5G Roaming Guidelines
Version 2.0
28 May 2020

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

Security Classification: Confidential - Full, Rapporteur, Associate and Affiliate Members

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

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

2.1.1 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
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
IMSI	International Mobile Subscriber Identity
IKE	Internet Key Exchange
IP-CAN	IP Connectivity Access Network
IPX	Internet packet Exchange
LA	Location Area

Acronym	Description
LBO	Local Break Out
LTE	Long Term Evolution (Radio)
MAP	Mobile Application Part (protocol)
MBR	Maximum Bit Rate
MME	Mobility Management Entity
NE	Network Element
NEF	Network Exposure Function
NF	Network Function
NR	New Radio (5G)
NRF	Network Repository Function
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
OCS	Online Charging System
PCF	Policy Control Function
PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
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
YAML	YAML Ain’t Markup Language

2.1.2 Terms

Term	Description
Data Off	See GSMA PRD IR.92 [9]
Data Off Enabled Service	See GSMA PRD IR.92 [9]

Term	Description
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

2.2 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 15
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
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

Ref	Document Number	Title
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

2.3 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.

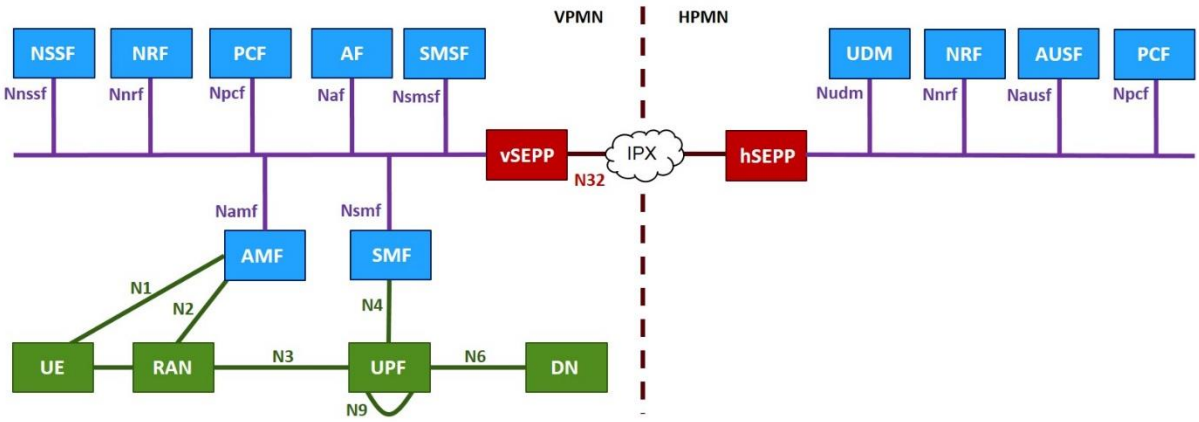

Figure 1 5G System Roaming architecture – Service Based Interface Representation (LBO)

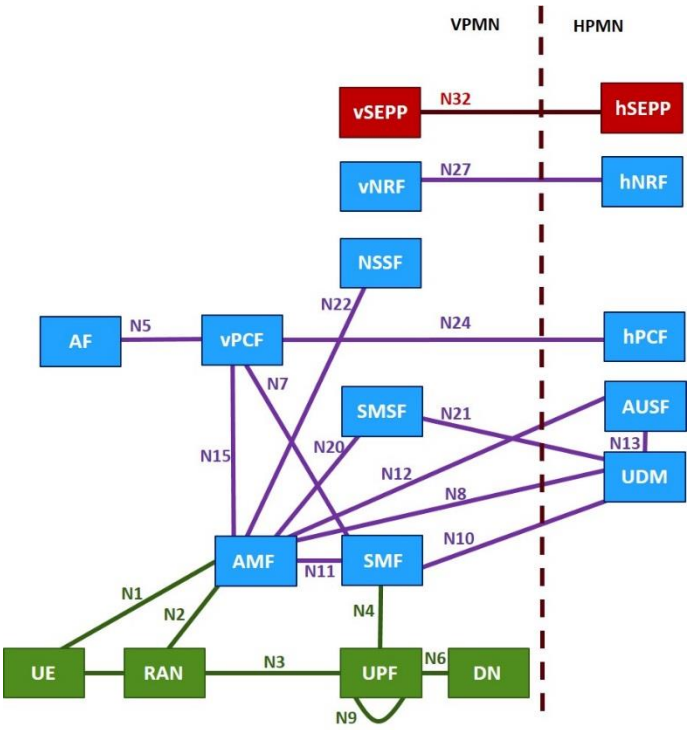

Figure 2 5G System Roaming architecture – Reference point Representation (LBO)

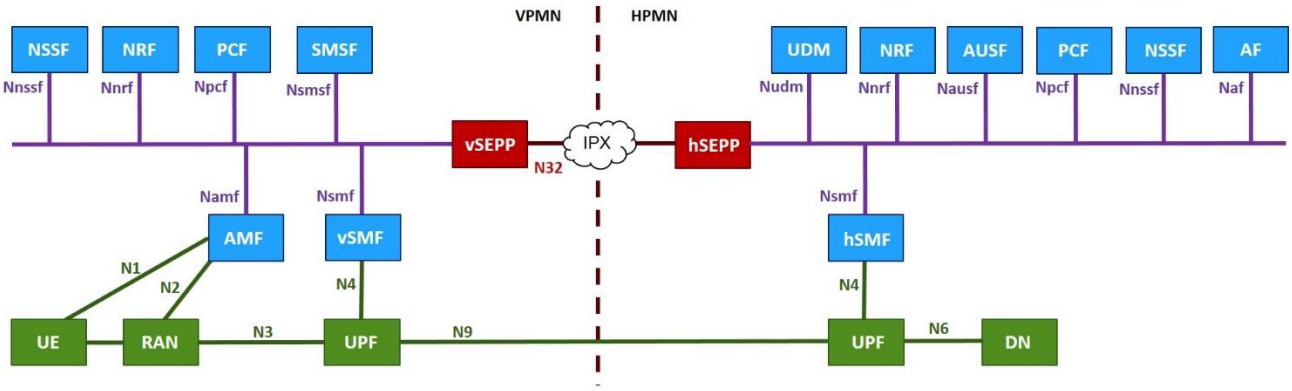

Figure 3 5G System Roaming architecture – Service Based Interface Representation (HR)

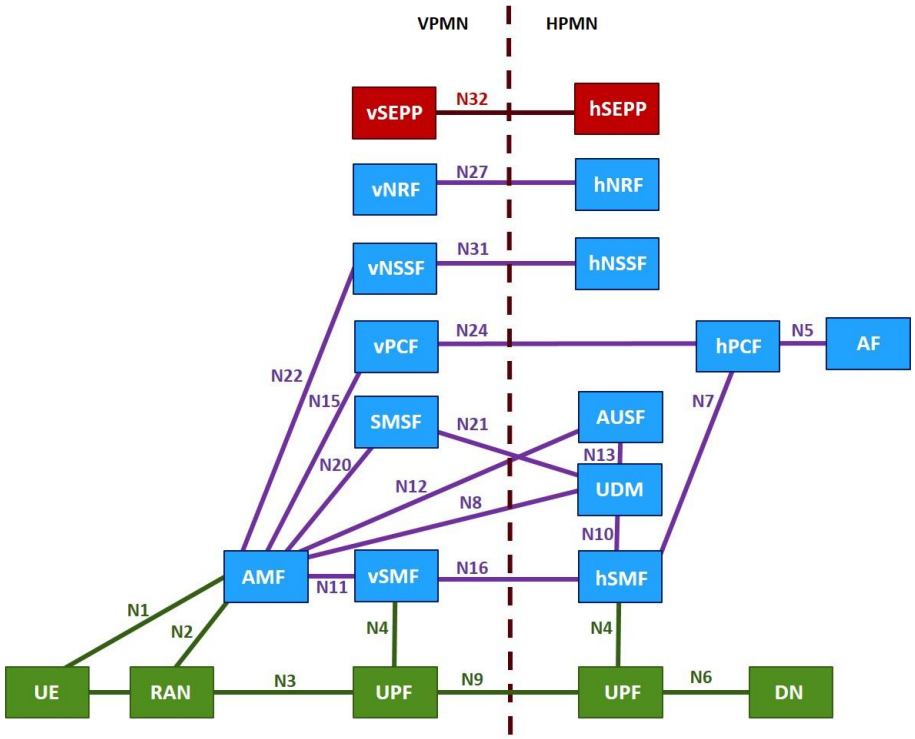

Figure 4 5G System Roaming architecture – Reference point Representation (HR)

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].

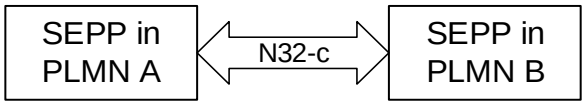

Figure 5 N32-c Interface

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].

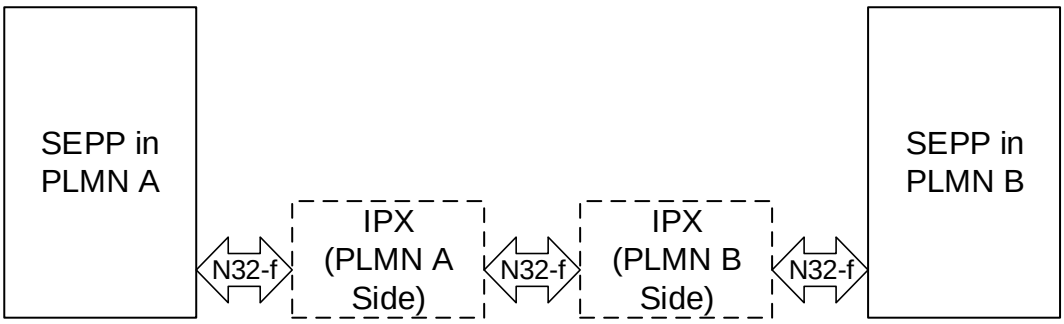

Figure 6 N32-f Interface

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.

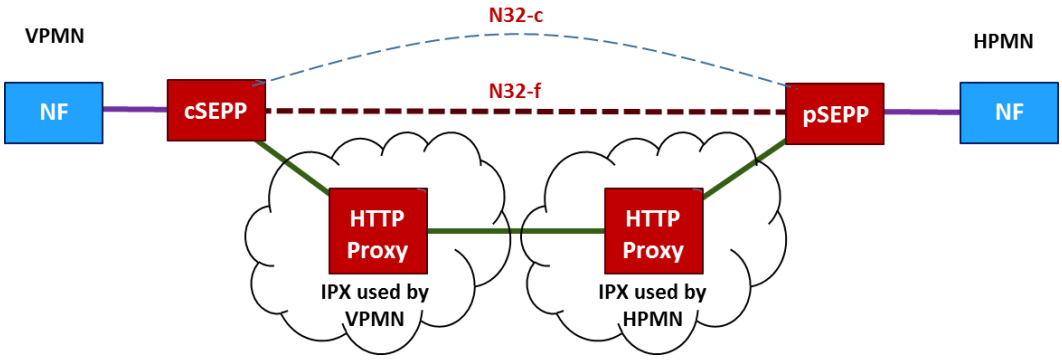

Figure 7 End to end HTTP/2 Roaming Architecture

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

4.3 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.

4.3.1 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.

4.3.2 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 are compliant to 3GPP TS 29.281 [18] Rel-15.

4.4 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 1.

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

Table 1 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+PGWC 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.

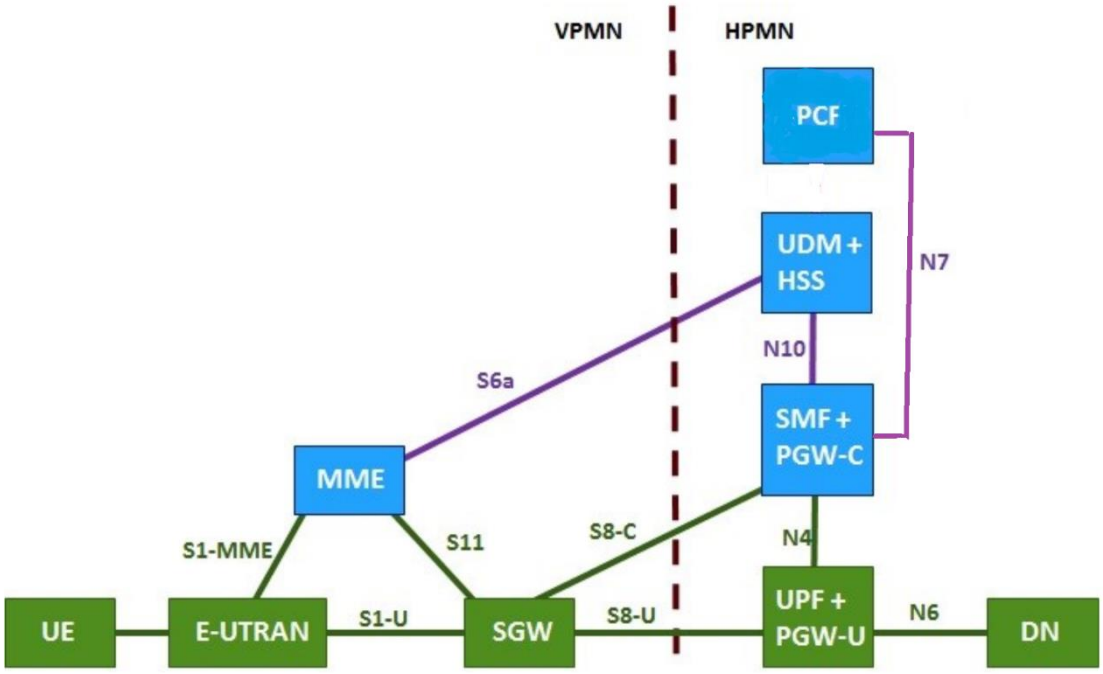

Figure 8 Home-routed roaming architecture for interworking between 5GS EPC/E-UTRAN

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.

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

6 Technical Requirements and Recommendations for Services

6.1 Network Slicing

A 5GS UE and 5GC shall support network slicing. When a UE registers, it will request a Requested NSSAI to the VPLMN, which contains zero or up to eight S-NSSAIs. The

Subscription information shall contain one or more S-NSSAI's. The UE subscription information shall contain at least one default S-NSSAI to be used when the UE registers and includes no S-NSSAI value in the Requested NSSAI. Network slicing and the use of S-NSSAI is described in 3GPP TS 23.501 [1] section 5.15.

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

The GSMA PRD NG.116 [27] provides a standardised view on how a Generic (Network) Slice Template (GST) can be used. The GST provides the template for which slice attributes that characterise a network slice can be applied to. A GST can be filled with values that create a NEST (NEtwork Slice Type), which is a set of attributes for a particular *Use Case* that may be supported by the roaming PLMN operators.

6.1.1 UE support of network slicing when roaming

As stated in 3GPP TS 23.501 [1] Section 5.15.6; if the UE only uses standard S-NSSAI values, then the same S-NSSAI values can be used in the VPLMN as in the HPLMN. If the VPLMN and the HPLMN have an agreement to support non-standard S-NSSAI values in the VPLMN, 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, during the registration procedure, and the AMF informs the UE about the mapped S-NSSAI values. If the UE includes S-NSSAI, then the UE provides to the network the S-NSSAI values provided by the HPLMN and, if available, the mapped S-NSSAI values provided by the VPLMN during registration and PDU session establishment procedure.

6.1.2 5GC support of network slicing when roaming

The UDM in the HPLMN will contain the Subscribed S-NSSAIs inside the Subscription Information. When roaming, the UDM shall provide to the VPLMN only the S-NSSAIs the HPLMN allows for the UE in the VPLMN. i.e. this may be a sub-set of multiple S-NSSAIs.

When the UDM updates the Subscribed S-NSSAI(s) to the serving VPLMN AMF, e.g. during registration procedure, the AMF determines by itself or by interacting with the NSSF.

- Configured NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs
- Allowed NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs.
- rejected S-NSSAIs

The serving AMF then updates the UE with the above information.

It is recommended that the S-NSSAI with eMBB [SST value 1] be supported for roaming, and be the minimum in Subscribed NSSAI in UDM for subscriptions using e.g. Internet access and IMS services. Other S-NSSAI 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.

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 9 below illustrates the AMF registration service operation.

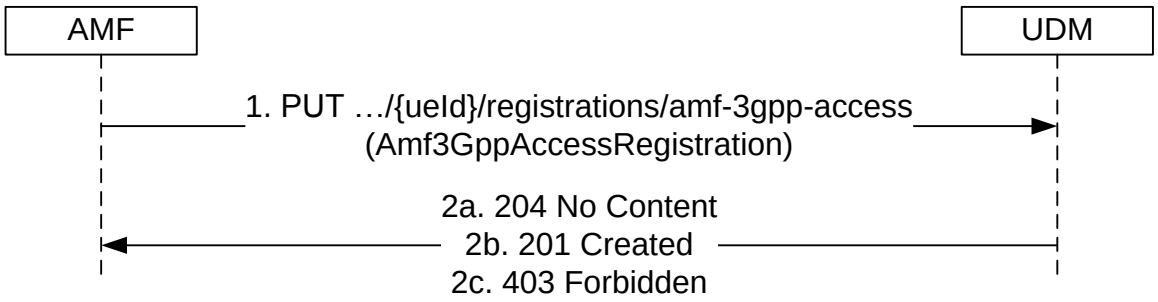

Figure 9 AMF registering for 3GPP access [10] Section 5.3.2.2.2

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 IMS well-known DNN utilises an SMF in the 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 roamed to VPMN" (“ROAMER_ACCESS_VPLMN_AP” in 3GPP TS 29.571 [40] is not active.

Note: The term DNN is used to indicate the SMF or part of the SMF that is 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 SMF in the 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
- The "VPLMN Address Allowed" parameter in the HSS is unset.

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. To achieve this, the SEPP performs application layer security 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

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 roaming control messages are exchanged between SEPPs over the N32 interface with a similar working as in LTE with the filtering of GTP-C roaming control messages as specified in GSMA PRD FS.20 [35]. However, in 5G the related transfer of GTP-U user control message is not altered and will still follow the N9 interface as in LTE.

In this context, a filtering solution, that determines if the GTP-U traffic is linked to a corresponding N32 session, will be needed. This way of working is still under consideration in 3GPP as new a new feature for Release 16 and likely related to a “UP GW Function” on the N9 interface as in 3GPP TS 33.885 [42] section 4.1.17. Further details will be provided with as soon as 3GPP completed their work.

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 **Error! Reference source not found.**) 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 **Error! Reference source not found.**, 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 10 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].

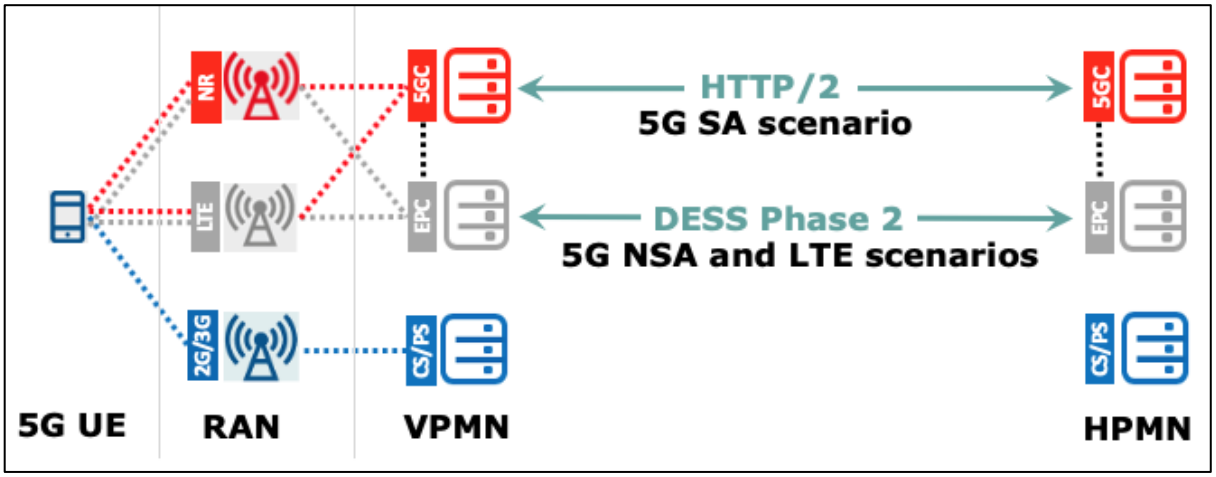

Figure 10 Confidentiality Protected Roaming Scenarios

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 11, 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].

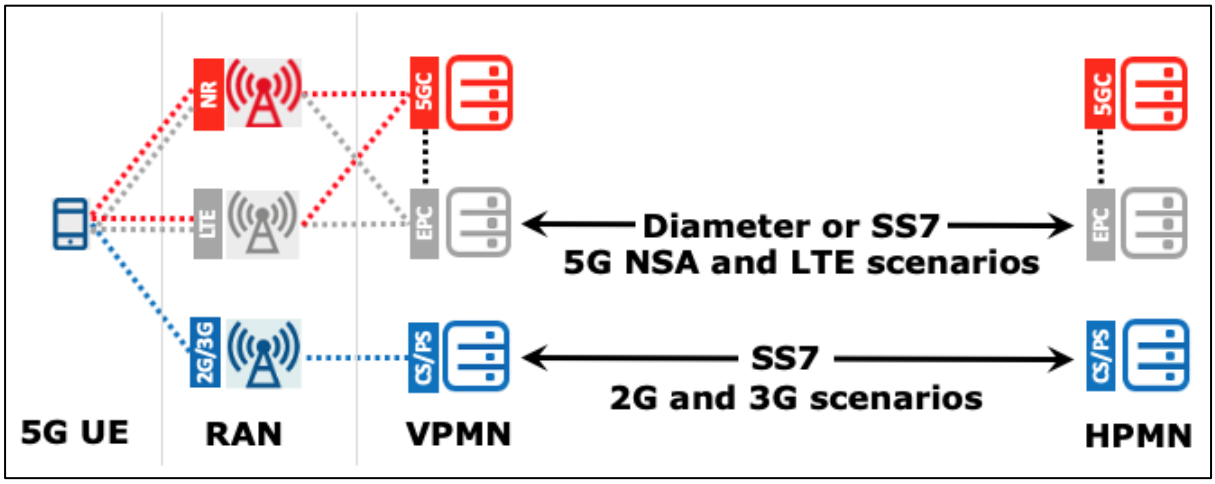

Figure 11 Least Protected Roaming Traffic Scenarios

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 using 5G SBA

3GPP have specified a new method to enable Steering of Roaming when using 5G-NR and the 5GC. Details are specified in GSMA PRD IR.73 [31].

8 Technical Requirements for QoS support

8.1 QoS Parameters definition

TS 23.501 – 5.7

8.2 QoS management

8.3 QoS control

9 Testing Framework

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

Annex A Document Management

A.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

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.