI 5);
- maximum values for ARP PL/PCI/PVI settings (Warning on the notion of maximum value for PCI/PVI); and
- maximum values for UE- and Session-AMBR, MFBR and GFBR values (UL and DL).
- Maximum Packet Loss rate (UL and DL) for a GBR QoS flow belonging to voice media

If a QoS profile is not explicitly described during the roaming agreement definition, the default profile, as described in “5GS Roaming information” in the VPLMN IR.21 shall implicitly apply.

Mobile Operators may have implemented in their networks QoS parameters for IMS services (5QI, ARP-PL, PVI, PCI, MFBR etc.) whose values could vary from operator to operator.

There are several challenges to support this diversity in a roaming environment including:

1. Inconsistent roaming experiences from one partner network to another, including conflicting priorities during a congestion. For example, an incoming roamer unlikely will get a better treatment than the home subscribers for the same service.
2. Complex roaming controls for inbound and outbound QoS management procedures on a per-partner basis.
3. Potential denial of service when the roaming partner does not accept the requested QoS profile

To overcome these challenges, guidelines to specify a minimum set of inbound roaming QoS parameters that all operators should support to allow a consistent and predictable N9HR roaming experience is proposed in Annex A. While this helps to facilitate roaming support ; bilateral roaming agreements always take precedence if the operators choose to negotiate different QoS parameters. For example, operators requiring 5QI=2 for video can negotiate through their bilateral roaming agreements different 5QI.

In order to ensure that a PDU session can be established successfully without violating the QoS profile for inbound roamers from a given HPLMN, the following functionalities are required by the VPLMN:

- During a PDU session establishment, the V-SMF may apply VPLMN policies related to the SLA negotiated with the HPLMN or with QoS values supported by the VPLMN; such policies may result in that V-SMF does not accept the PDU Session or does not accept some of the QoS Flows requested by the H-SMF. When the V-SMF accepts at least one QoS flow, it transfers (via the AMF), only for accepted QoS flows, the corresponding N2 (and NAS) request towards the 5G AN (and the UE). The V-SMF notifies the H-SMF about the rejected QoS Flows. See section 4.3.2.2.2 in 3GPP Release 16 TS 23.502 [2].

- During a PDU session modification: Based on the operator policies and roaming agreements, the V-SMF may decide to fully accept or reject the QoS information provided by the H-SMF. The V-SMF shall also be able to accept a subset of the QoS flows requested to be created or modified within a single H-SMF request i.e. V-SMF can accept some QoS flows and reject other QoS flows in the same response to the H-SMF. See section 4.3.3.3 in 3GPP Release 16 TS 23.502 [2].

If the 5QI, ARP, Session-AMBR, GFBR and MFBR values from the HPLMN are within the pre-configured range, the V-SMF must accept the procedure. If the V-SMF detects that Session-AMBR or MFBR and/or ARP PCI/PVI values are outside the range, the V-SMF may downgrade Session-AMBR, MFBR and/or ARP PCI/PVI values to the values based on the roaming agreement or reject the procedure. For 5QI, ARP Priority Level (PL) and GFBR values, if the V-SMF detects that a value is outside those ranges, the V-SMF shall reject the procedure.

To avoid downgrade of the Session-AMBR, MFBR and/or ARP PCI/PVI value, the HPLMN must ensure that the QoS parameters from the HPLMN are within the limits of the roaming agreement, see also section **Error! Reference source not found.**.

8.3.3 Requirements for the HPLMN

When a Policy and Charging infrastructure is deployed in the HPLMN, then the HPLMN's PCF provides the QoS parameters to the HPLMN's SMF, which in turn are sent to the VPLMN as part of all QoS flow management procedures.

In order to ensure that the requested QoS sent to a VPLMN is within the limits of the roaming agreement, the HPLMN's PCF must - in case of an outbound roamer – only provide QoS parameters (see section 8.2) to the HPLMN's SMF, which are within the limits of the roaming agreement with the respective VPLMN.

According to section 5.7.2.2 of 3GPP TS 23.501 [1], and unless otherwise specified within the Roaming agreement for specific services, HPLMN should not send ARP PL values between 1 and 8 for outbound roamers.

8.3.4 QoS Control for IMS APN in the N9HR Architecture

For the IMS "well known" APN, dedicated QoS flows are established to carry voice/video media. In order to minimize the effect when these QoS flows are used for non-voice/video

media services, the GBR value of these QoS flows (GBR QoS flow for voice, and optionally a second GBR QoS flow or a non-GBR flow for video media) must be enforced by the VPLMN, based on the roaming agreement, to protect the network e.g. to avoid capacity overuse. The GBR values should be in accordance with 3GPP TS 26.114 [51] depending on the codec use by the HPLMN.

For connections for an IMS “well known” APN, the services and corresponding 5QI must be supported by the HPLMN, as described in section 6.2.2.

Note: If neither the HPLMN, VPLMN, or both deploy the necessary QoS related functions (i.e. 5QI, ARP, Session-AMBR, GBR parameters, packet filters, and downgrading function) to support required QoS as agreed commercially between the HPLMN and VPLMN, there is a possibility that unnecessarily high QoS and/or wrong packet filters are applied for applications on established QoS flows, and this might cause negative impacts on the resource usage in the VPLMN. If the VPLMN is not able to control the QoS settings and hence these are applied on all home routed DNNs, the QoS settings associated with the IMS well known APN (5QI, ARP…) may be used also for other APNs than the IMS well known APN and get priority on all other customers, including domestic ones.

8.3.5 Support of QoS by the IPX

When one or more IPX providers are used in the path between the VPLMN and the HPLMN;

- The sending service provider is expected to map the 5QI value to DSCP (differentiate service code point) on the corresponding GTP.
    - Example: a GTP packets carrying 5QI=1 voice should be tagged with the corresponding DSCP value “EF”.
- The IPX providers are expected to honour the requested QoS and transparently transfer the DSCP value to the next hop.

8.3.6 Enforcement of QoS by the VPLMN

If a VPLMN has agreed to enforce QoS in a roaming agreement, then the VPLMN is required:

- To engineer its access and core networks to fulfil the correspondent QoS characteristics (Resource Type, Default Priority Level, Packet Delay Budget, Packet Error rate, Default Maximum Data Burst Volume and Default Averaging Window) according to Table 5.7.4-1 in 3GPP TS 23.501 [1] for the 5QIs covered by the roaming agreement.
- To apply the right Diffserv Code Points (DSCP) on all inter-PMN GTP-U flows of a given bearer depending on its 5QI.
- To support GBR bearers and provide the requested guaranteed bit rates within the negotiated limits as part of the roaming agreement.

- For connections to an IMS “well known” APN, the services and corresponding 5QIs must be supported by the VPLMN, as describe in section 6.2.2.

9 Testing Framework

IREG test cases for 5GS SBA roaming will be described in a future PRD.

Annex A Guidelines for Proposed Basic QoS Parameters for N9HR Roaming Scenario

This Annex describes the proposed QoS parameters for the N9HR roaming scenario. This is intended to represent the basic QoS parameters that a serving operator should support. However, bilateral agreements may allow operators to negotiate other values. Although this is primarily for IMS services, these recommendations include QoS settings for all services, including traditional internet traffic. These recommendations may be updated in the future to include RCS services.

The proposed QoS values and corresponding services are shown in Table 32.

Parameter	Minimum recommended roaming QoS values					
Service	IMS Voice		IMS Signalling[4]		IMS Video	Internet
5QI	1		5		2 or 8	9
ARP-PL	12		12		14	14
ARP-PVI	Enabled [5]	Disable[5]	Enabled [5]	Disable[5]	Enabled[5]	Enabled[5]
ARP-PCI	Disable[5]	Enabled[5]	Disable[5]	Enabled[5]	Enabled[5]	Disable[5]
MFBR-UL	156[3]					
MFBR-DL	156[3]					
GFBR-UL	156[3]					
GFBR-DL	156[3]					

Table 3 Roaming QoS values

Note 1: Values not shown in the table are out-of-scope of this recommendation and should be agreed bilaterally between operators prior to use.

Note 2: Values in this table are the values that an inbound operator at a minimum should support. If a lower value is requested for any parameter, it should be accepted (e.g. ARP-PL=14 has a lower priority than 12 hence it will be accepted for 5QI=1).

Note 3: MBR and GBR settings (in kbps) are based on the highest values needed to support three concurrent streams of 5QI voice for all codecs, profiles, and level in 3GPP TS 26.114 Annex E [51]. Currently, AMR-NB, RTT, AMR-WB, EVS 13.2, EVS 24.4 are covered. If more codecs are added in the future, this table needs to be updated.

Note 4: IMS signalling may include SIP signalling for IMS Voice, IMS Video, SMS over IP, and RCS services.

Note 5: The request to establish a QoS flow should not be denied based on PCI or PVI; instead, the VPLMN can downgrade 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.

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	26 Sept 2019	PRD First Draft	TG	MCGINLEY, MARK, AT&T
2.0	14 May 2020	Implementation of approved CRs: • NG.113 CR1002 • NG.113 CR1003 • NG.113 CR1004 • NG.113 CR1005 • NG.113 CR1006 • NG.113 CR1008 • NG.113 CR1009 • NG.113 CR1010 • NG.113 CR1011 • NG.113 CR1012 • NG.113 CR1013	TG	MCGINLEY, MARK, AT&T
2.0	21 August 2020	Implementation of NG.113 CR1007	TG	MCGINLEY, MARK, AT&T
3.0	10 November 2020	Implementation of approved CRs: • NG.113 CR1014 • NG.113 CR1015 • NG.113 CR1016 • NG.113 CR1017 • NG.113 CR1019 • NG.113 CR1020 • NG.113 CR1021 • NG.113 CR1022	TG	MCGINLEY, MARK, AT&T

Other Information

Type	Description
Document Owner	GSMA NG
Editor / Company	Mark McGinley, AT&T

Feedback

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.