5GS Roaming Guidelines

Version 14.0

January 2026

Security Classification: Non-Confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document 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

Disclaimer

The GSMA 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.

Compliance Notice

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

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

Table of Contents

1

Introduction

1.1 Overview

This document describes how 5G System (5GS) networks using 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. In addition to guidelines on the 5G roaming architecture, a key focus of this document is to describe deployment models and security impacts the operators need to consider when selecting the deployment models.

References are made to 3GPP specifications covering the 5GS and 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). 3GPP Release 16 is taken as a basis unless otherwise stated.

1.2 Scope

This PRD provides guidelines on the technical requirements, architectures, procedures, and call flows for the control and user plane, as well as on the security architectures for deployment models. The new security element, SEPP (Security Edge Protection Proxy), plays a vital role in protecting the traffic between two networks.

This PRD provides several deployment models for 5GS Roaming, including the trade-offs of each model, to balance operators' different business, operational and security requirements. This provides the reader with a complete picture when making deployment decisions.

GSMA introduces various types of SEPPs in addition to the SEPP defined in 3GPP 5G specifications. Some of which enable a service provider to provide the N32-endpoint on behalf of the PMN. The detailed architecture designs of the different deployment models are described to enable different protection schemes for direct bilateral and hubbing architectures. For hubbing deployments, both application layer end-to-end security and hop-by-hop transport layer link security solutions are described.

This PRD guides the operators on how to deploy various services and capabilities, such as voice, video, messaging, advanced location support, emergency services, steering of roaming, network slicing, URSP and others in a roaming scenario.

This PRD also describes the charging interfaces and Charging Function (CHF) supported for data roaming (HR and LBO), roaming mobility, and SMS over NAS to enable roaming wholesale and retail charging.

In the roaming case, the HPMN can deploy 5GC with EPC interworking (5GC/EPC interworking) support as specified in clause 4.3.2 in 3GPP TS 23.501 [1]. If both HPMN and VPMN 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 deploy two separate cores without 5GC/EPC interworking (denoted in the following as separate 5GC and EPC).

Table 1 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**

Table 1: Possible 5GC/EPC Roaming Scenarios

* 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

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

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

2 Definition of Terms and Acronyms

2.1 Definitions

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

Term	Description
Roaming Intermediary	A provider of roaming related services between VPMN and HPMN on the roaming interface. NOTE: For the purpose of this document the term Roaming Intermediary includes only those providers that deliver transit and hubbing services.
IP or IPX Service Hub	Defined in NG.137.
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 Access Point Name (APN) whose value has a defined specific string of characters

2.2 Abbreviations

Term	Description
3GPP	3rd Generation Partnership Project
5GC	5G Core Network
5GS	5G System
A/AAAA	Address record / IPv6 Address record
AF	Application Function
ALS	Application Level Security
AMF	Access and Mobility Management Function
APN	Access Point Name
ARP	Allocation and Retention Priority
AUSF	Authentication Server Function
CA	Certification Authority
CHF	Charging Functions
DEA	Diameter Edge Agent
DNN	Data Network Name
DNS	Domain Name System
DoS	Denial of Service
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
GMLC	Gateway Mobile Location Centre
GPRS	General Packet Radio Service
GRX	Global Roaming Exchange

Term	Description
GST	Generic (Network) Slice Template
GTP	GPRS Tunnelling Protocol
HBM	HUB MIX
HPMN	Home Public Mobile Network
HR	Home Routed
HSS	Home Subscriber Server
HTTP	Hyper-Text Transfer Protocol
IE	Information Element
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPUPS	Inter-PLMN User Plane Security
IPX	Internet packet Exchange
iSEPP	initiating Security Edge Protection Proxy
JSON	JavaScript Object Notation
LBO	Local Break Out
LMF	Location Management Function (5G)
LTE	Long Term Evolution (Radio)
MBR	Maximum Bit Rate
MCC	Mobile Country Code
MFBR	Maximum Flow Bit Rate
MIoT	Mobile Internet of Things
MME	Mobility Management Entity
MNC	Mobile Network Code
MNO	Mobile Network Operator
NAPTR	Name Authority Pointer Record
NAS	Non-Access Stratum
NDS	Network Domain Security
NEF	Network Exposure Function
NF	Network Function
NR	New Radio (5G)
NR CGI	New Radio (5G) Cell Global Identifier
NRF	Network Repository Function
NSA	Non-StandAlone
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PDR	Packet Detection Rule

Term	Description
PDU	Protocol Data Unit
PFCP	Packet Forwarding Control Protocol
PGW	PDN (Packet Data Network) Gateway
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMN	Public Mobile Network
PRD	Permanent Reference Document
PRINS	PRotocol for N32 INterconnect Security
PSK	Pre-Shared Key
QCI	QoS Class Identifier
QoS	Quality of Service
RAEX	Roaming Agreement EXchange
RAN	Radio Access Network
RAT	Radio Access Technology
RFC	Request For Comments
RH	Roaming Hub
RI	Roaming Intermediary
rSEPP	Responding Security Edge Protection Proxy
RVAS	Roaming Value Added Services
SA	StandAlone
SBA	Service Based Architecture
SBI	Service Based Interface (5G)
SCP	Service Communication Proxy
SEPP	Security Edge Protection Proxy
SIP	Session Initialization Protocol
SMF	Session Management Function
SMSF	Short Message Service Function
S-NSSAI	Single Network Slice Selection Assistance Information
SGW	Serving Gateway
SNI	Server Name Indication
SP	Service Provider
SRV	Service Record
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier
SUPI	Subscriber Permanent Identifier
TA	Tracking Area
TCP	Transmission Control Protocol
TLS	Transport Layer Security

Term	Description
TS	Technical Specification
TTL	Time to Live
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UPF	User Plane Function
UPSI	UE Policy Section Identifier
URI	Uniform Resource Identifier
URSP	UE Route Selection Policy
USIM	Universal Subscriber Identity Module
VLAN	Virtual Local Area Network
VPMN	Visited Public Mobile Network

2.3 References

Ref	Doc 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

Ref	Doc Number	Title
[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
[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	GSMA Key Management
[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 TR 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

Ref	Doc Number	Title
[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)
[52]	3GPP TS 29.501	5G System; Principles and Guidelines for Services Definition; Stage 3
[53]	3GPP TS 23.503	Policy and charging control framework for the 5G System (5GS)
[54]	3GPP TS 24.526	User Equipment (UE) policies for 5G System (5GS)
[55]	3GPP TS 23.167	IP Multimedia Subsystem (IMS) emergency sessions
[56]	GSMA PRD IR.21	GSM Association Roaming Database, Structure and Updating Procedures
[57]	GSMA PRD IR.85	Hubbing Provider Data, Structure and Updating Procedures
[58]	GSMA PRD IR.80	Technical Architecture Alternatives for Open Connectivity Roaming Hubbing Model
[59]	3GPP TS 32.240	Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging architecture and principles
[60]	3GPP TS 32.256	Technical Specification Group Services and System Aspects; Charging management; 5G connection and mobility domain charging; stage 2
[61]	3GPP TS 32.255	Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; 5G data connectivity domain charging; stage 2
[62]	3GPP TS 32.290	Telecommunication management; Charging management; 5G system, charging service; Services, operations and procedures of charging using Service Based Interface (SBI)
[63]	3GPP TS 32.291	Telecommunication management; Charging management; 5G system, charging service; Stage 3
[64]	3GPP TS 32.274	Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Short Message Service (SMS) charging
[65]	3GPP TS.23.273	Technical Specification Group Services and System Aspects; 5G System (5GS) Location Services (LCS); Stage 2
[66]	3GPP TS 29.515	Technical Specification Group Core Network and Terminals; 5G System; Gateway Mobile Location Services; Stage 3
[67]	GSMA PRD WA.51	5G SA Implementation Guidelines
[68]	3GPP TS 33.210	Network Domain Security (NDS); IP network layer security
[69]	3GPP TS 33.310	Network Domain Security (NDS); Authentication Framework

These 5GS Roaming guidelines are accompanied by additional guidelines in other GSMA documents:

- The surrounding security and operational aspects as outlined in GSMA PRD FS.21 [36].
- The support of roaming contracts for 5GS bilateral inter-PMN connection in RAEX utilizing GSMA PRD IR.21 [56] and GSMA PRD IR.85 [57].
- Intuitive descriptions for the internal RH solution options within operator groups as described in GSMA PRD IR.80 [58].
- The manual key management procedure for 5GS roaming support including SEPP Outsourcing in GSMA PRD FS.34 [37].
- The guidelines for 5G Interconnect Security in GSMA PRD FS.36 [41].
- SEPP FQDN resolution via DNS before N32 Handshake Procedure in GSMA PRD IR.67 [8].

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 RFC 2119 [22].

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.

3.1.1 5G System Roaming architecture – Local Breakout (LBO)

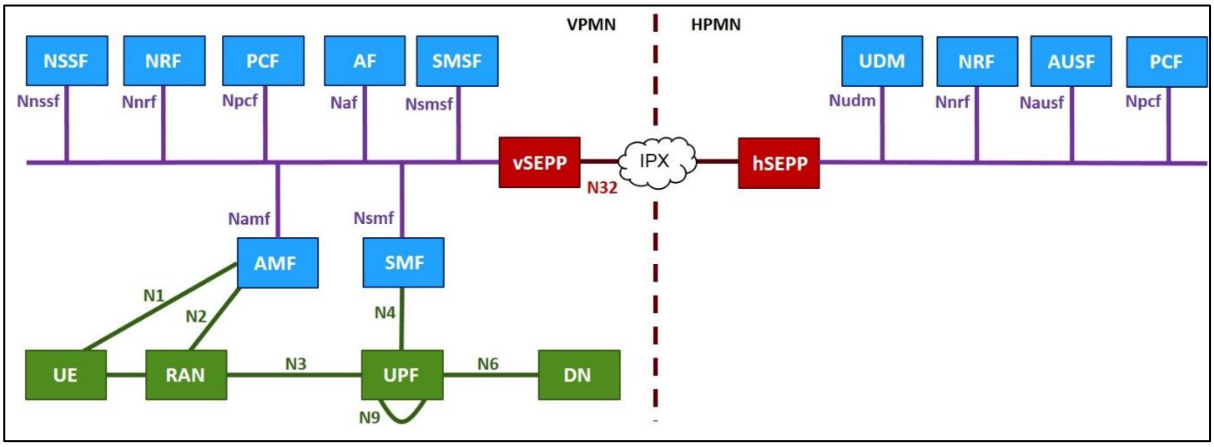


Figure 1 - 5G System Roaming architecture – Service Based Interface Representation (LBO)

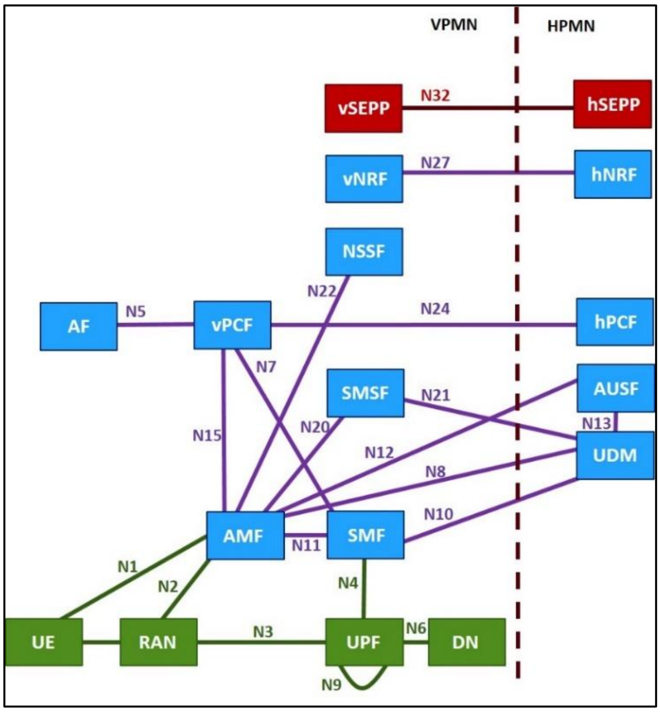


Figure 2 – 5G System Roaming architecture – Reference point Representation (LBO)

3GPP TS. 23.273 [65] defined additional reference points for location services:

- NL3: Reference point between vGMLC and the hGMLC defined in clause 4.2 of 3GPP TS 23.273 [65].
- N51: Reference point between Access and Mobility Management Function (AMF) in VPMN and the NEF in HPMN defined in clause 4.2 of 3GPP TS 23.273 [65].

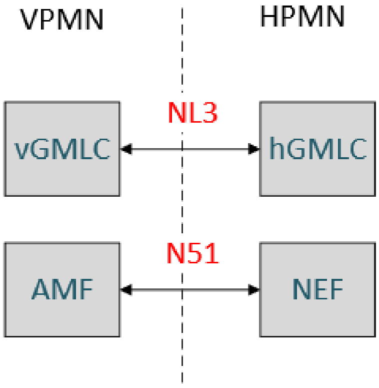


Figure 3 – 5G Reference point Representation (location)

3.1.2 5G System Roaming architecture – Home Routed (HR)

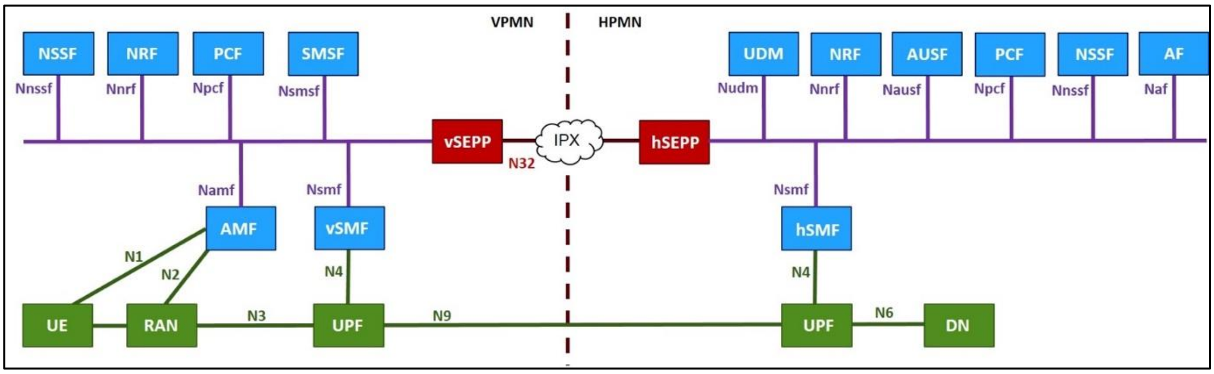


Figure 4 – 5G System Roaming architecture – Service Based Interface Representation (HR)

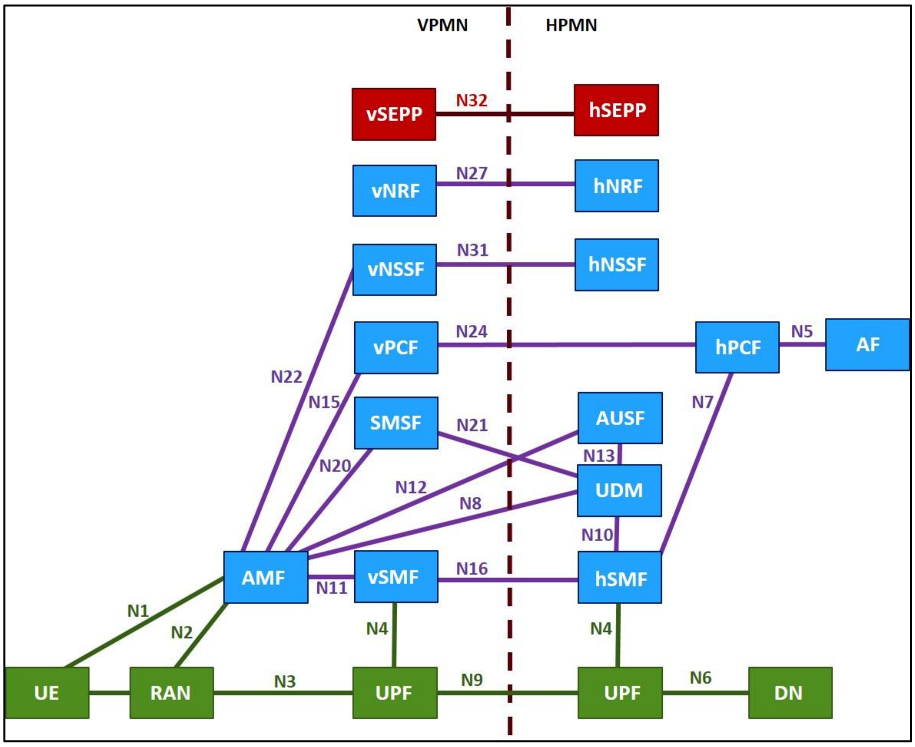


Figure 5 – 5G System Roaming architecture – Reference point Representation (HR)

The SEPP (Security Edge Protection Proxy) is part of the roaming security architecture and described in Section 4.4.

3.1.3 5G System Roaming architecture – Charging

3GPP TS 32.240 [59] defines additional reference points for charging services:

- N40: Reference point between SMF and the CHF in the same PMN defined in clause 4.2 of 3GPP TS 32.255 [61].
- N41: Reference point between AMF and CHF in HPMN defined in clause 4.2.2 of 3GPP Release 16 TS 32.256 [60].
- N42: Reference point between AMF and CHF in VPMN defined in clause 4.2.2 of 3GPP TS 32.256 [60].
- N46: Reference point between SMSF and CHF defined in clause 4.4 of 3GPP TS 32.274 [64].
- N47: Reference point between SMF and the CHF in different PMNs defined in clause 4.2 of 3GPP Release 17 TS 32.255 [61]. See note 4 in Section 3.2.1.
- N107: Reference point between V-CHF and the H-CHF in different PMNs defined in clause 4.2 of 3GPP Release 18 TS 32.255 [61]. See note 4 in Section 3.2.1.

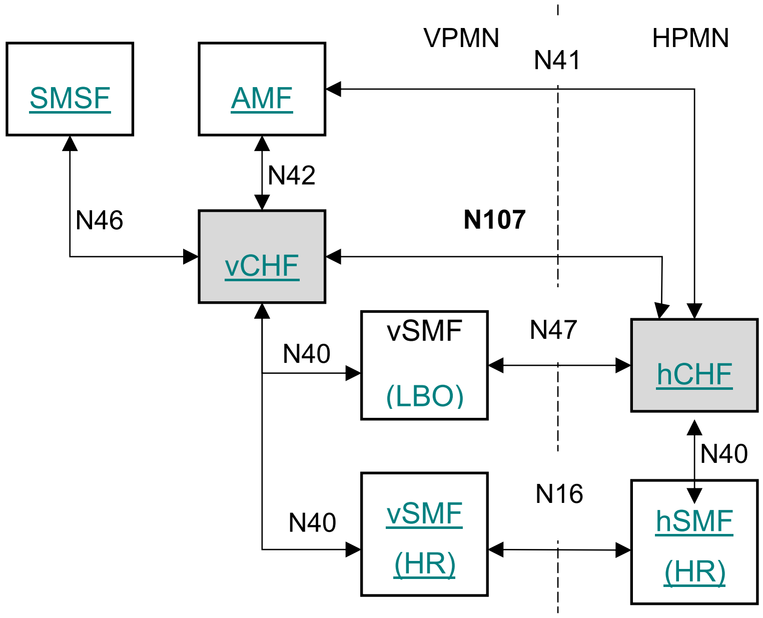


Figure 6 – 5G Reference point Representation (charging)

3.2 Roaming Interfaces and protocols

3.2.1 Interfaces

The following Inter-PMN 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 – AMF	N14	3GPP TS 29.518 [12]	LBO & HR, at Inter-PLMN mobility
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; see also Note 2
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
vAMF – hCHF	N41	3GPP TS 32.256 [60]	LBO & HR; see also Note 3
vCHF – hCHF	N107	3GPP TS 32.255 [61]	LBO; see also Note 4
vSMF – hCHF	N47	3GPP TS 32.255 [61]	LBO; see also Note 4
vGMLC – hGMLC	NL3	3GPP Release 16 TS 29.515 [66]	LBO & HR

Network Functions	Ref Point ID	Service Definition	Used for LBO, HR, or LBO & HR
AMF – NEF	N51	3GPP Release 16 TS 29.518 [12]	LBO & HR

Table 2 – Relevant inter-PMN interfaces for 5GC roaming

NOTE 1: 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.

NOTE 2: The N27 reference point is mandatory in order to discover NFs in the HPMN in roaming scenarios. The use of N27 is more general and applicable to the scenario where NSSF is not deployed by one of the roaming partners, hence the support of N31 is not recommended.

NOTE 3: N41 is defined from Release 16.

NOTE 4: N47 is defined from Release 17 and N107 is defined from Release 18. The N107 reference point provides direct communication between vCHF and hCHF charging functions, supports more than 2 actors in the billing flow and hence recommended as the unique billing interface for LBO roaming cases or multiple actors. The support of N47 is not recommended.

3.2.2 Protocols

General Requirements for Inter-PMN InterfaceRequirements 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.

3.2.2.1 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].

3.2.2.2 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 3GPP TS.23.501 [1] for the Service Based Interfaces.

3.2.2.3 Interface Definition Language – OpenAPI

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

3.2.2.4 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 PMNs can be found in 3GPP TS 29.500 [20].

Further detail on URI Structure can be found in TS.29.501 [52], Section 4.4.

3.3 5G Roaming User Plane Security

In support of 5G roaming, operators will need to exchange N9 traffic in a secure tunnel and filter and control their exchange of GTP-U messages over the N9 reference point with their roaming partners with the Inter-PLMN User Plane Security (IPUPS) functionality.

3.3.1 N9 Operator-to-Operator Security

As per 3GPP Release 16 TS 33.501 [19], N9 traffic over the IPX network shall be confidentiality, integrity, and replay protected by operators. This tunnelled connection shall originate and terminate within the perimeter of the operator (e.g. directly at the UPF or at a Security Gateway (SEG) designed for this purpose).

The key management procedure described in 7.6.5 and in GSMA PRD FS.34 [37] may be used to support the exchange of key material for these inter-operator tunnels in a secure way.

3.3.2 IPUPS

In the 5GS security architecture the 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 7 depicts the home routed roaming architecture where a UPF is inserted in the UP path for the IPUPS functionality.

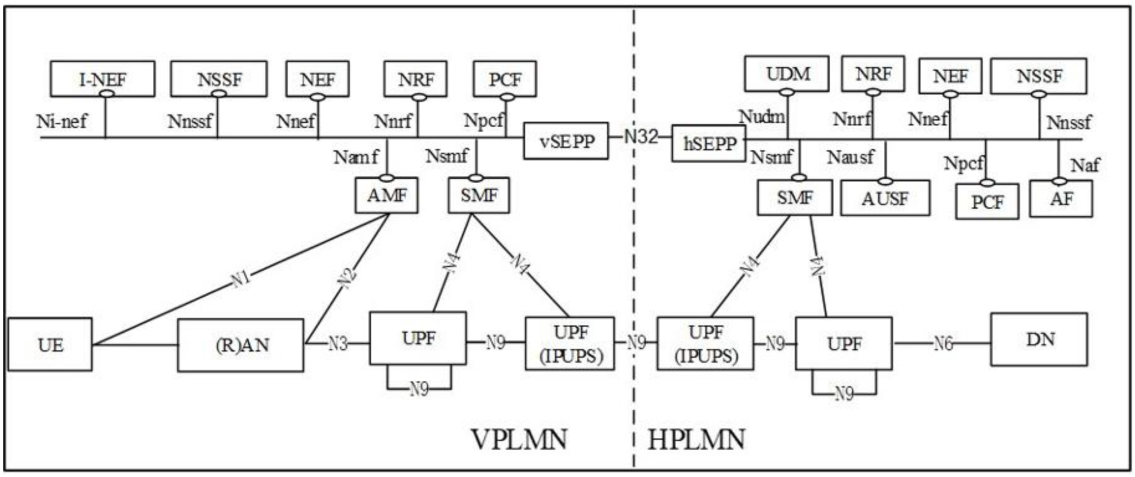


Figure 7 - Roaming Home Routing Scenario – In Serviced Based Interface Presentation

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.

4 Control Plane architecture and Interfaces

4.1 3GPP Architecture and Signalling Interfaces

4.1.1 Inter-PLMN (N32) Interface and Its Endpoints (SEPPs)

4.1.1.1 SEPP

The SEPP acts as a non-transparent Proxy for the NFs when service-based interfaces are used across PMNs. The SEPP is representing the edge of a PMN and connects to the edge of another PMN in roaming scenarios.

3GPP TS 29.573 [10] contains the protocol definitions and specifies message flows, as well as the APIs for the procedures on the PLMN (Public Land Mobile Network) N32 interconnection interface.

The N32 interface is used between the SEPPs. 3GPP has specified N32 to be considered as two separate interfaces, i.e.: N32-c and N32-f, to be established between an initiating SEPP and a receiving SEPP as described in more detail in the following sections. N32-c is used to negotiate the security details to use over N32-f. N32-f is used to transport between SEPPs all HTTP/2 messages that are exchanged between Network Functions (NFs) of different PMNs.

Operators must support using the same server FQDN and port for both N32-c and N32-f/TLS upon request, to meet the requirements of their roaming partners. This recommendation addresses roaming partners that do not support the SNDN32F feature as specified in 3GPP Release 18 TS 29.573 [10].

Note 1: SNDN32F is a feature name in Table 6.1.7-1 of 3GPP Release 18 TS 29.573 [10], not an abbreviation.

Port 443 is the standard and widely accepted server port for communication using HTTPS/TLS. It is recommended to use server port 443 for an N32-c endpoint, and N32-f/TLS endpoint. Port 443 can also be used for the N32-f/PRINS server port, as long as this does not interfere with PLMN-ID-based trust anchoring both in the context of N32-c and of direct N32-f/TLS connections. Details on N32-f/TLS and N32-f/PRINS are provided in the following sections.

The SNDN32F feature as specified in Table 6.1.7-1 of 3GPP Release 18 TS 29.573 [10] allows to use an alternative N32-f server port exchanged via senderN32fPortlist or senderN32fPort. The SNDN32F feature can only be used if both SEPPs support the feature.

Note 2: The SNDN32F feature is backwards compatible since if SNDN32F is not negotiated by two ends the SEPPs fall to the same behaviour as Rel-17 or earlier.

The N32 interface should use the 5G Control Roaming VLAN end-to-end as described on the IR.34.

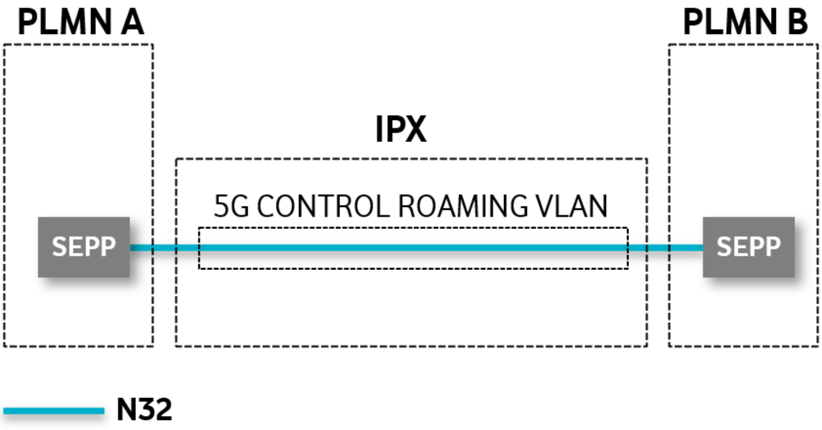


Figure 8 5G control roaming VLAN overview

4.1.1.2 N32-c Interface

N32-c is the Control Plane interface between the SEPPs as illustrated in Figure 9 using TLS for performing the initial handshake and negotiating the parameters to be applied for the actual N32 message forwarding on N32-f. See Section 4.2.2 of 3GPP TS 29.573 [10] on details for negotiating via N32-c in order to either establish bilateral TLS or PRINS to be used for N32-f afterwards. N32-c is also responsible for signalling error messages and tearing down N32-f.

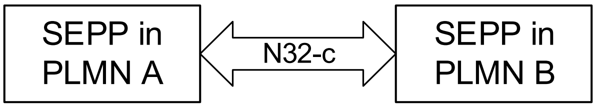


Figure 9 – N32-c Interface (see 3GPP TS 29.573)

If PRINS is negotiated, the SEPPs also exchange protection and modification policies and establish an N32-f security context. Once the initial HTTP/2 handshake is completed the short-lived N32-c connection is torn down.

The N32-c connection is End-to-End between the PMNs' SEPPs. While Roaming Intermediaries cannot intercept this connection, HTTP CONNECT can be used to allow a Roaming Intermediary (HTTP proxy server) to make a decision, whether to allow the SEPP of one PMN to connect to the SEPP of the other PMN via this Roaming Intermediary and allow for e2e negotiation between these two SEPPs.

The HTTP proxy remains on the N32-c path in this case.

NOTE 1: The HTTP CONNECT method is used by the SEPP to request the Roaming Intermediary to set up a TCP connection towards the SEPP. Once TLS is established over this TCP connection, the Roaming Intermediary cannot see what is negotiated between the two PMNs' SEPPs.

NOTE 2: The solution enhancements for PRINS, i.e., additional functionality using roaming intermediaries, such as HTTP CONNECT method and error messages, as further detailed in the next clause are specified in 3GPP TS 33.501 [19] for Rel-18. However as noted in the 3GPP specification, there is no technical limitation to support these enhancements in SEPP implementations starting from Release 16 onwards.

NOTE 3: Both TLS and PRINS are already specified since Rel-15.

4.1.1.3 N32-f Interface

N32-f is the Forwarding interface between two SEPPs representing the PMNs. N32-f is used for forwarding the HTTP/2 messages of the communication between the Network Function (NF) service consumer and the NF service producer either by TLS directly between two SEPPs or by PRINS via one or two Roaming Intermediaries using PRINS application level security protection is provided. See Section 4.2.3 of 3GPP TS Release 16 29.573 [10].

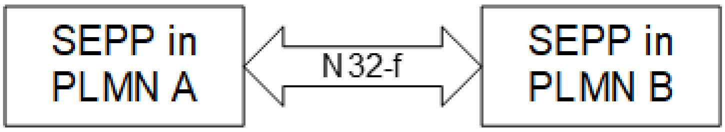


Figure 10 – N32-f Interface with TLS

If TLS is the negotiated security method between SEPPs, N32-f involves only the protection and forwarding of the HTTP/2 messages between the NF service producer and NF service consumer. Roaming Intermediaries can be only involved for IP level routing. Different TLS connections are used for N32-c and N32-f.

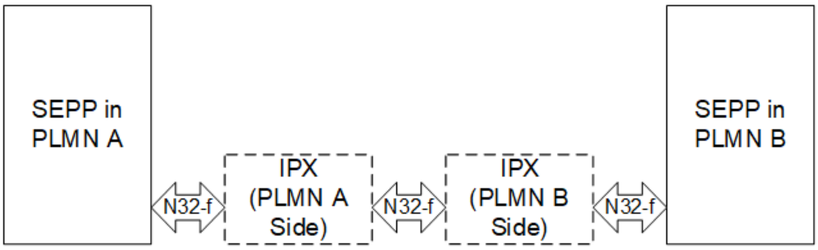


Figure 11 – N32-f Interface with PRINS (ALS)

If PRINS is the negotiated security mechanism between SEPPs, N32-f provides Application Layer Security (ALS) as specified in 3GPP Release 16 TS 33.501 [19] and detailed in 3GPP Release 16 TS 29.573 [10].

4.1.1.4 Roaming Intermediary

If PRINS is the negotiated security mechanism between SEPPs, N32-f provides Application Layer Security (ALS) as specified in 3GPP Release 16 TS 33.501 [19] and detailed in 3GPP Release 16 TS 29.573 [10].

Roaming Intermediary service providers between two SEPPs, and if using PRINS ALS, act as HTTP proxies that are able to modify IEs or insert IEs 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, but in contrast to Diameter, 5G as specified by 3GPP only allows this by the PRINS negotiated policies. This provides in 5G a degree of control and transparency on what can be inspected and modified by Roaming Intermediaries between the two SEPPs representing the roaming partners N32 end-points.

Figure 12 illustrates the End to End HTTP/2 Service Based Architecture HTTP Proxy functions are implemented by the PMN as part of a SEPP and are also needed at Roaming Intermediaries for PRINS. It shows both consumer's SEPP (cSEPP) and producer's SEPP (pSEPP). The cSEPP resides in the PMN where the service consumer NF is located. The pSEPP resides in the PMN where the service producer NF is located.

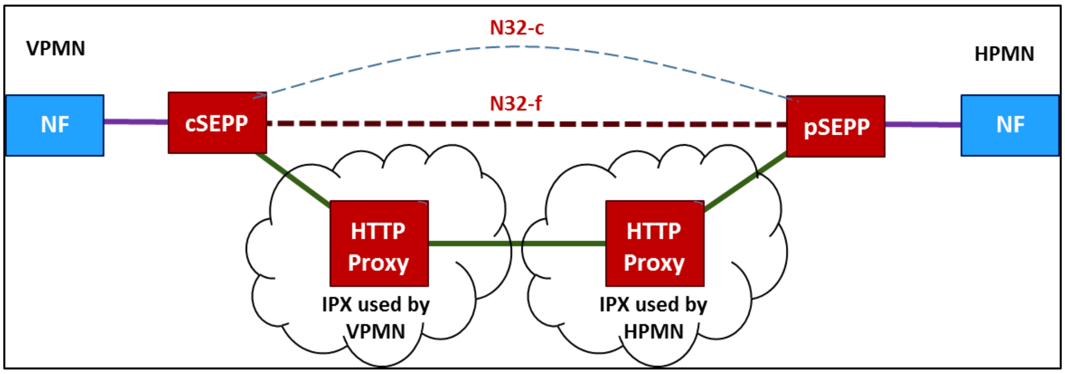


Figure 12 – N32-f Interface with PRINS end to end HTTP/2 Roaming Architecture with Roaming Intermediaries (e.g. IPX transit or Hub)

4.1.2 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 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 3 – 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 signalling is sent via SEPPs as described in Section 4.1.1. Consumers in the VPMN interact with producers in the HPMN. If TLS is used on the N32 interface, and the 3gpp-Sbi-Target-apiRoot header is used in a request by a NF sent to a SEPP, then the 3gpp-Sbi-Target-apiRoot header is not changed by the SEPP and kept in the request sent towards the SEPP in another PMN (remote SEPP) as specified in 3GPP Release 16 TS 29.500 [20].

If 3gpp-Sbi-Target-apiRoot header is used in a request by a NF sent to a SEPP, and the remote SEPP does not indicate support of the 3gpp-Sbi-Target-apiRoot header when negotiating the security policy, then the sending SEPP includes the content of 3gpp-Sbi-Target-apiRoot header into authority and removes the 3gpp-Sbi-Target-apiRoot header before sending the request towards the remote SEPP.

If the NF uses a telescopic FQDN in the HTTP Request to convey the target apiRoot to the sending SEPP, or if TLS is not used between the NF and the sending SEPP, the sending SEPP shall insert the 3gpp-Sbi-Target-apiRoot header in the HTTP request towards the remote SEPP and set it to the apiRoot of the target NF derived from the telescopic FQDN or from the request URI respectively as specified in 3GPP TS 29.500 [20]. If using telescopic FQDN and TLS protection between a NF (e.g. NRF) and the SEPP is required, then the NF and the SEPP have to support Nsepp_Telescopic_FQDN_Mapping Service as specified in Section 5.4 of 3GPP Release 16 TS 29.573 [10].

Whether the SEPP and NFs within the SEPP's PMN use telescopic FQDN or the 3gpp-Sbi-Target-apiRoot header is based on PMN operator's policy. The use of 3gpp-Sbi-Target-apiRoot header is recommended.

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 (see 3GPP TS 33.501 Annex R).

Sections 4.2 and 4.3 of this PRD provides the guidelines for the 5GS roaming deployment scenarios.

4.1.3 5GS domain, FQDN and URI

Mobile operators shall follow home network domain naming as specified in 3GPP TS 23.003 Section 28.2 (Home Network Domain), in the form of:

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

4.1.4 NRF FQDN and URI

Mobile operators shall follow home NF Repository Function (NRF) FQDN naming as specified in 3GPP TS 23.003 Section 28.3.2.3.2, in the form of:

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

vNRF should construct API URIs of the hNRF according to 3GPP TS23.003 Section 28.3.2.3.3, in the form of:

"https://nrf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org/"

If ‘3gpp-Sbi-Target-apiRoot’ header is supported, the above URI should be set in this header, and https scheme can be used to indicate the use of TLS.

4.1.5 SEPP Administration, Naming Conventions and Routing

A SEPP, or SEPP cluster will be identified by an FQDN, and corresponding IP-address obtained via SRV and (A or AAAA) procedures.

The FQDN defined by 3GPP shall be presented as (depicted as left FQDN hierarchy in the figure below):

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

Additionally, the following domain suffixes (defined in GSMA PRD IR.67 [8]) are proposed to support the different GSMA models which are described in detail in Section 4.3:

- mnc<MNC>.mcc<MCC>.3gppnetwork.org (strictly limited to a particular MNO) or group-<text>.3gppnetwork.org (strictly limited to group of MNO)

- mnc<MNC>.mcc<MCC>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org (for non-MNO participants acting under a mandate of a particular MNO)
- < UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org (for non-MNO participants acting outside a mandate of a particular MNO)

<SEPP-ID> is as specified in Section 13.2.2.4.2 of 3GPP TS 33.501 [19].

UNIQUE-IPX-PROVIDER-ID can be any valid alphanumeric host ID that can be put into a Fully Qualified Domain Name (FQDN). It must be unique across all IPX providers worldwide.

The well-known FQDN sepp.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org shall not be used for naming a SEPP. Instead it should be used for SEPP topology discovery procedures as outlined in GSMA PRD IR.67 [8].

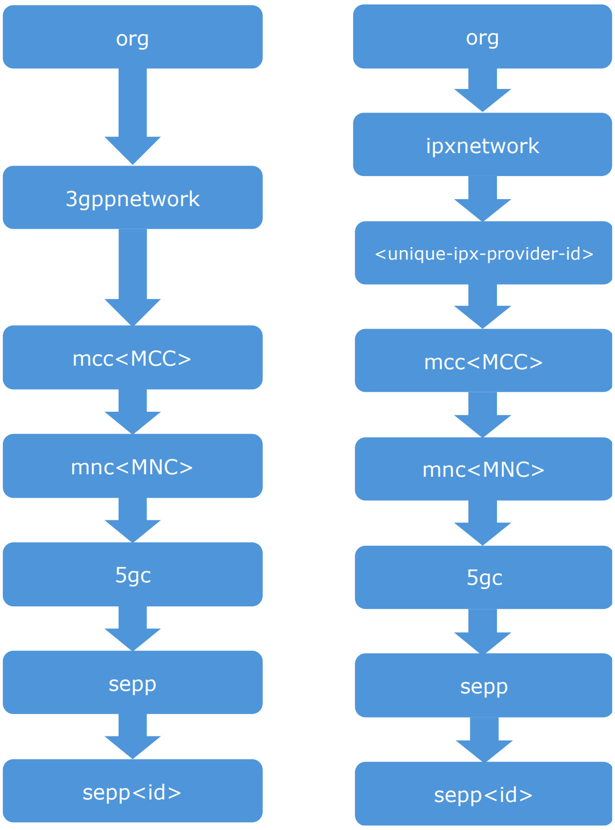


Figure 13 – FQDN hierarchy for MNO (left) and FQDN hierarchy for non-MNO (right)

The N32-c handshake procedure as in 3GPP TS 33.501 [19] contains a mTLS handshake. In order for TLS server (rSEPP) to always return the correct public key certificate to the TLS client (iSEPP) the TLS client shall always include the (non-well-known) SEPP server FQDN in the TLS Server Name Indication (SNI) parameter. For the avoidance of doubt, the SNI shall not contain the well-known SEPP FQDN.

GSMA PRD IR.21 [56] will specify the IP subnets where the to be discovered SEPPs will fall in. This makes sure that IP connectivity can be set-up between MNO SEPPs without additional IP firewall modifications.

GSMA PRD FS.34 [37] has more details on how PMN ID are tied to public key certificates. N32-f traffic from a peer MNO shall only be accepted where the PMN IDs are mentioned in the public key certificate. Traffic for other PMN IDs shall be rejected.

N32-f shall always terminate at the same responding SEPP as the corresponding N32-c. If the security mechanism is PRINS, the initiating-SEPP shall ensure this by using the FQDN of the responding SEPP in subsequent N32-f requests' apiRoot. This also applies to cases where the initially contacted SEPP redirects to another SEPP.

4.1.6 Fundamentals on IP layer

Security requires a comprehensive approach. There is the need for all PMN 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 PMNs;
- 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, PMN 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 PMNs 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 PMN operators and IPX Providers.

4.1.7 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 PMN SEPPs. Operators provision SEPPs with a Protection Policy based on bilateral agreements. Protection policies are exchanged via N32-c, which is protected by TLS.

The PMN SEPPs allow secure communication between service-consuming and service-producing NFs in different PMNs. The PMN SEPPs are located at the perimeter of each network and negotiate via N32-c interface

- the security mechanism for N32-f end-to-end protection (TLS or PRINS) and
- if PRINS has been selected,
  - the protection policies ensuring integrity and confidentiality protection for those elements to be protected and
  - the modification policies defining, which parts are allowed to be modified by one or two Roaming Intermediaries located on the N32 path between the two PMN SEPPs

before exchanging HTTP service messages via N32-f.

The functionality of a SEPP includes also message filtering and policing on Inter-PLMN control plane interfaces as well as topology hiding.

The PMN SEPP can provide Application Layer Security by PRINS (PRotocol for N32 INterconnect Security) on all HTTP messages before they are sent externally over the roaming interface (see clause 4.1.8.1).

The PMN 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.

Following 3GPP, PRINS allows Roaming Intermediaries to modify information elements received from the PMN SEPP in a controlled, attributable way.

4.1.8 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 8 the 5G roaming filter and control actions especially refer to application layer security by PRINS (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.

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 an “Allow 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:

a) GSMA PRD FS.17 [33] with detailed guidelines for both the HTTP/2 security aspects and the JSON security aspects

b) GSMA PRD FS.21 [36] with proposed sets of RFI/RFQ requirements for the 5GS functional elements and the related implementation and testing aspects.

4.1.8.1 PRINS application layer security (ALS)

PRINS, the ALS Protocol for N32 Interconnect Security, provides the following protection functionalities:

- The link protection between hops by TLS as pre-requisite for PRINS.
- Message protection of the information exchanged between NF service consumer and NF service producer by ALS.
- Attributability of any changes or insertions made on the path when forwarding the application layer protected message from the SEPP in one PMN to the SEPP in another PMN by way of using Roaming Intermediary service providers on the path.
- The Roaming Intermediary service 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 the SEPP of another PMN via a Roaming Intermediary, the HTTP/2 connection from a SEPP terminates at this next hop.

N32-f makes use of the HTTP/2 connection management requirements specified in 3GPP TS 29.500 [20]. If using ALS, additional transport confidentiality and integrity protection shall apply to the entire JOSE protected message between the hops by using either IPSec (NDS/IP) or TLS VPN between SEPP and Roaming Intermediary as well as between Roaming Intermediaries

N32-f in PRINS shall use “http” connections generated by a SEPP, but not “https” between the two PMNs’ SEPPs to allow for Roaming Intermediaries to read, modify or insert details on parts of the message that the operator has not encrypted.

NOTE: The HTTP/2 messages of the communication between the NF service consumer and the NF service producer are protected on the links and selectively protected against Roaming Intermediaries as negotiated during N32-c between the two SEPPs as per PMNs security policies.

4.1.8.2 HTTP/2 Security

The SEPP can support 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 clause 13.1 of 3GPP TS 33.501 [19].

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 PMN. The details of how SEPPs uses the telescopic FQDN to establish a TLS connection between a NF and the SEPP is defined in clause 13.1 of 3GPP TS 33.501 [19], clause C2.2 of 3GPP TS 29.573 [10], and clause 3.8.1 of GSMA PRD FS.21 [36].

If using PRINS, and 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 two IPX providers. If using PRINS, the IPX nodes in these IPX providers may modify messages according to the modification policy and create 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 clause 3.8.1 of GSMA PRD FS.21 [36], and clause 3.4.1 of GSMA PRD FS.36 [41].

4.1.8.3 JSON Security

If using PRINS, 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

4.1.8.4 API Security

With the service-based architecture defined in 5G, 3GPP network function (NF) applications interact with each other via Application Programming Interfaces (APIs). To secure any communication between NFs authentication, encryption, and authorization is needed.

Since APIs become a primary target for attackers in 5G, operators shall regularly test APIs to identify potential vulnerabilities.

4.1.8.4.1 Authentication

Mutual authentication of NFs is the pre-requisite for any interaction via APIs. TLS or NDS IP allows for authentication and also fulfils confidentiality requirements by applying encryption.

4.1.8.4.2 Certificates

Key and certificate management provides the necessary infrastructure.

4.1.8.4.3 Authorisation

For a NF to consume a service from another NF requires authorisation. It is recommended that both VPMN and HPMN use either static authorisation or authorisation using OAuth2 access token.

NOTE: Authorisation is not possible in case the HPMN only uses authorisation using OAuth2 access token and the VPMN only uses static authorisation.

If using OAuth2 access token authorisation, both VPMN and HPMN shall include oauth2Required IE as specified in 3GPP Release 16 TS 29.510 [16].

If the HPMN wants to use authorisation using Oauth2 only for some VPMNs then HPMN must support perPlmnOauth2ReqList IE as specified in 3GPP Release 17 TS 29.510 [16].

4.1.8.5 Security checks

This section outlines the protocols (IP, TLS, N32-c, N32-f) and parameters used for various security checks. The guiding principles can be found in FS.36 [41]. Basic roaming security controls are defined in IR.77 [32]. Some of the controls explained here are included in the call flows of the detailed designs in Annex B through Annex E.

4.1.8.5.1 Restricting IP connectivity

The first level of security is implemented at the IP protocol layer. SEPP IP addresses or ranges are defined in GSMA PRD IR.21 [56], Section A.16 - GRX/IPX Routing for Data Roaming.

The initiating SEPP IP address may be verified by the receiving party using IP firewalls or through SEPP configuration settings.

4.1.8.5.2 TLS trust anchoring

The TLS protocol is used by N32 (N32-c and N32-f), as well as N32s and N32p.

The TLS leaf certificate must be validated against a specific trust anchor.

Root CA certificates are exchanged between partners via the RAEX tool for certificates, managed by the GSMA. The correct trust anchor is identified based on PLMN-ID (for N32-c) or FQDN (for N32s and N32p), and the correct Root CA certificate in the trust anchor is identified using the issuer and subject fields. The details of trust anchor format can be found in GSMA PRD FS.34 [37] and 3GPP TS.33.501 [19].

4.1.8.5.3 PLMN-ID consistency checks

PLMN-IDs appear in several places in the roaming protocols. In order to address the attack surface with respect to impersonation or misrepresentation, consistency checks are specified for the various contexts, as follows.

4.1.8.5.3.1 N32-c checks (PLMN ID)

TLS trust anchor selection is based on the PLMN IDs in the TLS leaf certificate of the remote SEPP. Beyond this, it is recommended to validate the consistency of the PLMN IDs exchanged over N32-c against those in the TLS certificate and against those defined in GSMA PRD IR.21 [56], Section A.26 - 5G SA Roaming Information.

More specifically, if any PLMN IDs appear in the received N32-c PLMN ID Security Capability exchange that have not been included in the TLS leaf certificate, or are not declared in GSMA PRD IR.21 [56], appropriate actions should be taken, such as aborting the N32-c connection attempt.

All the PLMN IDs received during Security Capability exchange shall belong to the same organisation as declared in GSMA PRD IR.21 [56].

The PLMN ID check on N32-c can be performed using the following parameters:

- PLMNId list IE: Contains a list of PLMN IDs
- Sender IE: Extracts the PLMN ID from the SEPP FQDN

Note: the PLMN-IDs from the Security Capability Exchange are stored in the N32 context and are used as reference data for N32-f consistency checks.

4.1.8.5.3.2 N32-f checks (PLMN ID)

PLMN IDs exchanged on N32-f shall be compared to the PLMN IDs in the N32 context. In case of an inconsistency appropriate action shall be taken, e.g. rejecting the message that causes the mismatch.

Some N32-f messages, such as registration, include the originating network in the application layer. Others, like deregistration messages, do not. In such cases, the originating network is determined from other identifiers used and stored by NF consumers and producers.

For direct N32 connection, the originating network of an N32-f message can be identified by the receiving network's SEPP using a stateful correlation with the N32-c parameters that specify authorized PLMN IDs.

3GPP Release 17 TS 29.500 [40] introduces a new HTTP mandatory custom header (3gpp-Sbi-Originating-Network-Id) that enables originating network identification for N32-f messages:

- The header is sent by the NF, SCP, or SEPP (depending on operator configuration) in the originating network, when supported as per 3GPP Release 17 TS 29.500 [40].
- The SEPP in the receiving network can use this header (if available and supported) to identify or verify the originating network. The PLMN-ID(s) in that header shall also be checked for consistency with the PLMN-IDs in the N32 context.

Note: Detailed specifications of the 3gpp-Sbi-Originating-Network-Id header are found in Table 5.2.3.2.1-1 of Clause 5.2.3.2.1 and clause 5.2.3.2.15 of 3GPP Release 17 TS 29.500 [40].

4.1.8.5.3.3 N32s checks (PLMN ID)

In N32s no PLMN-IDs are included in TLS certificates of the RI, and no PLMN-IDs are exchanged over N32s-c for the RI. The TLS trust anchor is selected on the basis of the remote endpoint FQDN.

A local configuration at the N32s endpoint contains the list of PLMN-IDs of the roaming partners which this N32s connection is serving. No PLMN-ID may appear both in a N32 trust anchor and in a N32s local configuration, because each roaming relation is served either via N32 or via N32s, but not both. The local configuration information is used as reference data for N32s-f checks along the lines of N32-f as described earlier.

4.1.8.5.3.4 N32p checks (PLMN ID)

The N32p serves as a connection between two RIs that carries signalling for potentially multiple roaming relations. N32p endpoint shall have statically configured reference data indicating which roaming relations are open in which direction. Such reference data takes the form of an allow-list containing pairs of the form <PLMN-ID originating network, PLMN-ID destination network>. The pair <ABC originating network, XYZ destination network>, for example, indicates that the roaming relation with ABC being a PLMN-ID of the visited network and XYZ of the home network, is activated and allowed to be signalled over the N32p connection.

The exact details of the implementation of the reference data is not specified.

However, the N32p endpoint shall check N32p-f messages contain only PLMN-IDs that are consistent with the reference data, including direction (visited vs. home network). In case of mismatch the N32p-f message shall be dropped and a log entry shall be generated, according to RI policy.

4.1.8.5.4 N32-f checks (Category 0/1/2/3)

In 5G Standalone (SA) roaming, GSMA PRD FS.36 [41] (Section 3.5 and Annex A) defines message and signalling filtering on N32-f as a key mechanism to protect network elements, mitigate malicious attacks, and reduce unnecessary signalling traffic. These filters are categorized based on their purpose and criticality:

- Malformed Message Filtering

Filters out messages containing malformed data, repeated IEs, or missing IEs, making them non-compliant with schema.

- Category 1: Interface-Unauthorized Packet Filtering

  Checks whether a message is permitted on a given reference point. Typically based on operation type, and sometimes operation ID (for 5GC messages).

- Category 2: Home-Network Packet Filtering

  Validates that the message originates from the correct 'home' or allocated network of the subscriber. Detects inconsistencies between lower-layer and embedded packet/IE information.

- Category 3: Plausible-Network Packet Filtering

  Verifies that a message is sent from the network where the subscriber is currently located. Relies on inter-message correlation and plausibility analysis (e.g., location, velocity, and time).

4.1.9 Key Management for 5G Roaming Security

5G Inter-PLMN roaming security (as defined in 3GPP TS 33.501 [19]) requires cryptographic keys to achieve 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.

GSMA PRD FS.34 [37] describes the prerequisites for the certificate management, the caveats and the steps of the certificate management. It also provides background information on certificates, Certification Authorities (CA) and other related aspects.

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.

Further details are provided in GSMA PRD FS.34 [37] and shall be followed for 5G SA roaming.

By default, each MNOs should run its own roaming operations, deploy SEPPs and follow GSMA PRD FS.34 [37]. Depending on the service offering of the Roaming Intermediaries and on the agreements between MNOs and Roaming Intermediaries, some of the SEPP functionality may be operated by the Roaming Intermediaries on behalf of the MNO. In such a case, responsibilities move from the MNO to the Roaming Intermediaries who will then have to follow GSMAPRD FS.34 [37] on behalf of the MNO.

Certificate management needs to be done correctly and carefully to ensure that the certificates belong to the entity they claim they belong to and that the security controls are effective as GSMA PRD FS.34 [37] specifies.

4.1.10 Protection Policy Agreement and Exchange

Protection policies apply to the PRINS protocol. They consist of encryption policies and modification policies and are exchanged during N32-c negotiation phase.

The technical aspects of creating, handling, and exchanging can be found in 3GPP TS 29.573 [10].

GSMA also defines security profiles for protection policies. Please refer to Annex F.

NOTE: Keeping policies up-to date is essential for a successful negotiation between the two SEPPs.

4.2 GSMA Deployment Models

This section describes different 5G SA signalling deployment models and high-level security architectures proposed by GSMA.

Following 3GPP definition, the N32 endpoints are represented by SEPPs, i.e. the initiating and the responding SEPP. However, from a deployment perspective and in order to consider the need of all players in the 5G roaming eco-system, additional roaming solutions are envisioned by GSMA, e.g., a SEPP may be operated by a service provider inside or outside the MNO domain, or an operator group decides to use one group SEPP to handle all N32 connections towards the roaming partners of the operator group PMNs.

3GPP TS 33.501 [19] and TS 29.573 [10] define the technical details for e2e security compliant 5G service architecture solutions, i.e., TLS between the two PMN SEPPs, or PRINS if Roaming Intermediaries are on the path between the SEPPs).

This PRD provides detailed guidance on existing 3GPP solutions and documents those and other deployment solutions towards the 5G e2e service paradigm by introducing a hop-by-hop architecture without application layer security for the end-to-end secured exchange of control messages via N32.

The deployment models are described in 4.2.1 by use cases defining the business process and the actors involved in a technology-agnostic way.

Different security architectures can be applied to a deployment model and are described in 4.3 providing a high-level description of components and interfaces.

For the detailed design description for the different security architectures on how to build the components and used interfaces, including call flows, please refer to Annex B through Annex E.

NOTE: Only 5G SA signalling models are described into this Annex. Further work could be done to describe user plane if needed in the future.

4.2.1 Generic Deployment Models by Use Case/Actor Description

The basics of 5G SA roaming are defined in 3GPP, based on direct N32 connection between PMN SEPPs.

Four deployment models for 5G SA signalling are proposed by GSMA, allowing for different security architectures that are delivering various levels of security and different levels of delegation. These deployment models have been defined in order to serve particular business use cases within the mobile roaming ecosystem.

- Model 1 is the basic 3GPP direct bilateral roaming model between two PMNs.
- Model 2 is delegating the 5G SA SEPP deployment to Service Providers as a service option for one PMN or a Group of affiliated PMNs. Three model variants are defined:
  - Model 2.1 (Outsourced deployment model)
  - Model 2.2 (Hosted deployment model)
  - Model 2.3 (Operator Group model)
- Model 3 is delegating the 5G SA signalling management to Service Providers, acting as an 5G SA signalling aggregator (Service deployment model).
- Model 4 is delegating the 5G SA roaming management to Roaming Hubs.

NOTE 1: The model numbers have been assigned by GSMA.

NOTE 2: These deployment models are related to N32 interfaces level: IP connection is not part of these models and it is assumed that connectivity is provided by IPX IP transport services (see GSMA PRD IR.34 [5] for VLAN usage).

When a PMN decides to enable roaming with another PMN then it must choose one particular of the above models, and use this for selecting the appropriate contractual basis and for technically configuring its SEPP for the given roaming relation. It is not allowed and not supported for any pair of roaming partners to use multiple parallel roaming signalling routes that make use of different model combinations. That is, even if multiple such combinations would be available to the pair of roaming partners, they must select one for the signalling in the context of their particular roaming relation.

The GSMA models cannot be combined in all theoretically possible ways. For example, a partner using Model 1 cannot connect with a partner using Model 4. Instead, every pair of roaming partners must agree to a roaming signalling route that involves a combination of models that is interoperable.

The table below depicts the model combinations which are expected to be most useful in practice, namely those indicated with an “OK”.

Roaming partners	Model 1	Model 2.X	Model 3	Model 4
Model 1	OK	OK	N/A	N/A
Model 2.X	OK	OK	Out of scope (B)	Out of scope (B)
Model 3	N/A	Out of scope (B)	OK	Out of scope (A)
Model 4	N/A	Out of scope (B)	Out of scope (A)	OK

The combinations marked as “N/A” cannot interoperate due to technical limitations, in particular due to the fact that security mechanisms prevent the presence of certain types of active intermediaries on the path. The combinations marked with “Out of scope” could technically interoperate but are excluded due to market considerations, i.e. because no market demand is expected for such combinations. However, future versions of this document may include combinations that are currently out of scope if a need arises.

NOTE: More precisely, the combinations marked as “Out of scope (A)” are excluded because, historically (i.e. in pre-5G networks), there exist no contracts between signalling aggregators (service hubs) and roaming hubs and this is not expected to change. The combinations marked as “Out of scope (B)”, on the other hand, carry no history as they theoretically arise in the context of 5G protocols.

Services on the signalling path shall adhere to the 3GPP specifications for the messages addressed to NFs. This is necessary to avoid impact on the network functions and downstream services (e.g. analytics) of the roaming partner PMN.

For the deployment models, different business use cases to interconnect VPMN and HPMN for 5G SA roaming are described. Use case refers to the business process and the actors involved in a technology-agnostic way.

There are two generic use cases:

- bilateral contractual roaming agreement between the two roaming partners involving certain types of roaming intermediaries.
- contractual roaming agreements via Roaming Hubs.

Different types of roaming intermediaries (IPX Service Hub, Roaming Hub) require specific contractual agreements per actor.

NOTE 3: Business contracts are defined in GSMA PRD WA.51 [67].

4.2.2 Direct bilateral scenario with PMN internal SEPPs (Model 1)

This use case refers to a direct bilateral deployment model between a VPMN and a HPMN, which is depicted in Figure 14, whereby both the VPMN and HPMN have their own internal SEPP (not depicted) deployed within the PMN. The interconnection typically utilizes an IPX transport network.

The two SEPPs are connected based on a direct roaming agreement with the required technical information exchanged through GSMA RAEX IR.21 [56].

Both PMNs may have a single PMN ID or own multiple PMN IDs. In case of multiple PMN IDs, the same N32 is used as specified in clause 5.9.3.2 of 3GPP TS 33.501 [19].

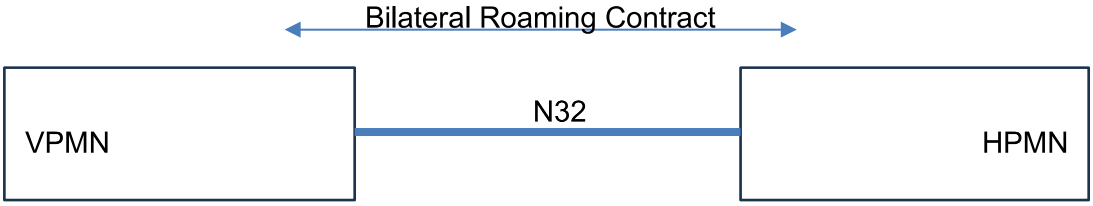


Figure 14 - Direct bilateral scenario with PMN SEPPs

4.2.3 Outsourced/Hosted SEPPs (Model 2.1/2.2)

These two deployment models apply to the use cases where the PMN has decided to delegate the SEPP management, i.e. a service provider provides a SEPP function on behalf of a PMN. Either one or both of VPMN and HPMN can make use of this model. The figures below depict the two use cases, where SEPP is provided by a Service Provider, based on an Outsourced SEPP (Model 2.1- Figure 15) or Hosted SEPP (Model 2.2 - Figure 16).

Both deployment models connect Outsourced/Hosted SEPP and roaming partner PMN (which can also have an Outsourced/Hosted SEPP) based on a direct roaming agreement with the required technical information exchanged through GSMA RAEX IR.21 [56].

The Outsourced SEPP in model 2.1 is deployed in the PMN security domain, while the Hosted SEPP in model 2.2 is deployed in the Service Provider domain.

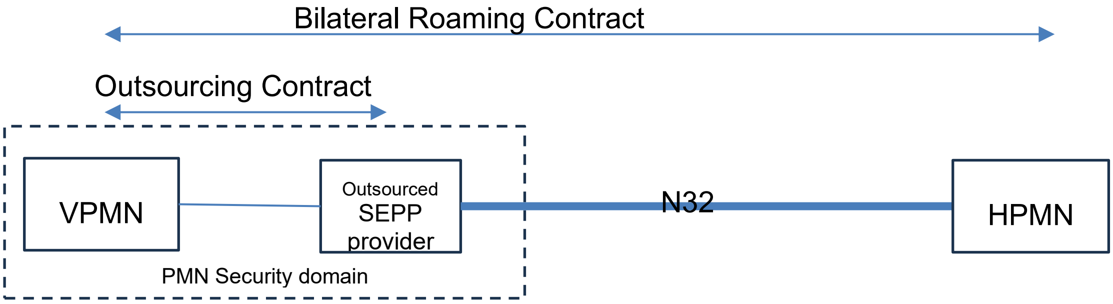


Figure 15 - Bilateral scenario with Outsourced SEPP provider

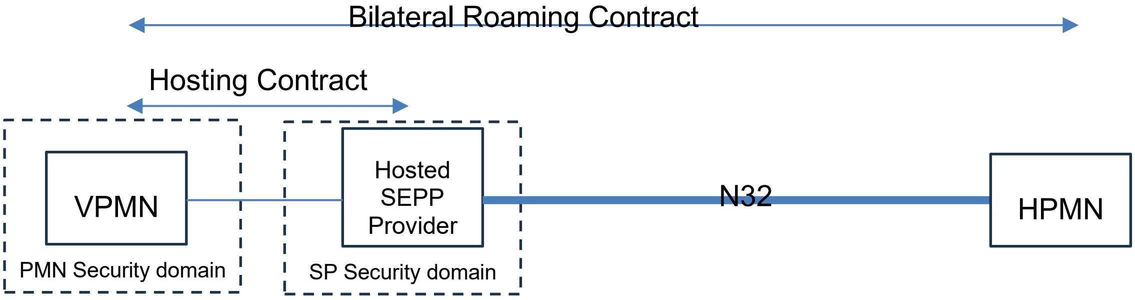


Figure 16 - Bilateral scenario with Hosted SEPP providers

4.2.4 Mobile Operator Group with a group SEPP (Model 2.3)

This use case refers to the deployment model of a central SEPP (group SEPP) for an operator grouping various operator PMNs. This group SEPP function is the single-entry point to the Operator Group arrangement with internal local Mobile OpCos (A1, A2 with B in the example below).

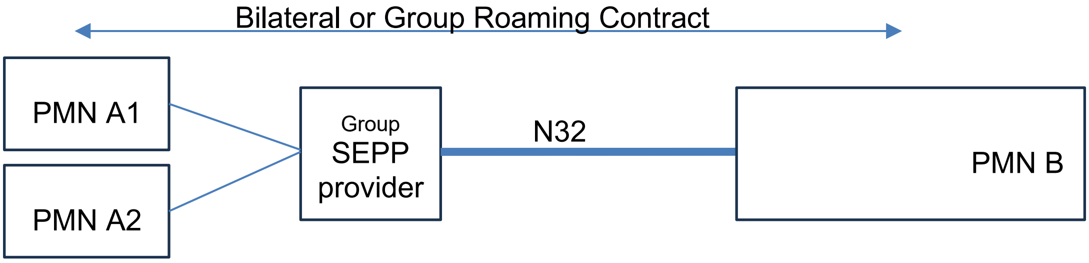


Figure 17 - Bilateral scenario between Mobile Operator Groups

In this scenario, the Group SEPP is acting on behalf of the individual affiliates (A1, A2, …) with bilateral agreement or a group bilateral arrangement to another PMN B. The required technical information is exchanged through GSMA RAEX IR.21 [56].

Each OpCo (A1, A2, …) is connected to the Group SEPP either using Model 2.1 or Model 2.2. A mixture of these two models among OpCos is possible. The Group SEPP represents all connected OpCos of the Operator Group and represents their PMN IDs. The same N32 can be used as specified in clause 5.9.3.2 of 3GPP TS 33.501 [19] for the entire Operator Group, having its endpoint at the Group SEPP.

4.2.5 Service Hub (Model 3)

This use case refers to roaming intermediate signalling actors (Service Hub provider) to connect PMNs, based on a bilateral roaming agreement between PMNs. The PMN A1 or A2 (using Service Hub A) have bilateral roaming agreements with PMN B1 or B2 (using Service Hub B). It is also possible that PMN A1 and A2 have a bilateral roaming agreement; in this case only Service Hub A is used.

A Service Hub manages the 5G SA signalling of several PMNs, member of the Service Hub (e.g., in Figure 18, Service Hub A manages the signalling of PMN A1 and PMN A2), so it is a multilateral interconnection. The Service Hub enables a PMN to delegate the 5G SA roaming signalling management to a Service Provider.

A Service Hub could provide several Roaming Value Added Services (not further detailed in this document).

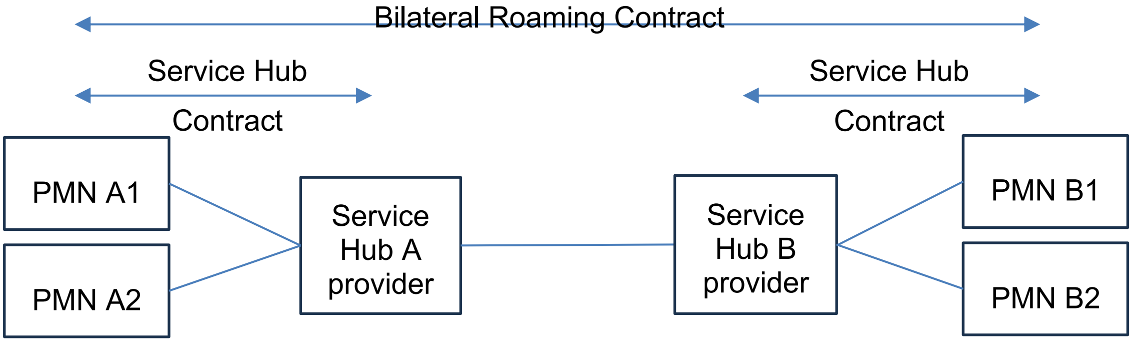


Figure 18 - Bilateral scenario using Service Hub

For this use case, different architectures are described in Section 4.3.3 and Section 4.3.4, respectively.

The Service Hub aggregates signalling traffic of multiple PMNs.

4.2.6 Roaming Hub (Model 4)

This use case refers to intermediate global actors (Roaming Hub provider) to connect PMNs, based on a roaming hub contract. The PMN A1 or A2 have roaming hub agreements with Roaming Hub A; in case of roaming between A1 and A2, only Roaming Hub A is used. The PMN B1 or B2 have roaming hub agreements with Roaming Hub B. The PMN A1 or A2 have no bilateral roaming agreements with PMN B1 or B2.

A Roaming Hub aggregates the 5G SA signalling of several PMNs, member of the Roaming Hub, enabling a PMN to outsource the 5G SA roaming signalling management.

In addition, the Roaming Hub manages additional aspects like roaming contract, billing, testing.

It is important to keep in mind that not all theoretically possible roaming relations are commercially and technically opened at any given point in time. Instead, PMNs indicate to their Roaming Hub which relations they wish to open, and which they wish to remain closed. The two Roaming Hubs in a chain need to continuously coordinate between themselves in order to maintain a consistent understanding of which relations to keep open.

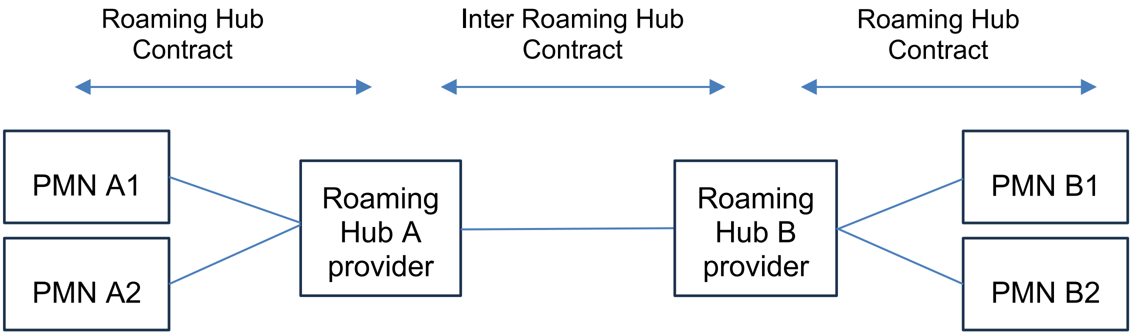


Figure 19 - Roaming Hub scenario

For this use case, different security architectures are described in Section 4.3.3 and Section 4.3.4, respectively.

The Roaming Hub aggregates signalling traffic of multiple PMNs. The required technical information is exchanged through GSMA Hubbing provider data IR.85 [57].

4.3 GSMA High Level Security Architecture

The following table lists options of security mechanisms defined in this PRD for the different deployment models to forward the HTTP/2 messages processed by a PMN SEPP either hop-by-hop secured (Model 3/4) or end-to-end secured (Model 1 and Model 3/4 based on PRINS) to another PMN, as well as for the SEPP delegation (Model 2) by one MNO.

NOTE: Different types of SEPPs are introduced in this PRD.

Model	Security mechanism (NOTE 0,1)
Model 1 – Direct Bilateral	TLS
Model 2.1 – Outsourced SEPP	TLS
Model 2.2 – Hosted SEPP	TLS
Model 2.3 - Operator Group	TLS
Model 3 – Service Hub architecture	Hop-by-hop TLS or PRINS
Model 4 – Roaming Hub architecture	Hop-by-hop TLS or PRINS

Table 4 Model and Security mechanisms

NOTE 0: This is a simplified table and lists supported security mechanisms between different actors. In Model 1, 3 and 4 the listed security mechanism is applied for communication between PMNs. In Model 2, the listed security mechanism is used between the PMN and its service provider or group operator, which is operating the Outsourced SEPP, Hosted SEPP or Group SEPP.

NOTE 1: Model 3 and 4 present similar architectures. Different security architectures are possible for these hubbing architectures. A combined description for model 3 and 4 is provided per security architecture, i.e. using the respective security mechanism:

- Section 4.3.3 for application layer security (ALS) with PRINS end-to-end security approach (on top of Hop-by-Hop TLS link protection)

- Section 4.3.4 for Link protection in a Hop-by-Hop security approach

NOTE 2: The option described in Section 4.3.4 of selecting TLS as a hop-by-hop security method without ALS in model 3 and 4 is not specified by 3GPP, and instead introduced in this document.

To meet the security requirements of their roaming partners, operators must support a bilateral TLS deployment model (Models 1 or 2) upon request.

4.3.1 Direct bilateral with end-to-end protection (applicable to Model 1)

This architecture is compliant with 3GPP specifications; see 3GPP TS 33.501 [19] (clause 5.9.3.2) and 3GPP TS 29.573 [10].

In the direct bilateral model, PMN SEPPs are interconnected using 3GPP N32 (with TLS as the selected security mechanism for N32-f).

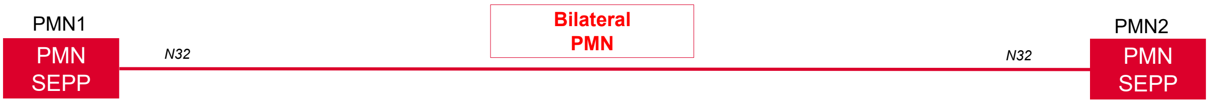


Figure 20 - Direct bilateral end-to-end TLS architecture

4.3.1.1 PMN SEPP

A PMN SEPP is a non-transparent proxy, identified by a PMN SEPP FQDN, supporting the following functionality:

- Routing of signalling to the appropriate N32 interface based on roaming partner identification
- Exchange of control messages directly with the peer SEPP over N32-c and exchange of NF API messages over N32-f interface
- PMN protection (message filtering and policing)
- Performing mutual authentication and data protection based on mTLS on N32 interfaces

When connecting to the roaming partner, a PMN SEPP can only connect to the roaming partner SEPP that deploys Direct Bilateral (model 1) or Outsourced/Hosted/Group SEPP (model 2). It cannot be used in combination with Service Hub (model 3) and Roaming Hub (model 4).

4.3.1.2 N32 interfaces

The N32 interface is used between the two PMN SEPPs:

- N32 is the 3GPP interface, used to connect two PMN SEPPs
- Roaming partners use well-known PMN FQDN to discover the SEPP of the roaming partner
- TLS based, TLS certificates using PMN SEPP FQDN
- One N32 interface per roaming partner
- Transports negotiation messages for the security method selection (i.e. TLS) and used to reset N32 (N32-c)
- Transports control messages (N32-f) for exchanging service messages between the two roaming partner PMNs' SEPPs

4.3.1.3 SEPP domain names

A PMN SEPP is identified by an FQDN, and a corresponding IP-address is obtained via DNS procedures as defined in GSMA PRD IR.67 [8].

The table below defines the SEPP FQDN:

SEPP	SEPP FQDN
PMN SEPP	<SEPP-ID>.sepp.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The well-known FQDN is used for SEPP topology discovery procedures as defined in GSMA PRD IR.67 [8].

SEPP	well-known FQDN
PMN SEPP	sepp.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

4.3.2 Outsourcing and Hosting architecture (applicable to Model 2)

4.3.2.1 Outsourcing architecture (applicable to Model 2.1)

This outsourcing architecture is not specified in 3GPP. It is a deployment model for a SEPP at one MNO.

Outsourced SEPP is equivalent to PMN SEPP (model 1) in that it is connected to PMN NFs via SBI, but SEPP management is delegated to a Service Provider.

Sections 4.3.1.1 through 4.3.1.3 apply equally.

The only difference to model 1 is that the Outsourced SEPP is operated by another entity on behalf of the MNO.

4.3.2.2 Hosting architecture (applicable to Model 2.2)

This hosting architecture is not specified in 3GPP. It is a deployment model for a SEPP at one MNO.

The Hosted SEPP model has different components:

- A PMN SEPP* is a non-transparent proxy, placed at the border of the PMN, able to connect to the Service Provider (Hosted SEPP), using the N32s interface.
- A Hosted SEPP provider, consists of 2 SEPP functions (messages are forwarded between the two SEPP functions):
    a) HS (Hosted SEPP) SEPP function, acting as a PMN SEPP for all roaming partners connected via the Hosted SEPP provider.
    b) SP (Service Provider) SEPP function, connected to PMN SEPP* using the N32s interface.

In the Hosted SEPP model, the PMN SEPP* is interconnected to an SP SEPP in the Hosted SEPP provider using N32s. SP SEPP is interfacing in an undefined manner the HS SEPP in the Hosted SEPP provider (acting as PMN SEPP). HS SEPP is connected to a roaming partner's SEPP using N32.

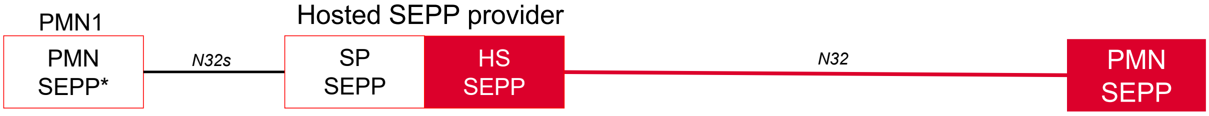


Figure 21 - Hosting architecture

4.3.2.2.1 PMN SEPP*

A PMN SEPP* is a non-transparent proxy, identified by a PMN SEPP* FQDN, connected to a Service Provider (SP) SEPP, supporting the following functionality:

- Exchange of signalling with Service Provider (SP) SEPP, using N32s interface based on SP SEPP FQDN
- PMN protection (message filtering and policing)
- Performing mutual authentication and data protection based on mTLS with the SP SEPP

4.3.2.2.2 SP SEPP

SP SEPP (function of Hosted SEPP provider) is dedicated per PMN and characterized by:

- Located within the domain of the service provider and identified by an SP SEPP FQDN
- Used to exchange signalling directly with client PMN SEPP*, using N32s interface based on PMN SEPP* FQDN
- Used to perform mutual authentication and data protection based on mTLS with the PMN SEPP*

4.3.2.2.3 HS SEPP

HS SEPP (function of Hosted SEPP provider, dedicated per PMN and connected to roaming partners PMN SEPP), characterised by:

- Equivalent to a PMN SEPP: A HS SEPP is a non-transparent proxy, playing the role of an PMN SEPP, enabling a PMN to outsource the 5G SA roaming signalling management to a Hosted SEPP Provider
- Located within the domain of the service provider and identified by a HS SEPP FQDN
- Used for Routing of the signalling to the appropriate N32 interface based on roaming partner identification
- Used to exchange signalling directly with other PMN or other HS SEPP, using N32 interface based on well-known SEPP FQDN
- Used for PMN / SP protection (message filtering and policing)
- Used to perform mutual authentication and data protection based on mTLS with roaming partner SEPP (PMN SEPP or other HS SEPP)

When connecting to the roaming partner, a HS SEPP can only connect to the roaming partner SEPP that deploys Direct Bilateral (model 1) or Outsourced/Hosted/Group SEPP (model 2). It cannot be used in combination with Service Hub (model 3) and Roaming Hub (model 4).

4.3.2.2.4 N32 interfaces

The following interfaces are used between the different SEPP components:

An N32 between HS SEPP and other PMN SEPP is 3GPP compliant N32 interface (same as in direct bilateral model 1)

An N32s is derived from 3GPP N32 with the following characteristics:

- Used to connect a PMN SEPP* to SP SEPP
- SP SEPP uses PMN SEPP* FQDN to discover the PMN SEPP* and PMN SEPP* uses the SP FQDN to discover the SP SEPP
- Uses TLS (TLS certificates using PMN SEPP* FQDN or SP SEPP)
- Uses one N32s connection for all the N32 PMN roaming routes outsourced and to be initiated by the Service Provider

4.3.2.2.5 Dedicated SEPP domain names

A SEPP is identified by an FQDN, and the corresponding IP-address is obtained via DNS procedures as defined in GSMA PRD IR.67 [8].

The table below defines dedicated SEPP FQDNs:

SEPP	SEPP FQDN
PMN SEPP*	<SEPP-ID>.sepp.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org or PMN specific
HS SEPP	<SEPP-ID>.sepp.5gc.mnc<MNC>.mcc<MCC>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org
SP SEPP	<SEPP-ID>.sepp.5gc.<CLIENT-ID>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org

Table 5 Dedicated SEPP FQDNs Definition

NOTE 1: CLIENT-ID is used to enable dedicated SP SEPP instances per hosted SEPP provider customer.

NOTE 2: MCC/MNC of the HS SEPP is the same as the PMN SEPP*.

Well-known FQDN is used for SEPP topology discovery procedures as defined in GSMA PRD IR.67 [8].

The table below defines the well-known FQDN to discover different types of SEPPs:

SEPP	well-known FQDN
HS SEPP	sepp.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

4.3.2.3 Mobile operator Group architecture (applicable to Model 2.3)

This architecture is based on 3GPP specifications TS 33.501 [19] (clause 13.1.2), compliant with the End-to-End Security principle from the Group SEPP (all PMNs within the mobile operator group are in the same security domain) to another PMN SEPP.

Figure 22 describes the Group SEPP which represents all the affiliates of the Group.

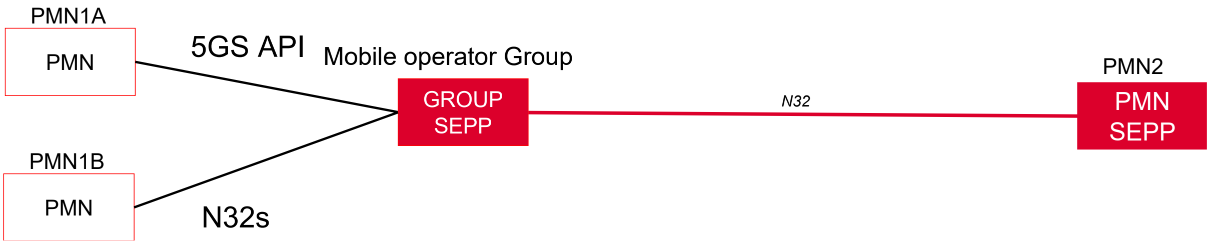


Figure 22- Operator Group architecture

4.3.2.3.1 Group SEPP

Group SEPP is a shared SEPP for all the PMNs of the group, characterised by:

- All the PMN IDs of the group are defined on the same Group SEPP (N32 and associated TLS certificates)
- For connecting the PMNs of the Operator Group to the Group SEPP, the technical architecture of Outsourced SEPP (model 2.1 -5GS API), or Hosted SEPP (model 2.2-N32s) can be used.
- Each roaming partner is connected via a common N32 connection in order to reach any affiliate of the group

Group SEPP could connect to affiliate PMN using one of the following interfaces:

- 5GS API: direct connection to PMN SCP or NF, reusing the same design as a PMN SEPP defined in annex B.
- N32s: connection to PMN SEPP* of a group affiliate; N32s was defined initially in the Hosted SEPP architecture and is described in Section 4.3.2.2.4 and Annex C. Annex G contains specific design aspects related to Group SEPP.

When connecting to the roaming partner, a Group SEPP can only connect to the roaming partner SEPP that deploys Direct Bilateral (model 1) or Outsourced/Hosted/Group SEPP (model 2). It cannot be used in combination with Service Hub (model 3) and Roaming Hub (model 4).

4.3.2.3.2 N32 interfaces

The following interfaces are used between the different SEPP components:

A N32 is 3GPP N32 with the following characteristics:

- Used to connect to other PMN using model 1 or model 2
- PMN List and leaf TLS certificate contain all the PMN IDs of the group affiliates

4.3.2.3.3 Dedicated SEPP domain names

A SEPP is identified by an FQDN, and the corresponding IP-address is obtained via DNS procedures as defined in GSMA PRD IR.67 [8].

The table below defines the dedicated SEPP FQDN to the roaming partner:

SEPP	SEPP FQDN
Group SEPP	Group SEPP could reuse different models, where Group SEPP is identified by the group-<text> identifier, representing all the operators of the Group. <SEPP-ID>.sepp.5gc.group-<text>.3gppnetwork.org (direct bilateral SEPP – model 1 or Outsourced SEPP - model 2.1.b) <SEPP-ID>.sepp.5gc.group-<text>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org (Hosted SEPP - model 2.2)

NOTE: The FQDN differs depending on whether the Group SEPP is managed within the PMN security domain or in a service provider security domain.

<text> shall be 2-10 characters following the DNS rule scheme.

group-<text> indicates that the FQDN represents a network element that belongs to an Operator Group.

Examples for valid SEPP FQDNs are as follows. For the sake of these examples, the imaginary <text> “EuropeNet” and IPX Provider “newIPX” are introduced.

sepp1.sepp.5gc.group-europenet.3gppnetwork.org

sepp7.sepp.5gc.group-europenet.newIPX.ipxnetwork.org

Well-known FQDN is used for SEPP topology discovery procedures as defined in GSMA PRD IR.67 [8].

The table below defines the well-known FQDN to discover the Group SEPP:

SEPP	well-known FQDN
Group SEPP	sepp.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

NOTE: All PMN IDs (MCC/MNC) of the group members are pointing to the Group SEPP FQDN

4.3.3 Hubbing architecture with end-to-end security based on application layer security (applicable to Model 3/4)

The end-to-end protected hubbing architecture is as specified by 3GPP TS 33.501 [19].

This architecture providing application layer security (PRINS) is a deployment model with Roaming Intermediaries keeping the control to the operator. It provides TLS security protection between the hops and protects signalling messages end-to-end at application layer by providing attributability of any modifications on the path. It further allows roaming intermediaries to intervene by creating own messages.

Note: Roaming Intermediary (RI) (defined in 3GPP 33.501 [19]) is an entity that provides roaming related services. IPX providers and roaming hubs are types of roaming intermediaries. RI will be used in the next part of the description.

This section explains the role of the following actors using PRINS architecture:

- PMN SEPP
- Roaming Intermediary (RI): Providing IPX services (SH or RH service provider) aggregating the 5G SA signalling of several PMNs and routing the signalling messages to the other PMN SEPP.

A Roaming Intermediary (RI) service provider consists of two parts:

- RI HTTP proxy: relaying HTTP messages on N32-c (HTTP CONNECT), being able to add patches to N32-f received ALS protected messages and to sign the modified message (patch) before forwarding
- Hub application: either service hub application or roaming hub application

The functional split between RI HTTP Proxy and the Hub application is implementation specific.

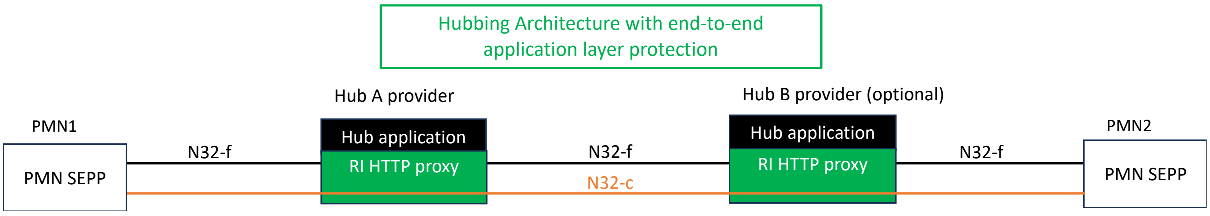


Figure 23 - Hubbing architecture (end-to-end ALS protection)

4.3.3.1 PMN SEPP

A PMN SEPP is a non-transparent proxy, identified by a PMN SEPP FQDN, supporting the following functionality:

- Setting up an end-to-end TLS connection (N32-c)
- Optionally, exchange of signalling with the RI HTTP Proxy using HTTP connect to prepare setting up an end-to-end TLS connection (N32-c) between PMN SEPPs via roaming intermediaries.

NOTE 1: The usage of HTTP connect is a well-known method and specified in Release 18 to accommodate roaming intermediaries to be informed of the setup of the end-to-end TLS connection for N32-c. There are no technical limitations to support this method also in earlier 5G 3GPP releases.

- Performs mutual authentication and signalling protection based on mTLS with the other PMN SEPP during the initial N32-c end-to-end handshake and negotiation phase making use of the certificates in the RAEX database, i.e.
    - Initiates the security capability exchange (N32-c) with the other PMN SEPP indicating PRINS.

  - Exchanges in N32-c the details of N32-f protection and modification policies either in detail or by providing a security profile identifier.

- Establishing TLS for mutual authentication and link protection to the next hop in preparation for end-to-end ALS

- Using N32-f to transport N32-f ALS protected signalling messages in line with the negotiated protection and modification policies including signature to provide attributability and to route the signalling of application layer protected messages to the next hop.

- Applies PMN protection (message filtering and policing)

4.3.3.2 Roaming Intermediary HTTP Proxy

NOTE: The functional split between RI HTTP Proxy and the Hub application is implementation specific.

The RI HTTP Proxy supports the following functionality:

- Establishing TLS for mutual authentication and link protection to the adjacent hop (PMN SEPP or RI).

- Used to exchange signalling between PMNs or an RI based on opening and closing of relations by the hub application.

- Provides the received signalling to the hub application.

- Processes N32-f/ALS protected signalling messages (JSON patches).

4.3.3.2.1 Hub application

NOTE: The functional split between Roaming Intermediary HTTP Proxy and the Hub application is implementation specific.

Hub application delivers the following functions:

- Controls 5G SA signalling for roaming routes commercially opened

- Provide support for other passive roaming services like probing (signalling traces) and business intelligence

4.3.3.3 N32 interfaces

The N32 interface as specified by 3GPP is used between the two PMN SEPPs

- Used to connect two PMN SEPPs with N32-c based on mTLS

- Used to connect two PMN SEPPs with N32-f/ALS based on mTLS between hops

- mTLS is used for link protection at transport layer

- ALS is used for end-to-end protection between the two PMN SEPPs at application layer (PRINS)

- Roaming partners use well-known PMN FQDN to discover the PMN SEPP of the roaming partner. TLS certificates with PMN SEPP FQDN are used.

- PMN SEPP uses the peer Hub FQDN to discover the RI HTTP proxy of the service provider hop

- Traffic aggregation over TLS for link protection is performed between an RI and one PMN SEPP or an RI and another RI

N32-c/HTTP connect is the standard HTTP method used to set-up a connection through the hops in preparation for end-to-end N32-c.

N32-c is specified by 3GPP to transport negotiation messages (N32-c) end-to-end between the two PMN SEPPs for the security method selection (i.e. PRINS), the exchange of protection and modification policies, and the tear down of N32.

N32-f is specified by 3GPP to transport signalling messages between the two PMN SEPPs protected by N32-f/ALS allowing hops to modify IEs with attributability.

4.3.3.4 SEPP domain names

Same as direct bilateral model (see Section 4.3.1) for PMN SEPPs.

Same as link protected hop-by-hop hubbing architecture (see Section 4.3.3) for RI service provider identification.

4.3.4 Hubbing architecture with transport layer link protection based on hop-by-hop security (applicable to Model 3/4)

The transport layer link protected hop-by-hop hubbing architecture is not specified by 3GPP.

It represents a deployment model for roaming intermediaries. It does not provide end-to-end security between PMNs. Instead, it merely provides TLS security between the different hops.

A Hub provider (service hub or roaming hub) aggregates the 5G SA signalling of several PMNs, members of the Hub, allowing each PMN to let the 5G SA roaming signalling management done by the Hub Provider. The Hub provider consists of two SEPP functions (SP SEPP and Hub SEPP) and one Hub application:

- Hub SEPP, connected to other Hub SEPP in a second hub provider to reach the roaming partners, using the N32p interface.

- Hub application, either service hub application or roaming hub application, processes and relays messages

- SP SEPP, connected to PMN SEPP* using N32s interface

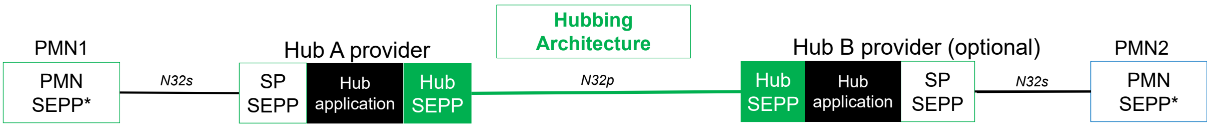


Figure 24 - Hubbing architecture (hop-by-hop transport layer link protection)

4.3.4.1 PMN SEPP*

A PMN SEPP* is a non-transparent proxy, identified by a PMN SEPP* FQDN, connected to a Service Provider (SP) SEPP (same as defined in the Hosted SEPP model).

4.3.4.2 SP SEPP

SP SEPP is similar to SP SEPP described in the Hosted SEPP architecture.

4.3.4.3 Hub SEPP

Hub SEPP (connects to another Hub SEPP) is characterized by:

- Located within the domain of the hub provider and identified by a Hub SEPP FQDN
- Routing of the signalling to the appropriate interface based on roaming partner identification
- Used to exchange signalling directly with the other Hub SEPP, using TLS N32p interface based on well-known Hub SEPP FQDN
- Provides Hub provider protection (message filtering and policing)
- Performs mutual authentication and data protection based on mTLS

A Hub SEPP can only connect to other Hub SEPPs of the same model. A Hub SEPP of a Service Hub (model 3) can only connect to a Hub SEPP of another Service Hub (model 3). A Hub SEPP of a Roaming Hub (model 4) can only connect to a Hub SEPP of another Roaming Hub (model 4). It cannot be used in combination with Direct Bilateral (model 1) or Outsourced/Hosted/Group SEPP (model 2).

NOTE: there is no Hub SEPP if only one Hub provider is involved. In this case, the signalling traffic is directly routed between the two SP SEPPs via the hub application.

4.3.4.4 Hub application

Hub application delivers the following functions:

- Relay 5G SA signalling from the SP SEPP to the Hub SEPP and vice versa for roaming routes commercially opened, and discard/reject 5G SA signalling for roaming routes commercially not opened
- Provide support for other passive roaming services like probing (signalling traces) and business intelligence

4.3.4.5 N32 interfaces

The following interfaces are used between the different SEPP components:

An N32s derived from 3GPP N32 with the following characteristics:

- Used to connect a PMN SEPP* to SP SEPP (see Hosted SEPP Section 4.3.2.2.3)

An N32p derived from 3GPP N32 with the following characteristics:

- Used to connect Hub SEPPs (inter-Hub cases)
- Hub SEPP uses the peer Hub FQDN to discover the peer Hub SEPP
- Uses TLS (TLS certificates using Hub SEPP FQDN)
- Uses one N32p interface for all the roaming partners of different Hubs

4.3.4.6 Dedicated SEPP domain names

A SEPP will be identified by an FQDN, and corresponding IP-address is obtained via DNS procedures as defined in GSMA PRD IR.67 [8].

The table below defines the SEPP FQDN:

SEPP	SEPP FQDN
SP SEPP	<TEXT>.<SEPP-ID>.sepp.5gc.hub.<CLIENT-Id>.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org (model 3 and 4) <TEXT> shall be SH, RH or HBM (combining SH and RH). HBM to be used to send all traffic and let the Service Hub (SH) provider, Roaming Hub (RH) provider separate it. MNO may insist to use separated two N32-s connections for the different types of traffics.
Hub SEPP	<TEXT>.<SEPP-ID>.sepp.5gc.hub.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org (model 3 and 4) <TEXT> shall be SH or RH HBM shall not be present in the peering side. Service Hub (SH) provider, Roaming Hub (RH) provider shall separate the traffic into different peering N32-p connections.

NOTE: CLIENT-ID is used to enable dedicated SP SEPP instances per Hub customer.

SEPP cluster FQDN is used for SEPP topology discovery procedures as outlined in GSMA PRD IR.67 [8]. This SEPP cluster FQDN needs to be distributed upfront. DNS procedures as defined in GSMA PRD IR.67 [8] begin with this SEPP cluster FQDN.

The table below defines the SEPP cluster FQDN to discover different SEPP:

SEPP	SEPP cluster FQDN
Hub SEPP	sepp.5gc.hub.<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org (model 3 and 4)

4.3.5 Security Considerations of the Different Roaming Deployments

The described high-level architectures assume different trust models. It is up to the roaming partners, which trust assumptions apply for their relationship. While this decision has to consider applicable regulation, the MNO should strive to achieve a consistent security level across all of its roaming relations.

The 5G trust model as specified by 3GPP keeps control at the two roaming partners of which information is visible and modifiable by roaming intermediaries, i.e. at the two PMN SEPPs that process service requests of the NFs of one PMN to consume services from the NFs of the roaming partner PMN. In addition, 3GPP included the deployment model of an Operator group roaming hub SEPP equivalent to a PMN SEPP which takes control on behalf of all its group members when in a roaming relation with a roaming partner outside of the group.

The deployment models Outsourced/Hosted SEPP as specified in this document allow the operator to delegate the initiation and control of the roaming relation to an entity within or outside the operator security domain.

For the Hubbing architecture, different security variants are foreseen:

- In the hop-by-hop deployment models, proposed in this PRD, all links are protected, but each hop has full access (read/modify/insert) to the operator’s data passing through without the roaming partner having the ability to attribute the message, i.e., to distinguish, whether the message received is the original message from its roaming partner. This has implications in terms of attributability, as the true source of a message or message part cannot be deduced from the message itself.

- The end-to-end secured deployment model with roaming intermediaries being allowed to selectively read/modify/insert, follows the 3GPP principles. Similar as in the hop-by-hop deployment model all links are protected. In addition, application layer security allows confidentiality of selected information elements and attributability of any changes (modify/insert) to the operator data passing through the roaming intermediaries. This solves the problem described in GSMA PRD FS.19, Section 3.2.1.

A more generic assessment of the described deployment models is provided in the next section.

4.3.6 Evaluation of the Different Roaming Security Architectures

For each roaming partner, one of the security architectures together with one of the deployment models described in this document must be chosen by the MNO. To facilitate an informed choice, this section presents a set of criteria that should be considered. Each architecture is evaluated along this set of criteria. Criteria are presented in no particular order.

By understanding the associated risks, the operator can take an informed decision on the security architecture and the need for additional means, if not achieved by technical security.

It is not implied that the criteria below ought to carry equal weights. Instead, depending on individual circumstances and on a per-roaming relation basis, different weights can and should be assigned by the operator. The assignment of such weights is currently outside the scope of this document.

Similarly, it is also not implied that the set of criteria is complete. Depending on individual circumstances, additional criteria may be used for the purposes of evaluation.

4.3.6.1 Attack Surface

Criterion Description

Since the roaming ecosystem operates within an adversarial environment, where attacks against operators, intermediaries, mobile subscribers and connected devices have been observed in the past, the protocols and mechanisms used in all architectures are built with security in mind. However, they provide different levels of security and therefore it is important to characterise the ways in which the mechanisms in each model address the attack surface.

The different levels of security arise because of differences in the way secure communication channels are setup between the entities in the described architectures, as well as differences in how integrity and confidentiality of signalling messages and their parts are provided. Depending on the MNO selected security architecture, roaming intermediaries and/or providers of outsourced/hosted/group SEPPs, have different degrees of access to SBI message content, including reading, writing/modifying and the ability to initiate signalling. These aspects are considered in the evaluation of this criterion.

Attacks may originate from different sources/actors. The following subset possibilities are considered. An adversary/attack source may be:

- an outsider trying to obtain access or interfere with the system by introducing unwanted signalling/traffic,
- a corrupted or compromised outsourced, hosted, or group SEPP provider,
- a corrupted or compromised Roaming Intermediary such as a Roaming Hub or an on-path Roaming Value Added Services (RVAS) provider (Service Hub), and/or
- a corrupted or compromised visited or home operator, e.g. by an insider.

Each of the above options represents some attack surface. A given architecture may address some attack surface thereby addressing the risks it represents. All attack surface that is not addressed is said to *remain* and the operator must take an informed decision to accept the associated risks or address them by other means.

It is worth noting that, in order to address some (but not all) of the remaining attack surface, special anomaly detection, firewall and consistency check algorithms can be deployed at the edge of the PLMN network, at a roaming intermediary, and/or at the operator of an outsourced or hosted SEPP. In the case of a roaming intermediary and hosted SEPP, such technology potentially benefits from the availability of the information that arises in the context of all mediated signalling, from multiple PLMN/customers. For example, if an intermediary detects an attack originating from a particular PLMN it may be in the position to block it for all destinations that are served via that particular intermediary. However, this criterion cannot take into account any reduction of attack surface due to such technology because

- such technology (which to a large extent is not standardised) is not subject to the evaluation (since the evaluation considers only the mechanisms described in this document and in 3GPP specifications), and
- such technology works only for as long as the entity deploying the technology is not compromised; this criterion, however, considers the protection the different security architectures offer in the case where the different entities *are* compromised.

Evaluation

Bilateral direct architecture (applicable to Model 1): This architecture exhibits the smallest attack surface compared to the other models, as the attack surface that *remains* corresponds to corrupted visited or home operator only.

Outsourced/Hosted/Group SEPP (applicable to Models 2.1, 2.2 and 2.3): The number of (operational) players having access to the signalling is increased compared to the security architecture described for Model 1. In particular, the attack surface that remains corresponds to corrupted visited or home operator, plus a corrupted outsourced, hosted, or group SEPP provider (as applicable) which can read/modify/delete all parameters of any message.

PRINS (applicable to Model 3 and 4): The number of players having access to the signalling is increased compared to the bilateral direct architecture (Model 1). The attack surface that *remains* corresponds to corrupted visited or home operator only, plus some attack surface corresponding to roaming intermediaries depending on the PRINS protection policies in place. Such policies, if too lax, may enable a corrupted Roaming Intermediary such as a Roaming Hub or an on-path RVAS provider (Service Hub), to introduce unwanted signalling. Carefully chosen PRINS protection policies can limit the attack surface that remains.

Hop-by-hop TLS (applicable to Model 3 and 4): This architecture exhibits the largest attack surface compared to the other security architectures, as the attack surface that *it addresses* only corresponds to outsiders trying to obtain access or interfere with the system by introducing unwanted signalling/traffic between hops. All other attack surface *remains*. Compared with Models 2.1, 2.2 and 2.3, in this model additional downstream intermediaries can be added to a given path since the specification does not require the next hop to be roaming partner's SEPP.

4.3.6.2 Attributability

Criterion Description

Attributability allows to identify the true source of any changes or insertions made on the path when forwarding signalling messages.

As the attack surface cannot be fully eliminated in any of the security architectures for the described deployment models, it is expected that some attacks will continue to be observed in 5G SA roaming. Moreover, it is expected that other forms of unwanted signalling will exist as well, for example due to misconfiguration of equipment, faulty implementations and operational errors. In these cases, it is important to be able to attribute the unwanted messages to their true source with as little effort as possible in order to isolate the source of attack or error, without affecting unrelated traffic flows.

Evaluation

Bilateral direct architecture (applicable to Model 1): This architecture exhibits the highest degree of attributability as the end-to-end nature of the security mechanisms ensures that attacks and unwanted signalling originate from the roaming partner’s infrastructure (home or visited network).

Outsourced/Hosted/Group SEPP (applicable to Models 2.1, 2.2 and 2.3): These architectures exhibit a somewhat lower degree of attributability compared to Model 1, since a new possible source of unwanted traffic has been introduced, namely the operator of the outsourced, hosted or group SEPP (as applicable), and no application-layer attributability mechanisms are provided by the protocols. However, differentiating between outsourced, hosted, and group SEPP as opposed to "in-house" PMN SEPP (as in bilateral direct) is an internal matter of the operator; the roaming partner does not need to know whether the attack source is the operator itself or its SEPP operator. That is, from the point of view of the roaming partner, attributability is as in the “bilateral direct architecture”.

PRINS (applicable to Model 3 and 4): This architecture exhibits an attributability level similar to “bilateral direct”, as signalling messages and message parts are digitally signed by their originators. An incoming signalling message can have multiple parts, each signed by a different entity (e.g. roaming partner, on-path RVAS provider (Service Hub), Roaming Hub); the receiver can determine which part originated from which entity without any further steps.

Hop-by-hop TLS (applicable to Model 3 and 4): This architecture exhibits a low attributability level compared to the other options. This is because an incoming message has passed through multiple entities, each of which may have changed the message. For the receiver it is not clear which of the entities last modified the message (e.g. roaming partner, on-path RVAS provider (Service Hub), Roaming Hub). Attributability must be provided by other means (e.g. contractual and/or manual). However, due to the usage of TLS between each hop, outsiders are excluded as potential attack sources in this architecture.

4.3.6.3 Ability to Delegate Roaming Services

Criterion Description

In certain situations, an operator would like to delegate the management of roaming relations to roaming partners or on-path Roaming Value Added Services (RVAS) to an external entity, for example an RVAS Provider, a Roaming Hub or a hosted SEPP provider. Part of such a service is also the connectivity management towards the roaming partners. Some deployment models and security architectures enable such delegation to a larger degree than others, and certain limits need to be considered. While both the delegation of the management of roaming relations as well as the provision of on-path RVAS contain both a contractual and a technical element, the provision of RVAS is typically more technically involved while the management of roaming relations sometimes also includes contractual clauses regarding the financial liability. It is important to note that this criterion considers all the above aspects of the ability to delegate roaming-related services.

Evaluation

Bilateral direct architecture (applicable to Model 1): In this architecture, no services can be delegated to an on-path RVAS provider or intermediary.

Outsourced/Hosted/Group SEPP (applicable to Models 2.1, 2.2 and 2.3): These architectures enable a relatively high degree of service delegation, as the operation of the SEPP is delegated to another entity. An Outsourced/Hosted/Group SEPP can integrate roaming partners connectivity management and RVAS operation.

PRINS (applicable to Model 3 and 4): The ability to delegate in this architecture is higher compared to “bilateral direct” and lower compared to “hop-by-hop TLS” (Model 3 and 4). Through the definition of appropriate policies, on-path RVAS providers (Service Hub) and Roaming Hubs are put in the position to actively participate in roaming signalling and thereby provide their services. It is possible to delegate roaming relation management to a Roaming Hub. However, since the PRINS mechanisms strive to optimise the relationship between security and the ability to delegate services, certain limits to the ability to delegate services apply, as follows.

- There is a fundamental conflict of interest between attributability and the need of certain (historical) RVAS services that require that the very existence of the service being hidden from the roaming partner. Since PRINS solves this conflict in favour of attributability, RVAS services whose existence ought to remain hidden from the roaming partner are *by design* not possible in this architecture.

- Some RVAS, which are sometimes part of a Roaming Hub service offering, are currently not available under this architecture due to slow adoption and difficulties in consistent interpretation of the related specifications. An example of such a service is the dynamic throttling of user plane consumption by the Roaming Hub.

- Compared with “hop-by-hop TLS”, in this architecture roaming intermediaries are more restricted in terms of setting up parallel and alternative signalling routes for the purposes of load balancing and backup routing. It is currently unclear if this can have a significant impact on recovery times after a given route failure compared “hop-by-hop TLS”.

Hop-by-hop TLS (applicable to Model 3 and 4): In this architecture services can be delegated to roaming intermediaries and on-path RVAS providers without restrictions imposed by security mechanisms.

4.3.6.4 Operational Cost

Criterion Description

Some security architectures are more costly for operators to operate than others. In this criterion, the cost efficiency from the operator’s perspective is considered. The costs incurred to other ecosystem stakeholders such as intermediaries are only considered to the extent of their impact on the operator.Also, costs are not quantified and depend on the degree of automation deployed in each individual setting. Factors that are considered in this criterion are the following.

- Importing root certificates for other ecosystem participants and keeping endpoint configurations up-to-date

- Defining and updating protection policies
- N32 Testing and connection management

Evaluation

Bilateral direct architecture (applicable to Model 1): In this architecture, a root certificate for each roaming partner must be imported and assigned to a trust anchor, and updated according to the FS.34 procedures. No certificates for roaming intermediaries are required. The costs in this model are proportionate to the number of roaming partners.

Outsourced/Hosted/Group SEPP (applicable to Models 2.1, 2.2 and 2.3): In these architectures the operator must obtain and maintain a root certificate for the SEPP provider to secure the N32s connection. There is only a single N32s connection towards the SEPP operator. Since this connection serves multiple roaming relations, there is a scalability advantage and the costs are effectively lower compared to bilateral direct. Moreover, typically a group SEPP is less costly from the operator's perspective compared to a hosted or outsourced SEPP since it is operated by a company within the same group.

PRINS (applicable to Model 3 and 4): In this architecture, the root certificate of the roaming partner as well as the roaming intermediary must be imported and updated according to the FS.34 procedures. Moreover, the PRINS protection policies need to be defined according to the business contracts between the operator and the intermediary. Depending on the situation a single PRINS policy set may be suitable for multiple roaming partners – or they may differ depending on the roaming partner. The testing of the connection and related protocol implementation may be more involved compared to testing in the other architectures; however, the burden of fixing issues during testing typically lies with the intermediary, not the operator.

There is only a single N32f connection (TLS VPN) between the operator and the intermediary. Because this connection serves multiple roaming relations, there is some scalability advantage and some cost saving effect occurs as is the case with a hosted SEPP. The overall costs, however, are higher compared to the architecture with a hosted SEPP due to the need to maintain per-roaming partner configuration (root certificates and PRINS policies).

Hop-by-hop TLS (applicable to Model 3 and 4): In this architecture, the root certificate of the roaming intermediary must be imported and updated. There is only a single N32s connection between the operator and the intermediary and therefore the scalability effect applies.

4.3.6.5 Comparison Table

This table summarises the evaluation above.

	Model 1	Model 2.1 / 2.2 / 2.3	Model 3 / 4	
Criterion / Security Architecture	**Bilateral Direct**	**Outsourced, Hosted, Group SEPP**	**Service / Roaming Hub PRINS**	**Service / Roaming Hub Hop-By-Hop TLS**

Attack surface addressed	E2E security between the two PMN SEPPs Only PMN SEPP can read/modify/delete all parameters of all messages.	E2E security between the SEPP provider and roaming partner. SEPP provider can read/modify/delete all parameters of all messages.	Cryptographic protection between PLMNs and Intermediaries Intermediaries can read/modify/delete only certain messages or parameters.	Cryptographic protection between hops, but no E2E encryption/integrity between PLMNs Hub provider can read/modify/delete all parameters of all messages.
Attributability	No cooperation is required in order to attribute message to its origin. Intermediaries are not possible originators.	MNO needs to collaborate in order to attribute origin of message either to itself or to outsourced or hosted SEPP operator. The operator of the Group SEPP must cooperate in order to attribute the origin of a message to a specific group member.	No cooperation is required in order to attribute message (parts) to its origin. Intermediaries are possible originators.	Next and previous hops are authenticated pairwise. Each hop in the chain must cooperate in order to attribute a message to its origin.
Delegation of services	No possibility to outsource RVAS or roaming relation management.	Possibility to outsource RVAS and connectivity management.	Hidden RVAS are not supported and further restrictions to the delegation of roaming services may apply (see evaluation).	Possibility to outsource RVAS, roaming relation management and agreement for RH.
Operational cost	All roaming relations are managed by MNO (N32, TLS certificates).	Single N32s connection towards the SEPP provider to manage all roaming relations. In case of Group SEPP, the operator is a company group member.	MNO needs to manage configuration of individual roaming relations (N32-c, TLS certificates, security policy).	Optimisation in terms of operation, due to scalability effect of Hub SEPP for several MNOs.

4.4 Security Edge Protection Proxy (SEPP)

Compared to the 2G/3G and 4G/LTE system, the 5G System (5GS) is built with security in mind on the basis of the “security by design” principle. This is why inherent security in 5G is a primary goal of the mobile industry and equally applies to the eco-system for 5G SA roaming.

The SEPP is a core element of the 5G architecture, concentrating multiple functions in one element:

- Discovery of a roaming partner’s or next hop SEPP and establishment of a communication channel to it;
- Routing and forwarding of signalling messages to/from roaming partners and/or roaming intermediaries;
- Termination of secure communication channels to internal NFs, and external SEPPs of other MNOs or roaming intermediaries;
- Verification of authenticity of external communication partners (i.e. other SEPPs);
- Verification of integrity of signalling messages;
- Protection of the 5GC at the network edge on application layer;
- Filtering and sanity checking of incoming signalling messages.

With this rich set of functionalities, SEPPs need to be compatible to ensure robust 5G SA roaming connections, and the security of the entire 5GC depends on secure implementation and configuration of the SEPP.

4.4.1 Requirements

4.4.1.1 Minimum SEPP requirements for compatibility

The SEPP shall support the functionalities listed below to maximise compatibility among PMNs and Roaming Intermediaries to ease deployment and operation of 5G SA roaming and to ensure availability of robust roaming connections. All these functionalities shall be supported, regardless which 3GPP release the MNO decides to deploy in its 5GC.

1. 3gpp-Sbi-Target-ApiRoot header shall be supported and used. Telescopic FQDN is deprecated and should not be supported.
2. Certificates shall be used for mutual authentication. Pre-Shared Keys (PSK) shall be rejected.
3. Dedicated certificate, representing the SEPP itself shall be supported in conjunction with 3gpp-Sbi-Target-ApiRoot header. Wildcard certificates should not be used.
4. All certificate handling shall meet the requirements of 3GPP TS 33.501 [19], clause 13.1 and be able to process the X.509 profiles and extensions defined by 3GPP TS 33.310 [69], clause 6.1.
5. TLS 1.2 and 1.3 shall be supported, as defined in 3GPP TS 33.210 [68], latest version, clause 6.2. No older version of TLS shall be supported. Use of TLS 1.3 is preferred.
6. Cipher suites, profiles, and extensions shall be supported and used, as defined in 3GPP TS 33.210 [68], latest version, clause 6.2.

NOTE: Regardless of the 3GPP Release implemented by a MNO, for communication security, only secure cipher suites and profiles are to be used. This is why the latest version of 3GPP TS 33.210 [68] applies in all cases.

7. For all incoming messages on N32, digital signatures shall be validated. On validation failure, messages shall be discarded.

8. The PMN SEPP shall verify that the PLMN ID list received from the remote SEPP during the N32-c security capability negotiation procedure only contains PLMN IDs that are declared in the IR.21 under 'Home PLMN ID list' and 'Visited PLMN ID list' of that roaming partner.

9. The SEPP shall check that each message within the N32-f interface is related to PLMN IDs that have been agreed upon establishment of the N32-c connection. The SEPP shall use the 3gpp-Sbi-Originating-Network-Id parameter.

10. The SEPP shall support HTTP redirection with and without target SEPP discovery, as defined in 3GPP Release 18 TS 29.573 [10] clause 6.1.8.1 and clause 6.1.8.2 respectively.

11. If the SEPP supports DNS-based SEPP discovery, it shall follow GSMA PRD IR.67 [8] and be capable of discovering the peer SEPP based on the well-known FQDN.

4.4.1.2 SEPP Requirements for PRINS

The SEPP in a PMN shall apply an operator-controlled policy that specifies which IEs can be modified by the Roaming Intermediary service provider, which is directly related to the particular SEPP, e.g. 'SUPI, Subscriber Permanent Identifier' or 'location data'.

As stated in 3GPP Release TS 33.501 [19], each PMN operator shall agree the modification policy with the Roaming Intermediary service provider that it has a relationship with, prior to establishment of an N32-f connection. Each modification policy applies to one individual relation between PMN-operator and its Roaming Intermediary service providers. In order to cover the end-to-end N32-f connection both involved PMNs' SEPPs have exchanged their modification policies during N32-c negotiation phase. Both complementary modification policies build the overall modification policy for a specific N32-f connection.

NOTE 1: 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.

NOTE 2: Modification includes removal and addition of new IEs. IEs therefore may not be present in the final message.

The IEs that the Roaming Intermediary is allowed to modify shall be specified in a list giving an enumeration of JSON paths within the JSON object created by the SEPP.

This policy shall be specific per PMN Operator and each of its Roaming Intermediary Service Provider.

The modification policy is under the control in the two SEPPs of the roaming partners.

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

The following basic rule shall always be applied irrespective of the policy exchanged between two parties: IEs requiring encryption shall not be inserted at a different location in the JSON object.

4.4.1.3 Security Requirements for SEPP Implementation

The SEPP shall support the security controls collected in this section to ensure a consistently high level of 5GS roaming security. The security of each MNO network and roaming intermediary can have an impact on all the others. This is why following these requirements is key for the entire industry. SEPP suppliers shall implement all these security controls and MNOs and roaming intermediaries should use them.

NOTE: Stakeholders in the roaming ecosystem may want to integrate fulfilment of these requirements in their contracts or agreements between each other to agree on expected security levels.

General SEPP Requirements

To enable MNOs and roaming intermediaries to deploy and use the functionality and features for 5G roaming, defined in this PRD, and for maximisation of compatibility, the SEPP shall support all necessary functionality defined in this PRD.

Req 01	General
The SEPP shall support all relevant security functionality, controls and features defined in this PRD and in referenced specifications.	

SEPP Security Requirements

For secure signalling and 5GC security, the SEPP shall support the security controls listed below and MNOs and roaming intermediaries shall use these security controls.

Req 02	Security
The SEPP shall support the following: 1. The SEPP shall support filtering of signalling messages on application layer for all categories according to GSMA PRD FS.36 [41], and validation of all incoming messages, before they are processed further. 2. The filtering functionality shall support stateful and stateless filtering to be able to filter all categories of messages as defined in GSMA PRD FS.36 [41]. 3. For all incoming messages on N32, header fields and information elements (IE) across layers of the network stack shall be validated for plausibility. 4. Dedicated trust anchor for certificates per roaming partner (i.e. per PLMN ID), as required in 3GPP TS 33.501 [19], clause 13.1.2 shall be supported.	

Req 02	Security
	5. Certificate exchange and handling, as defined in GSMA PRD FS.34 [37] shall be supported. 6. Certificate retrieval from RAEX Tool for Certificates via API, to retrieve root certificates of roaming partners and other stakeholders in an automated fashion shall be supported either by the SEPP or by the corresponding O&M system. 7. The SEPP shall meet all requirements of 3GPP TS 33.501 [19], clauses 5.9.3.1 through 5.9.3.3. 8. It shall be possible to add and remove cipher suites for TLS on already deployed SEPPs and it shall be possible by configuration to enable, disable and order cipher suites as needed to meet security policies.

For a secure mobile network, more is to be done than listed here. A comprehensive approach to security is required, which is outside the scope of this PRD. Some basic security requirements are collected in GSMA PRD IR.77 [32].

SEPP Privacy Requirements

A SEPP shall minimise access to personal data contained in signalling messages. This information is related to mobile subscribers and subject to privacy regulation and shall not be exposed to people who don't need access to it.

Req 03	SEPP privacy
The SEPP shall limit access to personal data in signalling messages to a minimum. Access shall only be possible for troubleshooting purposes and be limited to a small, pre-selected number of members of staff for the timeframe necessary. If signalling messages are forwarded to monitoring systems, user data shall be removed or anonymised.	

User data in the context of this requirement is any data transferred by the mobile user, which is transported between roaming partners. This user data is not needed for signalling message processing. Examples for user data are authentication vectors (AV) for the radio network and the content of SMS messages. The SUPI/IMSI and MSISDN are needed for routing and other services related to roaming and are not covered by user data, therefore.

NOTE: Local regulation applies and may override or enhance (parts of) the requirement above.

SEPP Multi Tenancy Requirements

A SEPP that serves multiple MNOs, i.e. an outsourced SEPP and a hosted SEPP, shall support multi-tenancy. The SEPP is able to handle routing, connection establishment, signalling messages, verifications, validations, filtering and any other functionality independently per customer MNO.

Req 04	SEPP multi-tenancy

A SEPP that serves multiple MNOs shall support:

1. A separate routing function per tenant;
2. Dedicated FQDNs per tenant, both well-known FQDN and SEPP FQDN;
3. A logical separation between N32 interfaces per tenant;
4. Dedicated certificates per tenant;
5. Individual filtering and sanity check rules per tenant;
6. Global filtering and sanity check rules applicable to all tenants;
7. User accounts that can limit access to dedicated tenants.

A SEPP that serves multiple MNOs should support:

8. Assign IP addresses individually per tenant;
9. Separate virtual networks per tenant;
10. Logically separate monitoring and logging functionalities per tenant;
11. Logically separate administration and O&M facilities per tenant;

4.4.2 Naming, Addressing and Routing for 5G SA Roaming

The procedure for dynamically discovering the SEPP IP address via DNS is similar to the approach currently used by IPX Data Roaming to resolve the PGW's IP address, as detailed in IR.67. Much of the existing DNS infrastructure can be repurposed for SEPP discovery through DNS. For DNS exchange between eDNS servers and IPX RootDNS, the DNS interface should use the IPX Data Roaming VLAN.

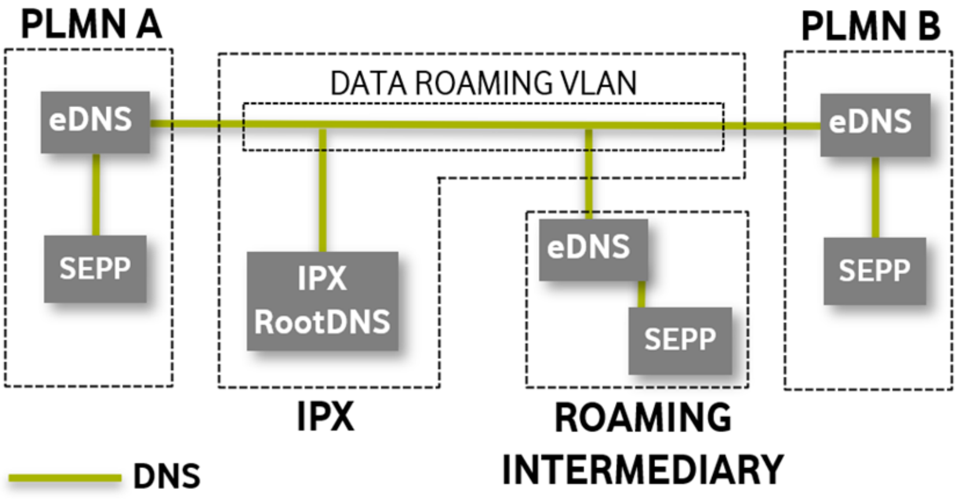


Figure 25– Data roaming VLAN overview.

4.4.3 SEPP Load Distribution

The initiating SEPP (iSEPP) shall distribute N32 traffic for a given MNC/MCC pair according to topology received in DNS SRV records, according to GSMA PRD IR.67 [8]:

```
#service._proto.name.                          TTL  class  SRV  priority  weight  port  target.
```

```
_n32._tcp.sepp.5gc.mnc345.mcc012.3gppnetwork.org.  600  IN    SRV  10      60     443
sepp1.5gc.mnc345.mcc012.3gppnetwork.org.

_n32._tcp.sepp.5gc.mnc345.mcc012.3gppnetwork.org.  600  IN    SRV  10      20     443
sepp2.5gc.mnc345.mcc012.3gppnetwork.org.

_n32._tcp.sepp.5gc.mnc345.mcc012.3gppnetwork.org.  600  IN    SRV  10      20     443
sepp3.5gc.mnc345.mcc012.3gppnetwork.org.

_n32._tcp.sepp.5gc.mnc345.mcc012.3gppnetwork.org.  600  IN    SRV  20       0     443
sepp4.5gc.mnc345.mcc012.3gppnetwork.org.
```

The iSEPP shall distribute the traffic for that MNC/MCC to the rSEPPs with the lowest integer in the priority field according to the weight. iSEPP shall only connect to rSEPPs with a higher integer if all rSEPPs with a lower integer in the priority field are unavailable.

When the connection to a SEPP with the lowest integer in the priority field is lost, traffic should be rebalanced between other SEPPs with the same integer value. In the example above, if the connection to SEPP1 is lost, then the traffic will be redistributed in proportion to SEPP2 and SEPP3; which in this case implies a 50/50 distribution.

When the configured Time To Live (TTL) expires the iSEPP shall obtain NAPTR and SRV records according to GSMA PRD IR.67 [8]: and reconsider the topology according to the received rSEPPs in the SRV record. This may include connecting to additional rSEPPs. When rSEPPs have active n32-f connections to the iSEPP who do no longer appear in the SRV record (or have a higher integer in the priority field) the iSEPP should refrain from sending traffic to that rSEPP. It should however wait for rSEPP to tear down the connection.

Note that the load distribution procedure is unidirectional. Depending on the traffic direction a SEPP is sometimes rSEPP (TLS/HTTP server) or iSEPP (TLS/HTTP/DNS client). This implies that also SEPP discovery and traffic distribution via DNS shall occur in the reverse direction to the peer network. Regardless of the offered topology there is in case of PRINS a need to establish a N32-c connection in the reverse direction to the same SEPP, but only at the point the N32-f needs to be terminated, or an error needs to be reported.

As described in 3GPP TS 33.501 [19], Section 13.2 about application layer security (PRINS) and 3GPP TS 29.573 [10], Sections 5.2.4 and 5.2.5, the reverse N32-c direction is established in order to run the ‘N32-f Context Termination’ or ‘N32-f Error Reporting’ procedure or to modify the security and protection policy.

Such connection must arrive at the same iSEPP who initiated the first N32-c connection (due to the association of ‘n32fContextId’). If no N32-c association for the n32fContextId exists, rSEPP shall establish this reversed N32-c connection based on iSEPP’s FQDN in its client certificate received during the original TLS handshake (from iSEPP to rSEPP connection). In this case rSEPP becomes the initiating SEPP, see 3GPP TS 29.573 [10].

Below is the load distribution according to the above SRV record. rSEPP4 is not connected due to a higher integer in the priority field.

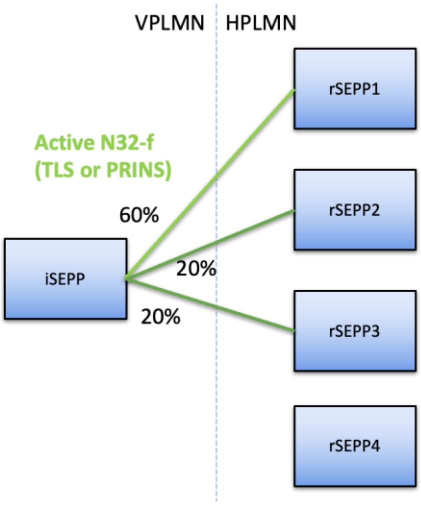


Figure 26 – Sample load distribution over rSEPPs

4.4.4 SEPP HTTP Redirections

A responding SEPP may redirect the N32-c to a different responding SEPP. It can do so after setup of TLS on N32-c with mutual authentication, by responding with an appropriate status code.

For redirections, two use cases are defined where the status code of “307 Temporary Redirect” shall be used. This redirect shall only occur on the first HTTP/2 request on the N32-c interface. The initiating SEPP shall from that moment onwards redirect all traffic to the offered redirected location in the HTTP/2 response header from the “307 Temporary Redirect”.

In the first use case, if the initially responding SEPP wants to redirect to a target SEPP for which no further SEPP discovery is required, than it shall act according to clause 6.1.8.1 of 3GPP Release 18 TS 29.573 [10].

In the second use case if the initially responding SEPP wants to redirect to a target SEPP for which a new SEPP discovery is required, than it shall act according to clause 6.1.8.2 of 3GPP Release 18 TS 29.573 [10].

If not established already, the initiating SEPP needs to establish a N32-c handshake, a N32-f handshake and corresponding TLS connections with the redirected SEPP.

Irrespective of whether or not HTTP redirection is used, the initiating SEPP chooses its egress IPX provider according to local policy. The egress IPX provider at the initiating SEPP side forwards the traffic (potentially via another IPX provider) towards the responding SEPP.

The redirection could have been put in place in order to ensure that, for this particular roaming relation, signalling traffic arrives over a different ingress IPX provider from the viewpoint of the responding SEPP operator. In such a case this IPX provider needs to forward traffic to the IP address of the new SEPP.

HTTP redirection can only point to a SEPP belonging to the same responding PMN and serving the same PLMN-ID. The reason is that application layer destination URIs in the

HTTP message could not be found within another PMN and messages could therefore not be delivered to a producer NF.

4.4.5 Error Handling

3GPP has specified error handling between SEPPs over several releases. In order to support error handling between SEPPs during testing and operation phases, both SEPPs need to be compliant with a particular 3GPP release as further detailed in the following section.

HTTP error handling shall be supported as specified in clause 5.2.4 of 3GPP TS 29.500 [20] and protocol Error Handling shall be supported as specified in clause 5.2.7.2 of 3GPP TS 29.500 [20].

4.4.5.1 N32-c error handling

The common application errors defined in the Table 5.2.7.2-1 of 3GPP TS 29.500 [20] may be used for the N32-c Handshake service.

The SEPP must support the application errors listed in Table 6.1.6.3-1 of 3GPP Release 17 TS 29.573 [10].

4.4.5.2 N32-f (TLS negotiated) error handling

When TLS is negotiated, the SEPP must support Section 5.3.3 of 3GPP Release 17 TS 29. 573 [10].

Support of application specific causes, e.g., “CONTEXT not found”, is specified in Table 5.3.3-1 of 3GPP Release 18 TS 29. 573 [10].

4.4.5.3 N32-f (PRINS negotiated) error handling

When PRINS is negotiated, the SEPP must support the application errors defined for JOSE protected message forwarding API on N32-f as listed in Table 6.2.6.3-1 of 3GPP Release 17 TS 29.573 .

5 User Plane Architecture and Interfaces

5.1 SMF and UPF in HPMN and VPMN

5.1.1 VPMN 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 VPMN. Similar to the non-roaming case, the AMF provides the SMF in VPMN with UE location information and the SMF in VPMN can select during PDU session establishment an UPF at edge location close to the location of the UE, see also Section 6.3.3.3 of 3GPP TS 23.501 [1] and section 4.3.2.2.1 of 3GPP TS 23.502 [2]. If the location of UE changes, the SMF in VPMN can, e.g.:

- Keep the anchor UPF and insert or re-allocate an I-UPF, see section 4.9.1.2 and section 4.9.1.2.4 of 3GPP TS 23.502 [2], respectively, or
- Trigger re-establishment of PDU Session or release the PDU Session after handover procedure, see section 4.9.1.3 of 3GPP TS 23.502 [2].

5.1.2 N9 Interface between VPMN and HPMN UPF

The Home Routed (HR) scenario makes use of both SMF's and UPF's in the VPMN and HPMN. In this case the SMF in the HPMN (H-SMF) selects the UPF(s) in the HPMN, and the SMF in the VPMN (V-SMF in this case) selects the UPF(s) in the VPMN. Thus, the N9 reference point for user plane traffic is applicable to the HR scenario, as seen in Figure 4 and Figure 5. Both V-SMF and H-SMF are selected by the AMF during PDU session establishment. The V-SMF can be changed, e g., during N2 handover procedure as described in section 4.23 of 3GPP TS 23.502 [2].

The use of a SMF and UPF in the VPMN enables VPMN charging.

NOTE: Pause of charging as specified in section 4.4.4 of 3GPP TS 23.502 [2] has no use case, hence the support of pause of charging is not recommended.

The use of SMF and UPF in the VPMN also enables VPMN LI and minimizes the impact on the HPMN of the UE mobility within the VPMN (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 HPMN 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.

5.1.3 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 V-SMF in the VPMN.
- The V-SMF forwards to the H-SMF in the HPMN SM related information.
- The H-SMF receives the SUPI of the UE from the V-SMF during the PDU Session Establishment procedure.
- The H-SMF 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 H-SMF obtains the subscription data directly from the HPMN UDM (Unified Data Management).
- The H-SMF may send QoS requirements associated with a PDU Session to the V-SMF. This may happen during the PDU Session Establishment procedure and after the PDU Session is established. The interface between H-SMF and V-SMF is also used to carry (N9) User Plane forwarding information exchanged between the H-SMF

and the V-SMF . The V-SMF may check QoS requests from the H-SMF with respect to roaming agreements.

In the HR roaming case, the AMF (Access and Mobility Management Function) selects both a V-SMF and a H-SMF as described in clause 4.3.2.2.3.3 of 3GPP TS 23.502 [2], and provides the identifier of the selected H-SMF to the selected V-SMF as described in clause 4.3.2.2.2 of 3GPP TS 23.502 [2].

Conversely, in roaming with LBO, the AMF selects a SMF in the VPMN as described in clause 4.3.2.2.3.2 of 3GPP TS 23.502 [2].

5.1.4 GTP-U

The N9 interface makes use of the GPRS Tunnelling Protocol, GTP version 1 for the User Plane. The UPF's inside the PMNs making use of the Home-Routed solution architecture are compliant to 3GPP Release 16 TS 29.281 [18] 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 3.3.

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

5.2.1 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 27 illustrates the Home-routed roaming architecture for interworking between 5GS EPC/E-UTRAN making use of the interfaces to the EPC.

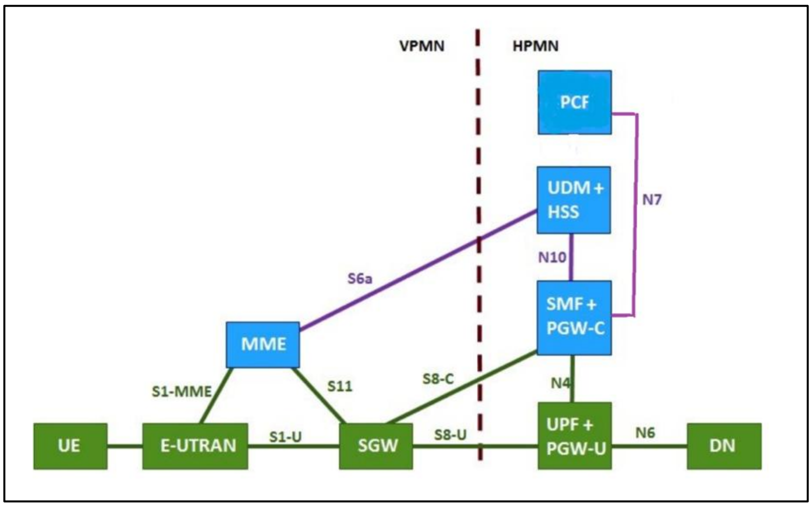


Figure 27 – Home-routed roaming architecture for interworking between 5GS EPC/E-UTRAN

A 5GC in the HPMN that supports this interworking architecture, is therefore able to support 4G network roaming to an EPC based VPMN. 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 VPMN 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].

5.2.2 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 PMN.

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.

5.2.2.1 PGW selection

The visited MME has the task to select the appropriate PGW. This is based on the selected APN, whether local break out is allowed, and on specific subscription parameter which are enhanced for 5GC.

In case the traffic is home routed, and if HPMN has introduced 5GC as an overlay to the existing EPC and steers the specific subscriber traffic towards the new PGWs supporting 5GC (e.g. combined PGW-C/SMF), the MME at VPMN needs to support the 5GC subscription parameter and translate these into corresponding NAPTR DNS request and specific service tags. This allows the HPMN to control the PGW selection by MME of VPMN between legacy PGWs in EPC or combined SMF/PGW-C.

In case the MME at VPMN is pre-3GPP Rel15 MME not capable to support the 5G parameter, the MME will only select PGW from legacy EPC as the specific service tags in DNS will be missing and point to the EPC PGW pool addresses.

For these scenarios it is recommended to make use of an existing mechanism which is available in the 3GPP standards from early Releases and applicable for 2G/3G and 4G access. “APN-OI replacement” parameter can be set in the subscription parameter, which will be added as an appendix into the APN FQDN and therefore allows operator to offer such a PGW selection for all legacy interworking use cases. For more details, see GSMA PRD IR.88 [3].

5.2.3 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 4.3.1.1). 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.

5.2.4 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].

5.2.4.1 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 VPMN that utilises 5GC will not be permitted to handover to NR connected to 5GC.

5.2.4.2 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 VPMN that utilises EPC will not be permitted to handover to E-UTRAN connected to EPC.

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

[Editor’s Note: Placeholder for future content]

6 5GS Services

6.1 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.

6.1.1 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.

If the procedure is to be rejected, then the appropriate error cause is:

- 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).
- Cause #27 (N1 mode not allowed) if the VPMN already has a Roaming Agreement with the HPMN covering other Radio Access Technologies (RATs), it forces the UE to disable N1 capabilities and reselect another RAT in the same PMN.

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.

6.1.2 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 28 below illustrates the AMF registration service operation.

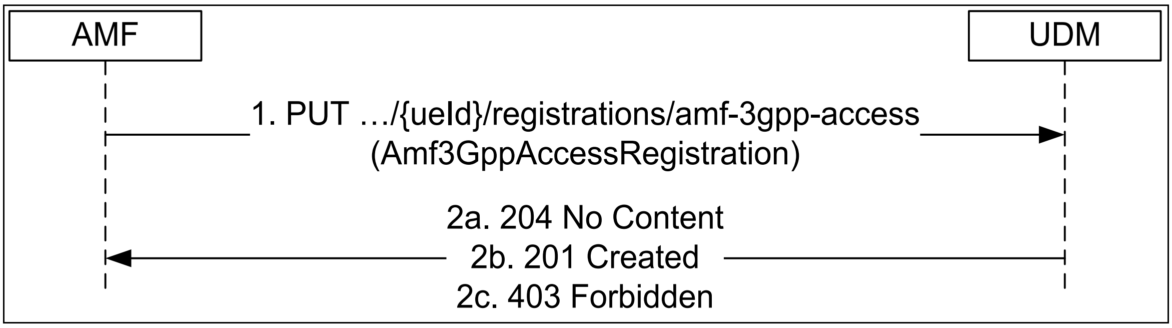

AMF
UDM
1. PUT …/{ueId}/registrations/amf-3gpp-access
(Amf3GppAccessRegistration)
2a. 204 No Content
2b. 201 Created
2c. 403 Forbidden

Figure 28 – 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.)

6.2 Data Sessions

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.

6.2.1 UE Addressing

6.2.1.1 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.

6.2.1.2 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].

6.2.2 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.

6.2.3 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 PMN NF services make use of IPv6 only.

6.2.3.1 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 PMNs, where the correct target NF service should be reached. Where the target URI authority designates an origin server not in the same PMN 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 PMN, the FQDN of the target NF shall have the Home Domain as the trailing part – i.e.

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

6.2.4 DNN for Home Operator Services

6.2.4.1 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.

6.2.4.2 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.

6.2.4.3 Inter-PLMN roaming hand over

If the PDU session to the DNN for Home Operator Services is maintained after moving from one PMN 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].

6.2.4.4 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.

6.3 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 standard value for eMBB (SST= 1 and no SD).

GSMA PRD NG.114 [21] provides the guidelines on the IMS profile for voice, video and messaging over 5GS.

6.3.1 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.

6.3.2 IMS Voice Roaming Architecture

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 6.8 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);
- Downlink service level gating (to avoid additional and unexpected traffic on the signalling bearer) as described in 3GPP TS 23.501 [1] and 3GPP TS 23.503 [53].
- This is also needed to avoid that additional and unexpected traffic on the signalling bearer reaches the lawful interception functions for N9HR in the VPMN.

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.

6.3.2.1 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].

6.3.2.2 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 6.8.2 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);
- Downlink service level gating (to avoid additional and unexpected traffic on the signalling bearer) as described in 3GPP TS 23.501 [1] and 3GPP TS 23.503 [53].

This is also needed to avoid that additional and unexpected traffic on the signalling bearer reaches the lawful interception functions for N9HR in the VPMN.

If data media for IMS Data Channel as specified in section 5.1 of 3GPP Release 16 TS 26.114 [51] is supported, then QoS flow e.g. with 5QI=9, 71, 72, 73, 74, 76 as determined by the IMS data channel service.

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.

NOTE4: As stated in section 5.16.4.1 of 3GPP TS 23.501 [1], IMS emergency services can also, as per policy of the VPMN and local regulation, be provided to:

- inbound roamers without an IMS voice roaming agreement,
- inbound roamers with a SUPI that cannot be authenticated, or
- inbound roamers without a SUPI.

This behaviour is independent of any roaming relationship between the two operators.

3. 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);
- If data media for IMS Data Channel as specified in section 5.1 of 3GPP Release 16 TS 26.114 [51] is supported, then QoS flow e.g. with 5QI=9, 71, 72, 73, 74, 76 as determined by the IMS data channel service.

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.

6.3.2.3 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].

6.3.2.4 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.

NOTE1 : For a voice centric UE, the IMS Voice Roaming restriction described in this section will result in the UE not selecting a cell connecting only to 5GC, as specified in section 5.16.3.5 of 3GPP TS 23.501 [1], even if roaming restrictions for 5GC as described in Section 6.1 are not applicable to the UE.

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].

NOTE 2: 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].

NOTE 3: 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.

6.4 Emergency Services

6.4.1 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 [55], 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.

6.4.2 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.

6.5 Network Slicing

A 5GS UE and 5GC must support network slicing. When a UE registers to the VPMN, it can include a Requested NSSAI, which contains up to eight S-NSSAIs. The UE subscription information must contain one or more S-NSSAIs. 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].

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. GSMA PRD

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].

6.5.1 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 VPMN as in the HPMN for the network slices serving the UE. Based on local VPMN policy or if the VPMN and the HPMN have an agreement to support S-NSSAI with non-standard values in the VPMN, the AMF or the NSSF of the VPMN maps the Subscribed S-NSSAI values (provided by the HPMN) to the respective S-NSSAI values to be used in the VPMN. 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:

- VPMN with the Configured NSSAI for the serving PMN: applies to the VPMN only, and/or
- HPMN with the Default Configured NSSAI: applies to any serving PMN (VPMN if roaming) 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 PMN only if the UE has no Configured NSSAI for this serving PMN.

The Configured NSSAI for the serving PMN includes the S-NSSAI values which can be used in the VPMN and may be associated with mapping of each S-NSSAI of the Configured NSSAI to one or more corresponding HPMN 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 VPMN
- Default Configured NSSAI if available, and if no Configured NSSAI for the serving PMN is available
- Configured NSSAI for the serving PMN, 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 PMN (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 VPMN can map S-NSSAI values provided by different HPMNs into the same S-NSSAI value used in the VPMN.

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].

6.5.2 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 (GSMA PRDs WA.51[67], BA.27 and WA.52). Guidance on billing and charging (BCE) processes are available in GSMA PRD TD.201 [46]. Successful completion of all networks, device and billing related steps are required to support network slice roaming.

A fundamental aspect of the roaming support in the 5GS is the definition in the serving PMN of a mapping between the HPMN S-NSSAI value and VPMN S-NSSAI value. This mapping is based on the agreement between the roaming partners of what NEST (or attributes) is associated to a S-NSSAI of the HPMN. In the case of GSMA-defined NEST, the NEST is defined in GSMA PRD NG.116 [27]. The VPMN decides on all mappings between an HPMN S-NSSAI value and an VPMN S-NSSAI value and configures its network accordingly.

The HPMN informs the required technical information to the VPMN utilizing GSMA PRD IR.21 [56] or other means; this technical information includes, amongst others, which S-NSSAI, DNN and 5QI are used by outbound roamers.

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

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

- Configured NSSAI for the serving PMN 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 authorisation as described in Section 5.15.10 of 3GPP Release 16 3GPP TS 23.501 [1].

In roaming scenarios it is recommended that the serving AMF provides the UE with mapped S-NSSAI(s) as specified in 3GPP TS 24.501 [28].

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 standard value for eMBB [SST=1 and no SD] is supported globally for roaming as a globally by all 5GS PMNs 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 S-NSSAIs if required.

The VPMN provides to the HPMN the HPMN S-NSSAI and DNN during PDU session establishment. The HPMN provides to the VPMN the 5QI for the default QoS flow. If a dedicated QoS flow is established, the HPMN provides to the VPMN the 5QI for the dedicated QoS flow.

For other Subscribed S-NSSAIs, that the HPMN allows for the UE in the VPMN, it is recommended that these S-NSSAIs

- Use either one of the standardized SST values as specified in Table 5.15.2.2-1 of 3GPP TS 23.501 [1], or have an SST that both roaming parties agree with if this not one of the standardized SST values
- Have either no SD or an SD that both roaming parties agree, and
- Have a corresponding NEST in GSMA PRD NG.116 [27] or be associated with a NEST that both roaming parties agree as applicable.

A HPMN S-NSSAI using a standardized SST (and no SD) can either be used with the same value in the VPMN or be mapped in the VPMN to

- a VPMN S-NSSAI value using the same SST value and a SD value determined by the VPMN, i.e., to an S-NSSAI with non-standard value but with same SST, or
- any other VPMN S-NSSAI with any SST.

6.6 Location Services

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 29 hereafter, using potentially different interfaces to retrieve location in roaming.

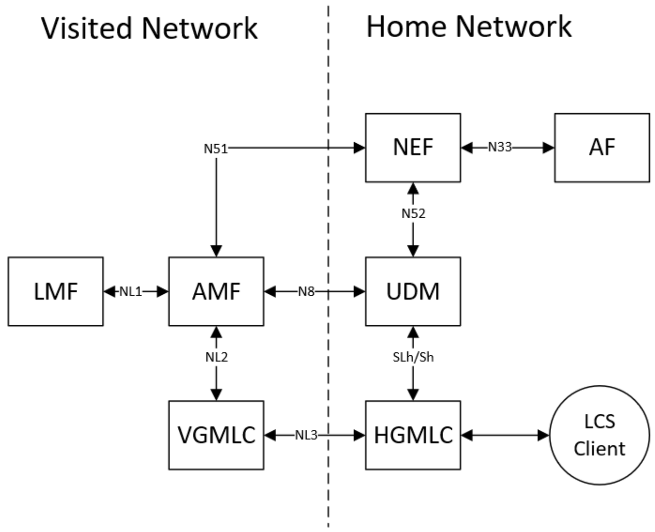


Figure 29 – Location Support

In order to retrieve the location information from the visited network, 3 different HTTPs signalling messages could be used:

- N8: ProvideLocationInfo
- NL3: ProvidePositioningInfo (LCS architecture related to MT-LR procedure)
- N51: EventExposure (N51 between AMF and NEF is specified in 3GPP TS 29.518 [12] and detailed in Section 7.1 of GSMA PRD NG.120 [45].)

NL3 (3GPP TS 23.273 [65], §4.4.2) supports location requests forwarded by an HGMLC to a VGMLC. N51 (3GPP TS 23.273 [65], §4.4.9) supports queries from an NEF to a serving AMF for the location of a target UE.

The figure hereafter describes the Service Based approach for Location Services.

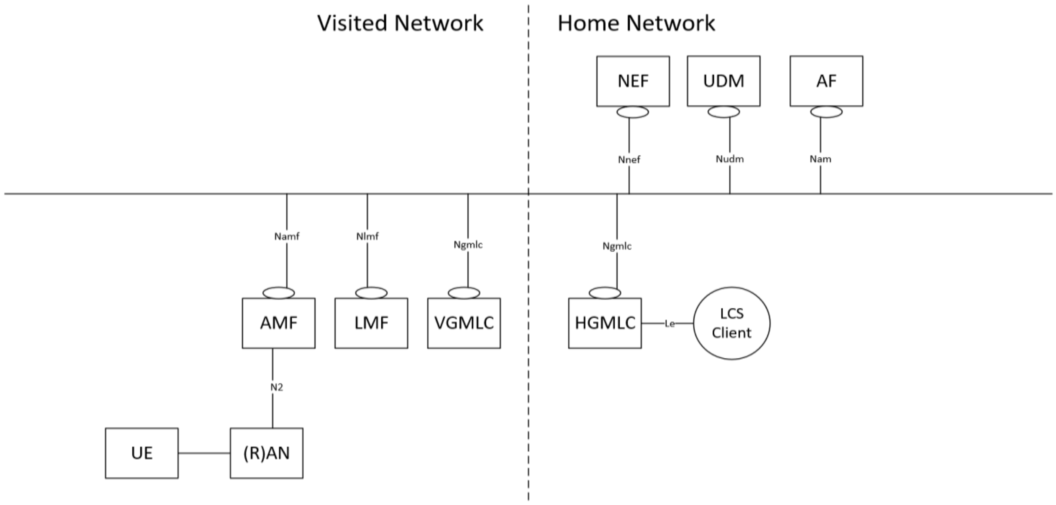


Figure 30 – 5G location detailed architecture (service based)

- Ngmlc_Location (3GPP TS 29.515 [66], §5.2) enables an NF to request location determination for a target UE.
- Namf_EventExposure Service (3GPP TS 29.518 [11], §5.3) defines an additional method: Event: Location-Report: NEF subscribes to this event to receive the last known location of a UE or a group of UEs or any UE, and Updated Location of any of these UEs when AMF becomes aware of a location change of any of these UEs with the granularity as requested.

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.

6.7 UE Route Selection Policy

UE Route Selection Policy (URSP) is specified in 3GPP TS 23.503 [53]. If it is supported to provide URSP to the UE when roaming, then the AMF in the VPMN establishes a policy association via the V-PCF with the H-PCF in the HPMN. N24 is the reference point between the V-PCF and the H-PCF, see also Section 3.2. The establishment of the policy association is triggered, e.g., by receiving the UE Policy Container from the UE during the registration procedure, see also GSMA PRD NG.114 [21].

If the H-PCF generates URSP rules, then the H-PCF includes the UE policy information delivered to the UE into one or more Policy Sections each identified by a Policy Section Identifier (PSI). H-PCF compares generated URSP policies with PSIs provided by UE in the UE Policy Container. If policies generated at H-PCF are same as the ones reported by UE then URSP rules are not updated.

NOTE 1: It is possible that the H-PCF does not generate URSP rules and consequently none would be delivered to the UE.

The H-PCF provides the URSP rules via the V-PCF to the AMF. The AMF uses network-initiated NAS transport procedure to provide the URSP rules to the UE as specified in section 5.4.5.3 of 3GPP TS 24.501 [28].

NOTE 2: 3GPP TS 24.501 [28] uses UE Policy Section Identifier (UPSI) whereas 3GPP TS 23.503 [53] uses PSI to denote the same.

A URSP rule contains Rule Precedence, Traffic Descriptor and list of Route Selection Descriptors. It may also contain Route Selection Validation as specified in 3GPP Release 16 TS 23.503 [53]. The H-PCF generates the Traffic Descriptor based on available information. The following table provides some examples how to use Traffic Descriptors and Route

Selection Descriptors to select S-NSSAI and if possible also DNN to be used for PDU session establishment. As specified in 3GPP Release 16 TS 23.503 [53], the supporting UE can also use URSP to determine the DNN for PDN connection establishment in EPS.

NOTE 3: The list of Route Selection Descriptors may also include other components than DNN and S-NSSAI.

Traffic Descriptor	Route Selection Descriptors	Comments
DNN	S-NSSAI, and optionally, DNN	For pre-Rel-17 UEs and networks, If using DNN as Traffic Descriptor, DNN cannot be used as Route Selection Descriptor (RSD). For Rel-17 UEs and networks: If using DNN as Traffic Descriptor, the DNN can be in both the Traffic Descriptor and in the corresponding Route Selection Descriptor (RSD). To provide uniform service experience for UEs from Releases prior to Rel-17, when a USRP rule with a Route Selection Descriptor including a DNN different from DNN(s) provided in the Traffic descriptor is provided to the UEs, the DNN(s) used in the Traffic descriptor would also need to be included in the policy for DNN replacement in the network. In addition, a lower priority Route Selection Descriptor without a DNN would also need to be provided to the UEs. See 3GPP Release 17 TS 23.503 [53]. (See Note 1)
Connection Capabilities	S-NSSAI, DNN	3GPP TS 24.526 [54] has standardized identifiers for IMS, MMS, SUPL, and Internet. Connection Capabilities can allow up to 255 values.
Application Descriptor	S-NSSAI, DNN	Application Descriptor includes OSId and OSAppID, both are OS specific, and the formats and naming rules are not further specified by 3GPP. The HPMN may receive this information directly from the OS vendors and App vendors.
IP / Non IP Descriptors	S-NSSAI, DNN	Either Destination IP Descriptor or Non-IP Descriptor may be used. Not further specified in 3GPP.
Domain Descriptor	S-NSSAI, DNN	Domain Descriptor includes either FQDN(s) or a regular expression. Not further specified in 3GPP.
NOTE 1: This is needed because: (1) pre-rel-17 UEs would consider the Route Selection Descriptor with DNN as invalid and therefore ignore it and then would use the lower priority Route Selection Descriptor without DNN, and (2) therefore, the DNN used by the pre-rel-17 UEs would be from the Traffic Descriptor, which would have to be replaced by the network to match the DNN in the higher priority Route Selection Descriptor.		

Table 6 – Examples of Traffic Descriptors and Route Selection Descriptors (See 3GPP TS 23.503 [53} and 3GPP TS 24.526 [54]

6.8 DNN for IMS based services

6.8.1 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).

6.8.2 IMS well-known DNN

6.8.2.1 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.

6.8.2.2 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 establish 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].

6.8.2.3 Inter-PLMN Roaming Hand Over

If the PDU session to the IMS well-known APN is maintained after moving from one PMN 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.

6.9 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].

7 Technical Requirements and Recommendations for Charging

Charging Function (CHF) is the Network Function in the SBA which exposes the Nchf services, enabling three basic scenarios, specified in TS 32.290 [62] and TS 32.291 [63]:

- Data charging (HR or LBO)
- Mobility charging
- SMS over NAS charging

7.1 Data charging

7.1.1 Home Routed data charging

5G data connectivity converged charging architecture for Home Routed data roaming is defined in the Figure 31 below (3GPP TS 32.255 [61] - figure 4.2.4). The N40 reference point is defined for the interactions between H-SMF and H-CHF and between V-SMF and V-CHF in the reference point representation:

- V-SMF shall consume Nchf services offered by V-CHF via N40 reference point for CDR generation in VPMN
- H-SMF shall consume Nchf services offered by H-CHF via N40 reference point for CDR generation in HPMN to manage online or offline charging with or without quota management

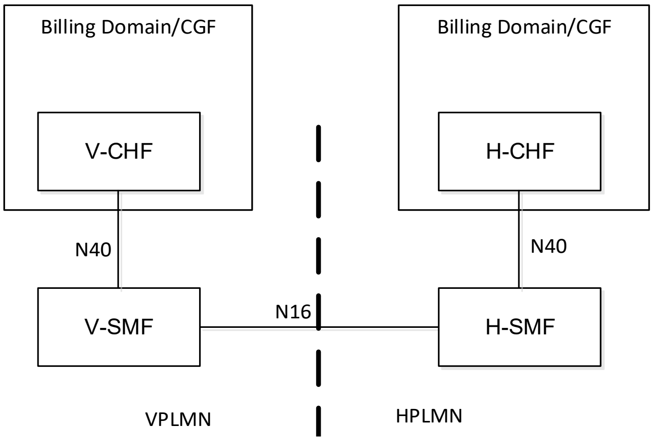


Figure 31 – 5G Reference point Representation (data HR charging)

In home routed roaming scenario, for each UE roaming in VPMN:

The SMF in the VPMN (V-SMF) shall be able to collect charging information per QoS Flow within a PDU session when UE is determined as an in-bound roamer, for CDR generation in VPMN (wholesale purpose).

The V-CHF will generate QoS flow Based Charging (QBC) CHF CDRs containing:

- the PDU Session Charging Information, incl. HPMN S-NSSAI, DNN and 5QI, see also Section 6.4.2
- the Roaming QoS flow Based Charging (QBC) Information (for Wholesale Invoicing)

The SMF in the HPMN (H-SMF) shall be able to collect charging information per QoS Flow within a PDU session when UE is determined as an out-bound roamer, for CDR generation in HPMN (retail purpose)

The H-CHF will generate PDU Session Charging CHF CDRs containing:

- Multiple Unit Usage (MUU) for Flow Based Charging (FBC) for retail
- PDU Session Charging Information (for retail/Wholesale)
- Roaming QBC Information (for Wholesale reconciliation)

In home routed scenario, this charging information collection mechanism is achieved under Roaming QoS flow Based Charging (QBC) performed by each PMN, based on a set of charging parameters exchanged between the V-SMF and the H-SMF on a per PDU session basis.

7.1.2 LBO data charging

The Figure 32 below (3GPP TS 32.255 [61] - figure 4.2.6a – Release 18) depicts the 5G data connectivity converged charging architecture for roaming Local breakout in reference point representation:

- V-SMF shall consume Nchf services offered by V-CHF via N40 reference point for CDR generation in VPMN for wholesale charging
- V-CHF shall consume Nchf services offered by H-CHF via N107 (transported across N32) for CDR generation in HPMN for retail charging

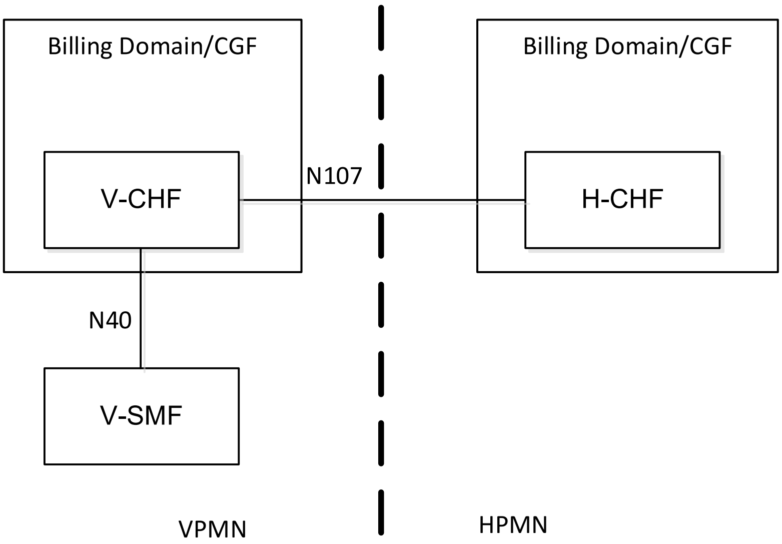


Figure 32 – 5G Reference point Representation (data LBO charging)

In local breakout scenario, for each UE roaming in VPMN, the SMF in VPMN (V-SMF) shall be able to collect charging information within a PDU session when UE is determined as a roamer:

- per QoS flow for CDR generation by V-CHF in VPMN and CDR generation by H-CHF in HPMN
- per service data flow for converged charging, based on PCC rules from V-PCF which uses locally configured policies according to the roaming agreement with the HPMN operator.

7.2 Mobility charging

The following Figure 33 (figure 4.2.2.2 in 3GPP TS 32.256 [60]) depicts the 5G connectivity and mobility converged charging architecture in reference point representation:

- The N41 reference point (transported across N32) is defined for the interactions between AMF and H-CHF for retail charging
- The N42 reference point is defined for the interactions between AMF and V-CHF for wholesale charging

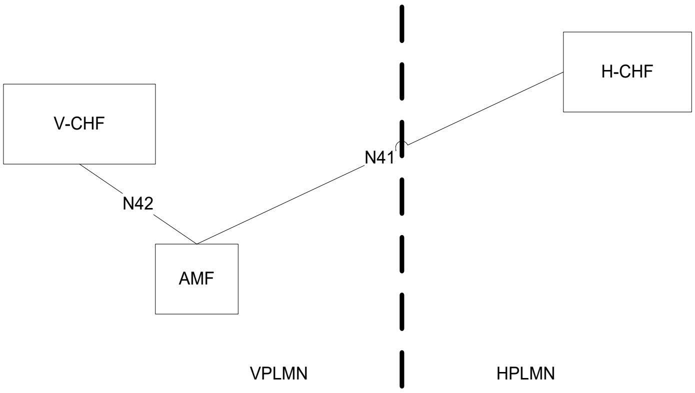


Figure 33 – 5G Reference point Representation (mobility charging)

5G connection and mobility converged charging, when activated, may be performed by the AMF interacting with both V-CHF and H-CHF using Nchf specified in TS 32.290 [62] and TS 32.291 [63]. In order to provide the data required for the management activities outlined in TS 32.240 [59] (Credit-Control, accounting, billing, statistics, etc.), the AMF shall be able to perform converged charging.

7.3 SMS over NAS charging

The following Figure 34 (figure 4.4.2. in 3GPP TS 32.274 [64]) depicts the 5G SMS over NAS converged charging architecture in reference point representation (SMS node is the SMSF):

- N46 Reference point is based on Nchf service based interface, and provides charging information between SMSF and V-CHF for in-bound roamer (wholesale charging)

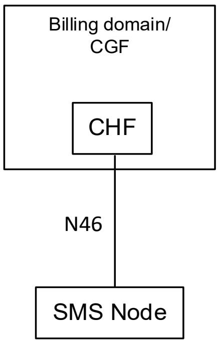


Figure 34 – 5G Reference point Representation (SMS charging)

SMS charging uses the Event Charging with Unit Reservation (ECUR) principle, enabling to charge SMS only if acknowledgement is received from the Home SMSC.

A typical example is presented hereafter based on figure 5.3.2.1.2 in 3GPP TS 32.274 [64], defining how to charge SMS submission (1) and also on the submission acknowledgement (6).

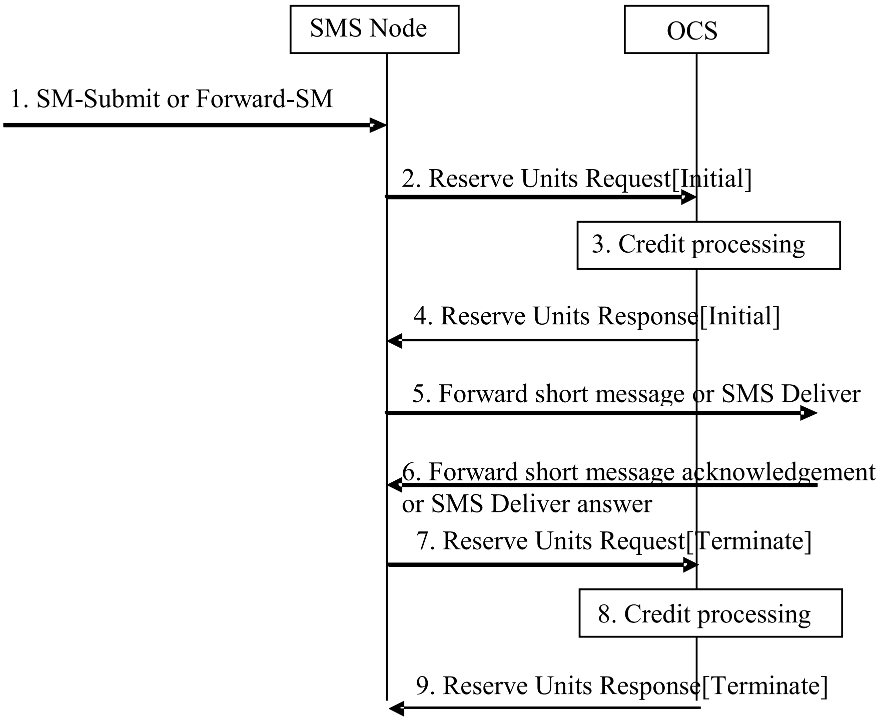

SMS Node
OCS
1. SM-Submit or Forward-SM
2. Reserve Units Request[Initial]
3. Credit processing
4. Reserve Units Response[Initial]
5. Forward short message or SMS Deliver
6. Forward short message acknowledgement
or SMS Deliver answer
7. Reserve Units Request[Terminate]
8. Credit processing
9. Reserve Units Response[Terminate]

Figure 35 – Online charging in simple submission (with Unit Reservation)

8 Further Roaming Security Considerations

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 PMN 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 addresses the secure deployment and operation of 5GS roaming. Aspects, such as security controls at the network edge, secure communication, key management and protection policy exchange are covered.

PMN operators and roaming service providers are advised to adhere to the recommendations which are given in this section.

8.1 Preparatory Steps per 5G Roaming Relation

Each operator shall establish its own operational policies and the necessary keys (for interacting with a specific roaming partner bilateral or via its associated roaming intermediary) to allow for secure exchanging of the protection policies via N32-c.

Operators shall establish communication channels to easily deploy policies and key updates.

8.2 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.

8.3 Risks from Interworking with Different Technology Generations and Signalling 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 signalling.

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 signalling 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:

- 5G SA scenario
- 5G NSA and native LTE scenario
- 5GC with EPC interworking scenario

- Native 2G and 3G scenarios.

As an illustration, Figure 36 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 signalling 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 signalling support between the Diameter Edge Agent (DEA)/SigFW border elements of the EPC networks as specified in GSMA PRD FS.19 [34].

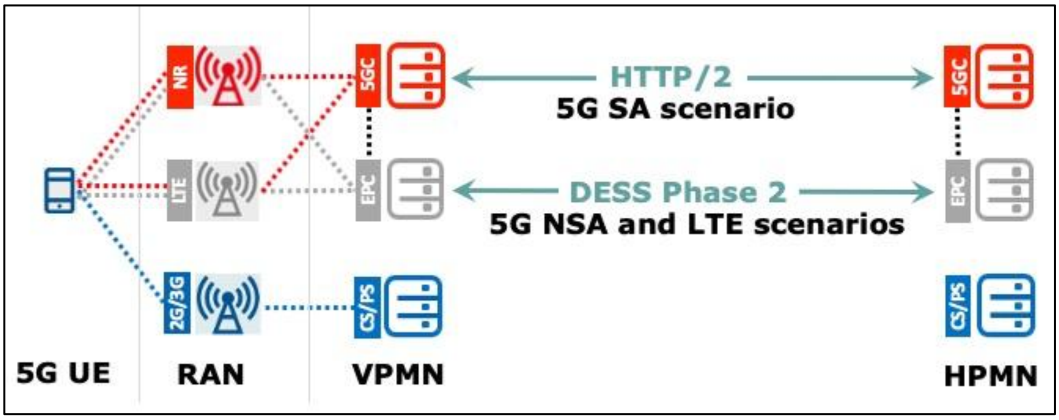


Figure 36 – Confidentiality Protected Roaming Scenarios

NOTE 1: 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 signalling (without the DESS enhancements) or via SS7 signalling.

This is illustrated in Figure 37, 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 signalling 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].

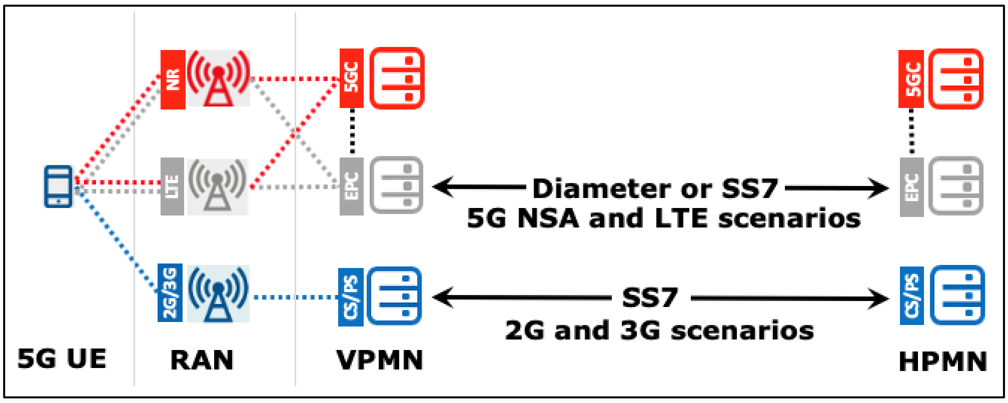


Figure 37 – Least Protected Roaming Traffic Scenarios

NOTE 2: 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 signalling by the parallelism of technologies like 2G, 3G, 4G and 5G in combination with the coexistence of SS7, Diameter and HTTP/2 signalling protocol suites.

9 Technical Requirements for QoS support

This section covers the functionality needed in the VPMN and in the HPMN 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 VPMN.

9.1 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.

9.2 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].

9.3 QoS control

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

9.3.1 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 HPMN to implement a PCC infrastructure which is mandatory if the HPMN 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 HPMN. See the architecture diagram below.

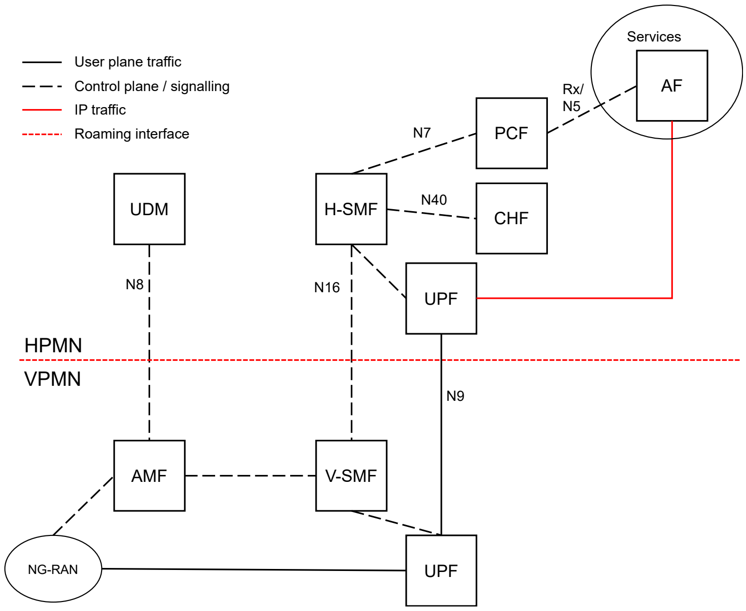


Figure 38 – PCC Architecture with Home Routed Architecture

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

15. The VPMN must support the relevant QoS control procedures.

16. The VPMN and the HPMN must be able to ensure that QoS parameters of roamers are within the limits of the roaming agreement.

17. The VPMN 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 VPMN must support PDU session modification procedures, initiated by the H-SMF based on HPMN 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.

9.3.2 Requirements for the VPMN

Control of QoS parameters within the VPMN 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 VPMN 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:

14. 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.
15. Complex roaming controls for inbound and outbound QoS management procedures on a per-partner basis.
16. 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 HPMN, the following functionalities are required by the VPMN:

- During a PDU session establishment, the V-SMF may apply VPMN policies related to the SLA negotiated with the HPMN or with QoS values supported by the VPMN; 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].
- The V-SMF provides the QoS constraints from the VPMN for the default QoS flow to the H-SMF (as specified in section 6.1.6 of 3GPP Release 17 TS 29.502 [14]) during
    - PDU session establishment as specified in section 4.3.2.2.2 of 3GPP Release 17 TS 23.502 [2],
    - intra-5GS mobility with V-SMF insertion or V-SMF change as specified in section 4.23.7 of 3GPP Release 17 TS 23.502 [2], and
    - EPS to 5GS idle mobility and handover procedures as specified in section 4.11.1.3.3 and 4.11.1.2.2.2 of 3GPP Release 17 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 HPMN 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 HPMN must ensure that the QoS parameters from the HPMN are within the limits of the roaming agreement, see also section 9.3.3.

9.3.3 Requirements for the HPMN

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

If the H-SMF receives QoS constraints from the VPMN for the default QoS flow as specified in section 6.1.6 of 3GPP Release 17 TS 29.502 [14], the H-SMF provides the QoS constraints from the VPMN to PCF. The PCF takes this into account when making policy decisions as specified in section 4.3.2.2.2 and in section 4.11.1.2.2.2 of 3GPP Release 17 TS 23.502 [2].

In order to ensure that the requested QoS sent to a VPMN is within the limits of the roaming agreement, the HPMN's PCF must - in case of an outbound roamer – only provide QoS parameters (see Section 9.2) to the HPMN's SMF, which are within the limits of the roaming agreement with the respective VPMN, and taking into account received QoS constraints from the VPMN.

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

9.3.4 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 VPMN, 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 HPMN.

For connections for an IMS "well known" APN, the services and corresponding 5QI must be supported by the HPMN, as described in Section 6.3.2.

NOTE: If neither the HPMN, VPMN, 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 HPMN and VPMN, 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 VPMN. If the VPMN 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.

9.3.5 Support of QoS by the IPX

When one or more IPX providers are used in the path between the VPMN and the HPMN;

- 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.

9.3.6 Enforcement of QoS by the VPMN

If a VPMN has agreed to enforce QoS in a roaming agreement, then the VPMN 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-PLMN 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 VPMN, as describe in Section 6.3.2.

10 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 6.

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	Disabled[5]	Enabled[5]	Disabled[5]	Enabled[5]	Enabled[5]	Enabled[5]
ARP-PCI	Enabled[5]	Disabled[5]	Enabled[5]	Disabled[5]	Enabled[5]	Disabled[5]
MFBR-UL	156[3]					
MFBR-DL	156[3]					
GFBR-UL	156[3]					
GFBR-DL	156[3]					

Table 7 – 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 VPMN can downgrade the requested PCI and/or PVI and accept the request. PVI downgrade is used to change the HPMN Disabled request to Enabled in the VPMN while PCI downgrade is used to change the HPMN Enabled request to Disabled in the VPMN.

Annex B Detailed design for inter-PLMN connection using direct TLS

This detailed design is following 3GPP specifications.

B.1 Introduction

This Annex describes the inter-PLMN connection setup between a pair of SEPPs of two PLMNs. It covers the deployment scenario with initial dynamic SEPP discovery, TLS connection setup, N32-c connection setup and N32-f connection setup.

For the sake of clarity, the call flows do not show all parameters but only certain examples where relevant.

B.2 Scenario description

An NF in PLMN A needs to send a message to an NF in PLMN B. The SEPPs on either side are responsible to set up and secure the connection between both PLMNs. The scenario also covers messages initiated by PLMN B after the initial connection setup from PLMN A to PLMN B.

Table 1 shows the situation that PLMN A has 2 PLMN IDs and one SEPP.

	MCC	MNC
PLMNID1	999	888
PLMNID2	999	777

Table 8 - PLMN has 2 PLMN IDs and one SEPP

Table 2 shows the situation that PLMN B has 2 PLMN IDs and 2 SEPPs, each SEPP can handle both PLMN IDs.

	MCC	MNC
PLMNID1	001	001
PLMNID2	001	002

Table 9 - PLMN has 2 PLMN IDs and 2 SEPPs, each SEPP can handle both PLMN IDs

In order to illustrate the different aspects of the connection setup it is assumed that the initial message from the NF in PLMN A targets the NF in PLMN B associated with the secondary PLMN ID of PLMN B.

The N32 connection can be established at the time of provisioning (i.e. not as a result of the initial message mentioned above). The alternative of setting up the connection on the first message from PLMN A to PLMN B only impacts the way in which the well-known FQDN is obtained (i.e. 3gpp-Sbi-Target-ApiRoot header).

B.3 Call flows

B.3.1 N32 Connection Setup

The N32 connection setup passes the following steps with the sample call flows described in the following subsections B.3.2 – B.3.4.

- Dynamic SEPP discovery (optional)
- TLS connection setup (prerequisite for n32-c and n32-f connection setup)
- N32-c connection setup
- N32-f connection setup

B.3.2 Dynamic SEPP discovery

It is assumed that a DNS client within the SEPP takes care of the DNS queries either directly or through a local DNS cache. The DNS client does not make any decisions on next steps but returns the result of each query to the SEPP application layer.

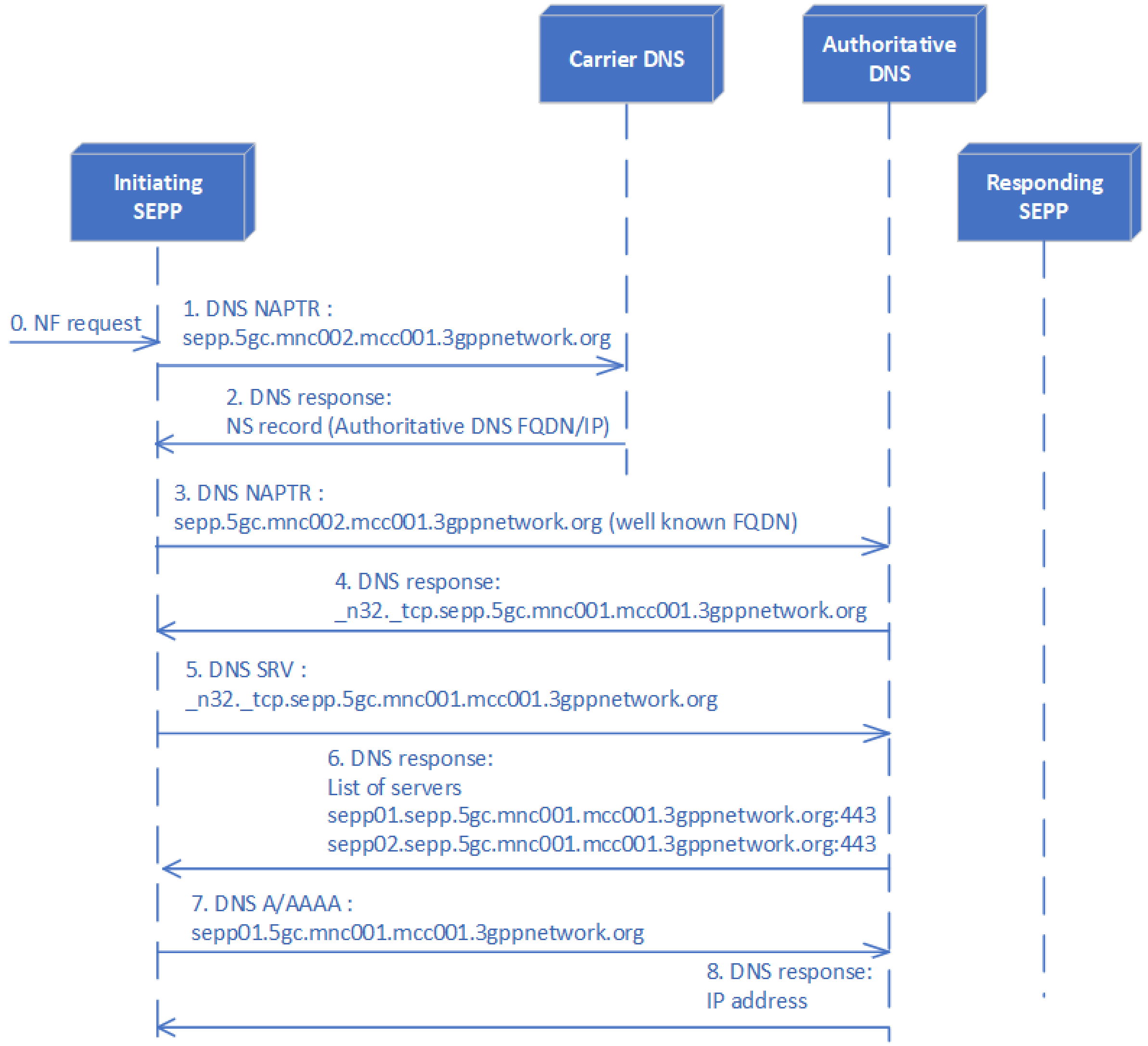

Carrier DNS
Authoritative DNS
Initiating SEPP
Responding SEPP
0. NF request
1. DNS NAPTR :
sepp.5gc.mnc002.mcc001.3gppnetwork.org
2. DNS response:
NS record (Authoritative DNS FQDN/IP)
3. DNS NAPTR :
sepp.5gc.mnc002.mcc001.3gppnetwork.org (well known FQDN)
4. DNS response:
_n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org
5. DNS SRV :
_n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org
6. DNS response:
List of servers
sepp01.sepp.5gc.mnc001.mcc001.3gppnetwork.org:443
sepp02.sepp.5gc.mnc001.mcc001.3gppnetwork.org:443
7. DNS A/AAAA :
sepp01.5gc.mnc001.mcc001.3gppnetwork.org
8. DNS response:
IP address

Figure 39 - Dynamic SEPP Discovery

The SEPP application layer decides on the next DNS query to be sent (refer to section 4.19 of IR.67 [10]).

0. The i-SEPP obtains from its local configuration the well-known FQDN of PLMN B. If the connection is established on the first message towards PLMN B, the 3gpp-Sbi-

Target-ApiRoot header in the message is used to construct a well-known FQDN based on the PLMN ID within the 3gpp-Sbi-Target-ApiRoot header. In addition, the PLMN ID is used to select a trust anchor for verifying the TLS server certificate chain. Example:

3gpp-Sbi-Target-ApiRoot	Well-known FQDN
nrf.5gc.mnc002.mcc001.3gppnetwork.org	sepp.5gc.mnc002.mcc001.3gppnetwork.org

1. The i-SEPP sends a DNS NAPTR query to the IPX Secondary Root DNS (IR.67 [10] section 2.2) using the well-known FQDN (i.e., sepp.5gc.mnc002.mcc001.3gppnetwork.org).

NOTE: This step is optional and only used to discover the DNS of the target PLMN. The DNS IP of the target PLMN can also be obtained from IR.21, the i-SEPP proceeds with step 3. If the DNS cache contains an entry for the well-known FQDN, the i-SEPP proceeds with step 5.

2. The IPX Secondary Root DNS returns an NS record containing the FQDN and IP of the authoritative DNS.

3. The i-SEPP sends the same DNS NAPTR query as in step 1 to the authoritative DNS of PLMN B.

4. The DNS server returns one or more NAPTR records containing the domain name of the N32 service. Note that the mnc/mcc value of the returned domain can be different from the mnc/mcc in the well-known FQDN. The goal is to allow the PLMN to use the same SEPP (FQDN) for multiple PLMN IDs.

```
sepp.5gc.mnc002.mcc001.3gppnetwork.org. 14400 IN NAPTR  50 100 “s” “x-3gpp-sepp:x-n32c”  “” _n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org
```

5. The i-SEPP selects one of the available NAPTR records based on the needed service and sends a DNS SRV query to the authoritative DNS using the selected domain.

   (i.e., _N32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org). Note: if the DNS cache contains an entry for the selected record, the i-SEPP proceeds with step 7.

6. The DNS returns one or more SRV records indicating the SEPP topology of PLMN B. The SRV records contain a priority and weight to allow the i-SEPP to select a responding SEPP (r-SEPP) (Ref.: RFC 2782 [16]), and the FQDN and ports to be used to establish N32-c to each r-SEPP. (Details for N32-f are described below)

```
                                                  TTL class SRV priority weight port target.

_n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org.  600 IN    SRV 10       60     443  sepp1.sepp.5gc.mnc001.mcc001.3gppnetwork.org.
_n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org.  600 IN    SRV 10       20     443  sepp2.sepp.5gc.mnc001.mcc001.3gppnetwork.org.
```

7. The i-SEPP selects one or multiple r-SEPPs based on the available SRV records. If multiple r-SEPPs are selected, the i-SEPP shall set up N32 connections to each selected r-SEPP to allow load balancing of traffic. Details on how and when peer SEPPs are discovered and how traffic can be load balanced are described in detail in IR.67. The i-SEPP sends a DNS A/AAAA query to resolve the IP address of the

selected r-SEPP or r-SEPPs. For this document it is assumed one r-SEPP is selected.

NOTE: If the DNS cache contains an entry for the selected FQDN, the DNS A/AAAA query is skipped.

8. The DNS returns an A/AAAA record with the correct IP address.

NOTE: If the DNS server is configured so that the IP addresses are already returned in step 6 then step 8 can be skipped.

B.3.3 TLS Connection Setup

Once an r-SEPP is dynamically discovered or obtained from static configuration, the i-SEPP can initiate TLS connection setup. The mTLS connection setup is the prerequisite for initiating n32-c and n32-f.

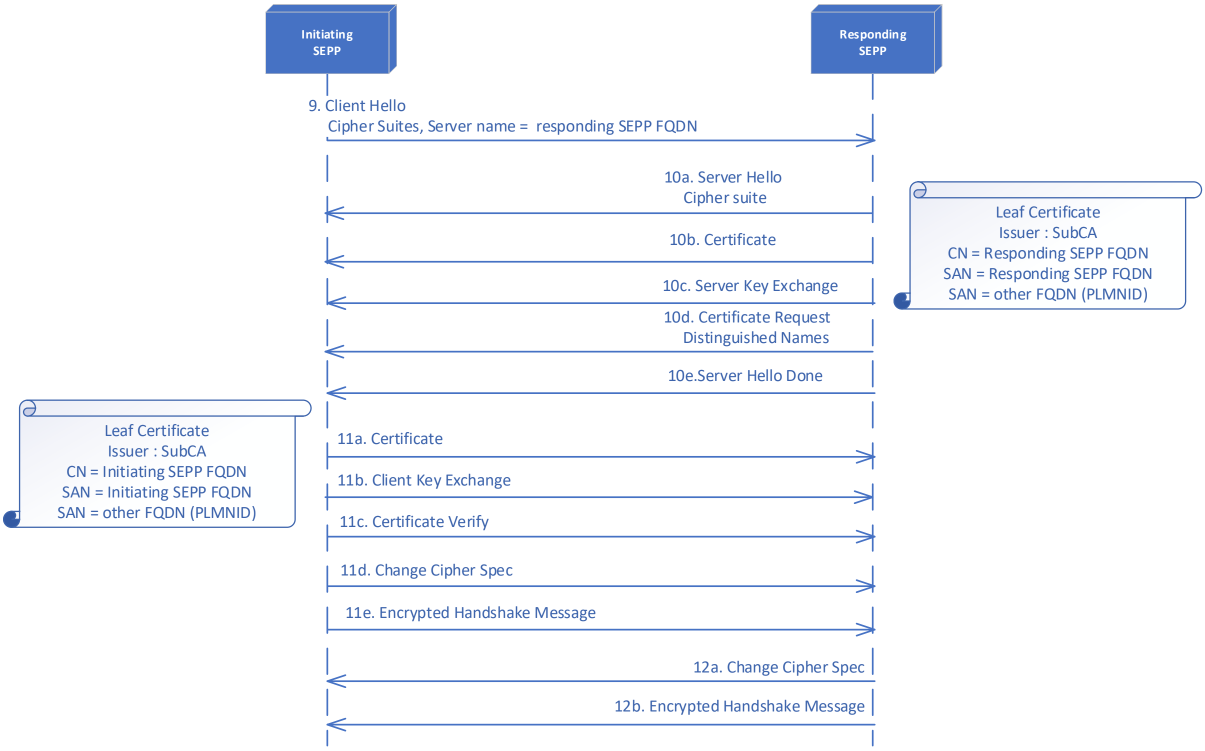


Figure 40 - TLS Handshake

The mTLS handshake procedure (RFC8446) is the same for n32-c and n32-f. However, the FQDNs and certificates used might differ.

9. The i-SEPP sets up a TCP connection to the r-SEPP and sends a TLS client Hello to initiate the TLS handshake indicating the supported cipher suites and adds the selected r-SEPP FQDN(s) to the SNI extension.

10. The r-SEPP responds according to the TLS protocols, selects its TLS server certificate (if it has multiple certificates it uses the SNI field to select one) and sends the selected leaf certificate to the i-SEPP. This leaf certificate is signed by the subCA certificate of the respective PLMN. The subCA certificate is signed by the root CA of the respective PLMN. During certificate exchange, the certificate chain up to but not

including the root CA shall be sent. The leaf (server) certificate contains all applicable Fully Qualified Domain Names (FQDNs) in Subject Alternative Name (SAN) fields as Domain Name System (DNS) name. The SAN fields shall also contain all PLMN IDs for which the SEPP intends to use the N32 connection E.g.

```
SAN
DNS         sepp1.sepp.5gc.mnc001.mcc001.3gppnetwork.org
DNS         sepp1.sepp.5gc.mnc002.mcc001.3gppnetwork.org
```

NOTE: For more certificate formatting and signing information please refer to FS.34.

While it is expected that the r-SEPP will typically include all the PLMN IDs managed by the PLMN in its server certificate, it may choose to use separate N32 connections for different subsets of PLMN IDs, and this is to be reflected in the certificates.

The PLMN IDs in the SAN records shall be kept being crosschecked against the PLMN IDs in the N32-c handshake (B.3.4.1).

The r-SEPP proceeds with the TLS handshake (10c) and requests the client’s certificate (10d). The r-SEPP may indicate which Root CAs it trusts.

At this stage the r-SEPP has no knowledge yet about the identity of the i-SEPP.

The i-SEPP matches the PLMN ID of the well-known FQDN to the SAN records. If the PLMN ID is not found in any of the SAN records, the certificate validation shall fail and the TCP connection shall be torn down. Similarly, the i-SEPP matches the FQDN selected in step 7 (B.3.2) to the SAN records received from the r-SEPP. If the FQDN is not found (exact string match, case-insensitive) in any of the SAN records the certificate validation shall fail and the TCP connection shall be torn down.

The i-SEPP further extracts the PLMN ID from each of the SAN records. All PLMN IDs in the SAN records shall map to the same corresponding trust anchor selected in step 0. The certificate chain received from the r-SEPP shall be verified against the list of Root CAs in the trust anchor. If chain verification fails, the TLS handshake fails with error code 48 (unknown_ca). (Ref.: 3GPP TS 33.501 [19], clause 13.1.2).

11. The i-SEPP sends its TLS client certificate (11a) to the r-SEPP with its FQDN in the SAN records, with an additional FQDN for each of its supported PLMN IDs.

```
SAN
DNS         sepp1.sepp.5gc.mnc888.mcc999.3gppnetwork.org
DNS         sepp1.sepp.5gc.mnc777.mcc999.3gppnetwork.org
```

Only from this moment the r-SEPP is aware of the identity of the i-SEPP.

The i-SEPP shall send its keys (11b) and the certificate verification result (11c) to the r-SEPP.

The r-SEPP performs the same security checks as in step 10. More precisely, the r-SEPP shall check:

- That at least one SAN entry in the client TLS certificate contains a PLMN ID

- For any given SAN record with an encoded PLMN ID it holds that the PLMN ID maps to the same trust anchor as the PLMN IDs encoded in all other SAN records. This trust anchor is then "selected".
- The client TLS certificate chain is anchored at one of the root CAs included in the selected trust anchor.

If any of the checks fails, the TLS handshake fails with error code 48 (unknown_ca).

11d – 12b: the bidirectional Change Cipher Spec and Encrypted handshake complete the mTLS handshake.

B.3.4 N32 Connection

B.3.4.1 N32-c Handshake

The N32-c handshake is used to establish the N32-f connection between two endpoints represented as FQDN. The N32-c context can be used to correlate N32-f connections (set up afterwards) with the correct N32-c connection, i.e. the parent N32-c context for TLS security. This is needed for tearing down N32-f connections, and for identifying N32-f connections used for a specific PLMN when the SEPP or roaming intermediary supports serving multiple PLMNs. An N32-f context consists of a pair of endpoints represented by FQDN of i-SEPP and FQDN of r-SEPP) and optionally the N32 Handshake ID.

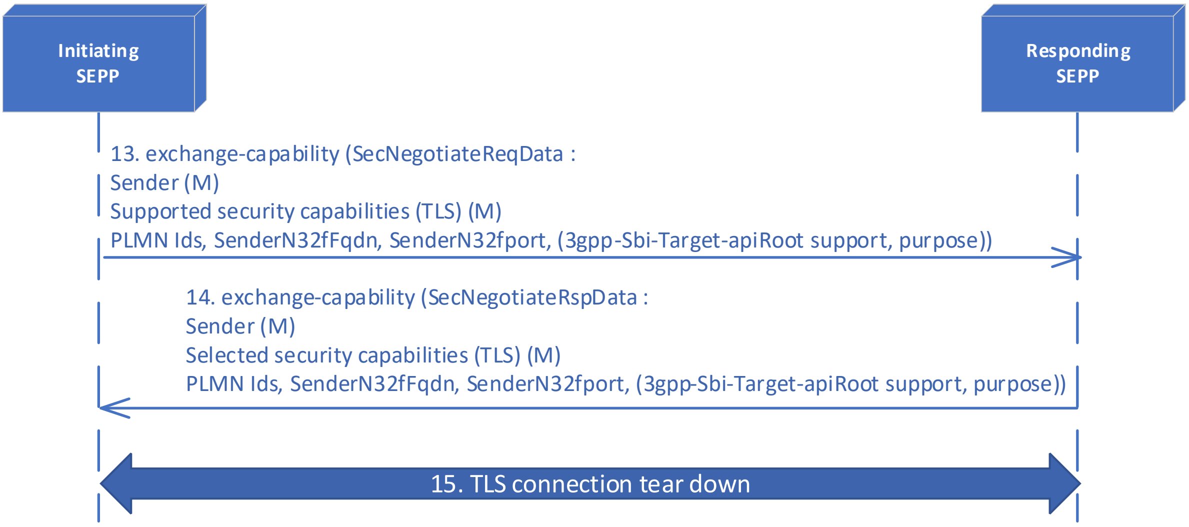

Initiating SEPP
Responding SEPP
13. exchange-capability (SecNegotiateReqData :
Sender (M)
Supported security capabilities (TLS) (M)
PLMN Ids, SenderN32fFqdn, SenderN32fport, (3gpp-Sbi-Target-apiRoot support, purpose))
14. exchange-capability (SecNegotiateRspData :
Sender (M)
Selected security capabilities (TLS) (M)
PLMN Ids, SenderN32fFqdn, SenderN32fport, (3gpp-Sbi-Target-apiRoot support, purpose))
15. TLS connection tear down

Figure 41 - N32-c Handshake

13. Within the previously established mTLS tunnel the i-SEPP sends an http/2 n32-c exchange capability message to the r-SEPP. The “:authority” header is set to the r-SEPP FQDN.

    The SecNegotiateReqData contains the FQDN of the i-SEPP in the Sender IE (sepp01.sepp.5gc.mnc888.mcc999.3gppnetwork.org) and indicates TLS in the Supported security capability IE. Assuming that the following checks succeed, the Sender IE shall be used by the r-SEPP to uniquely identify the i-SEPP and to build an N32-f context consisting of the i-SEPP FQDN and r-SEPP FQDN pair.

The sender PLMN IDs (IE = plmnIdList) and target PLMN ID shall be sent.

If the plmnIdList IE is missing, the r-SEPP shall respond with an appropriate 4xx/5xx status code. If any of the PLMN IDs in the plmnIdList IE or the Sender IE does not match the PLMN IDs in the SAN records of the TLS certificate of the i-SEPP, then further actions shall be taken according to operator policy. Likewise, if the PLMN IDs in the plmnIdList IE or the Sender IE do not belong to the same and correct organisation according to IR.21 information, further action shall be taken according to operator policy.

If the i-SEPP wants incoming N32-f connections to be set up to a different FQDN and/or port, the i-SEPP can indicate this in the SenderN32fFqdn and/or SenderN32fPort IEs as specified in 3GPP Release 18 29.573 [10].

The i-SEPP may also add the n32HandshakeId. If supported by the r-SEPP it shall be used by the r-SEPP in all N32-f forwarded messages.

All the received IEs are stored within the N32-f context on the r-SEPP.

14. The SecNegotiateRspData from the r-SEPP contains the FQDN of the r-SEPP in the Sender IE and TLS in the Selected security capability. The Sender IE shall be used by the i-SEPP to uniquely identify the r-SEPP and to build an N32-f context consisting of the i-SEPP FQDN and r-SEPP FQDN pair.

    The sender PLMN IDs (IE = plmnIdList) shall be sent. If the plmnIdList is missing the connection shall be torn down. (Note: the i-SEPP cannot respond with an error code since it is the HTTP client.) If any of the PLMN IDs in the plmnIdList IE or the Sender IE does not match the PLMN IDs in the SAN records of the TLS certificate of the r-SEPP, then further actions shall be taken according to operator policy. Likewise, if the PLMN IDs in the plmnIdList IE or the Sender IE do not belong to the same and correct organisation according to IR.21 information, further action shall be taken according to operator policy.

    If the r-SEPP wants incoming N32-f connection to be set up to a different FQDN and/or port, the r-SEPP can indicate this in the SenderN32fFqdn and/or SenderN32fPort Is as specified in 3GPP Release 18 29.573 [10].

    All the received IEs are stored within the N32-f context on the i-SEPP.

    The r-SEPP may also add the n32HandshakeId. If supported by the i-SEPP it shall be used by the i-SEPP in all N32-f forwarded messages.

15. Once the N32-c handshake has concluded, the mTLS connection shall be torn down.

B.3.4.2 N32-f Connection setup

After the N32-c handshake a long lived mTLS connection may be initiated from i-SEPP in PLMN A to r-SEPP in PLMN B, for NF service requests sent from PLMN A to PLMN B. Subsequently another long lived mTLS connection may be initiated from PLMN B to PLMN A for NF service requests sent in another N32-f connection from PLMN B to PLMN A. The N32-f connection from PLMN B to PLMN A is optional and will only be set up if NF service requests have to be sent. If the pair of SEPPs in PLMN A and PLMN B is the same as for the initial N32-f mTLS connection the secondary N32-f mTLS connection will be part of the same N32-f context and no new N32-c handshake is required.

Support of SenderN32fFQDN and SenderN32fPort is indicated during the N32-c handshake procedure by setting the relevant flag for the SNDN32F in the supported Features attribute. If either SEPP does not support the feature, the same FQDN as for the N32-c handshake and, the default destination port (443) or locally configured port, is used to set up the TLS connection for N32-f. See also section 4.1.1.

NOTE: The use of SenderN32fFQDN and SenderN32fPort was introduced in Rel.18.

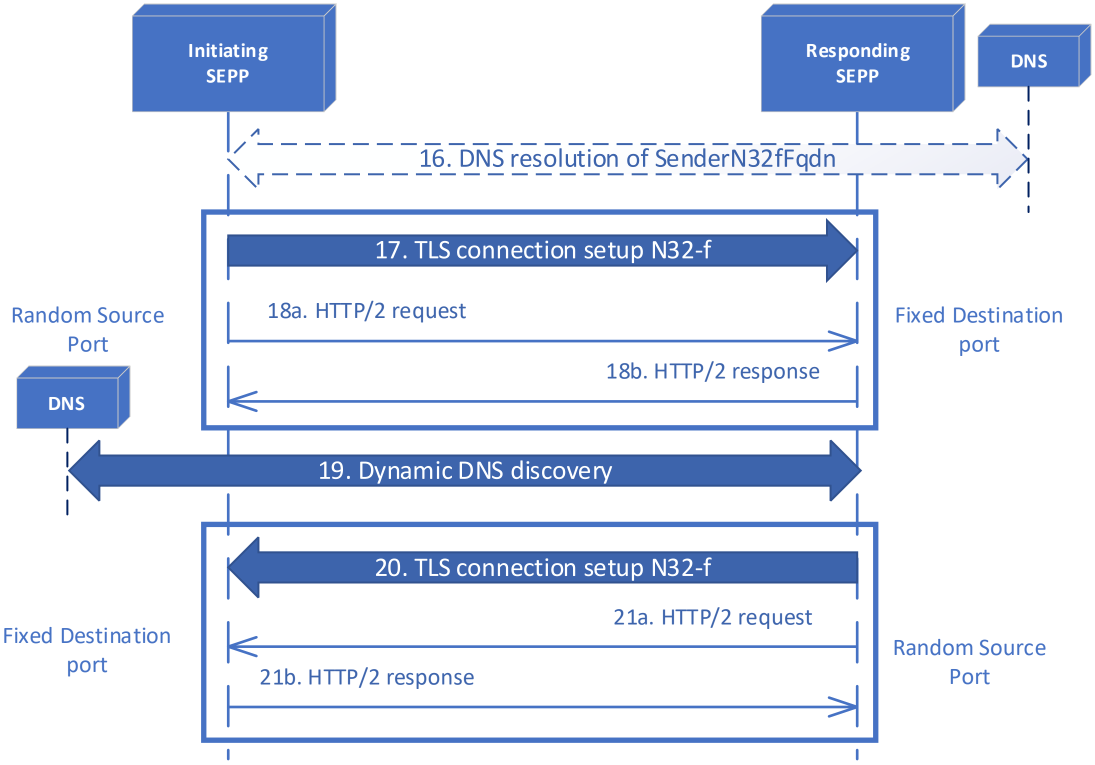


Figure 42 - N32-f connection establishment

16. If the SenderN32fFqdn and/or SenderN32Port were provided by the r-SEPP (and are different from the N32-c FQDN and/or Port) the supporting i-SEPP shall initiate a new DNS A/AAAA query to the authoritative DNS to retrieve the corresponding IP address.

    If the SenderN32fFqdn and/or SenderN32fPort were not provided by the r-SEPP, the same FQDN and/or port as used for the N32-c Handshake shall be used by the i-SEPP unless the N32-f port has been locally configured on the i-SEPP.

17. The same procedure and security checks as defined in B.3.3 shall be used to set up a long lived mTLS tunnel from i-SEPP to r-SEPP. If any of the checks fail, further action shall be taken according to operator policy.

    Additionally, if the N32-f certificate contains any PLMN ID which is not present in the corresponding N32-c certificate, then the certificate shall be rejected.

Correlation of the N32-f connection to the N32-c context shall be done following B.3.4.2.1.

18. NF service requests are forwarded within the mTLS connection unchanged. The :authority header will be set to the r-SEPP FQDN (or SenderN32fFQDN if exchanged in the N32-c handshake). The 3gpp-Sbi-Target-ApiRoot header shall be kept as received from the NF (Ref.: 3GPP TS 29.573 [10] section C.2.).

The 3gpp-Sbi-N32-Handshake-Id header shall be set to the n32HandshakeId returned by the r-SEPP during the N32-c handshake.

19. If PLMN B needs to send an NF service request to PLMN A, and has no information from a previous dynamic discovery, it shall initiate the Dynamic discovery procedure as described in B.3.2, to discover the appropriate SEPP. If the selected FQDN matches a previously established N32-f context, then the N32-c handshake shall be skipped. If the selected FQDN does not match any previously established N32-f context, then a new N32-c handshake shall be initiated, creating a new N32-f context.

NOTE: The NF service request can be notifications for implicit or explicit subscriptions, or inter-PMN service requests initiated by NFs in PLMN B.

20. The same procedure and security checks as defined in B.3.3 shall be used to set up a long-lived TLS tunnel from r-SEPP to i-SEPP. If any of the checks fail, further action shall be taken according to operator policy.

    Additionally, if the N32-f certificate contains any PLMN ID which is not present in the corresponding N32-c certificate, then the certificate shall be rejected. (Ref: 3GPP TS 33.501 [19]).

    Correlation of the N32-f connection to the N32-c context shall be done following B.3.4.2.1.

21. NF service requests are forwarded within the mTLS connection unchanged. The ":authority" header will be set to the i-SEPP FQDN (or SenderN32fFQDN if exchanged in the N32-c handshake). The 3gpp-Sbi-Target-ApiRoot header shall be kept as received from the NF (Ref.: 3GPP TS 29.573 [10] section C.f2.).

    The 3gpp-Sbi-N32-Handshake-Id header shall be set to the n32HandshakeId returned by the i-SEPP during the N32-c handshake.

B.3.4.2.1 Correlation of N32-f TLS connections to N32-c contexts

Inbound TLS will have to be identified and correlated to the correct N32-c context. When TLS connection is set up there is no indication if this is a short-lived TLS connection for N32-c handshake procedures or a long-lived TLS connection for N32-f message exchange.

The way correlation is done depends on the number of contexts per pair of SEPPs, use of shared certificates and negotiated handshake IDs and purpose. For inbound TLS connections a decision tree will have to be followed and if in the end correlation cannot be achieved the N32-f TLS connection shall be rejected or closed.

The SEPP shall use the FQDNs in the SAN fields of the certificate provided by the peer SEPP to correlate the inbound mTLS connection to the corresponding N32-c context. Each FQDN in the SAN fields shall be compared (case-insensitive) to the Sender IE or SenderN32fFQDN IE in all active contexts. If all FQDNs in the SAN fields map to the same N32-c context then correlation is accomplished.

If multiple N32-c contexts were identified as potentially matching, the correlation can only be done based on the first HTTP message on this connection.

If the certificate SAN records contain FQDNs of different SEPPs (e.g. shared certificates) then the “Via” header in the first message shall be used to identify the peer SEPP and corresponding context(s).

If multiple contexts have been negotiated between the same pair of SEPPs (e.g. for different purposes) and a n32HandshakeId was exchanged in the N32-c handshake procedure, the “3gpp-Sbi-N32-Handshake-Id” header in the first message shall be used to identify the N32-c context.

If the handshake ID was not negotiated and the intendedUsagePurpose was provided during the N32-c handshake then the “3gpp-Sbi-Interplmn-Purpose” header in the first message shall be used to identify the N32-c context.

If the TLS connection cannot be uniquely correlated to an existing context and the first message is not an N32-c exchange capability message, then the connection shall be closed with an error message.

NOTE1: The usage of different purposes between PMNs is for further study and not explored in this version of the document.

NOTE2: If the context can only be correctly identified after the first message, any additional security checks for (e.g. PLMN ID check) will have to be deferred until the first message arrives.

Editor’s Note: The error message to be used if correlation is not possible is ffs.

B.3.4.3 N32 Termination

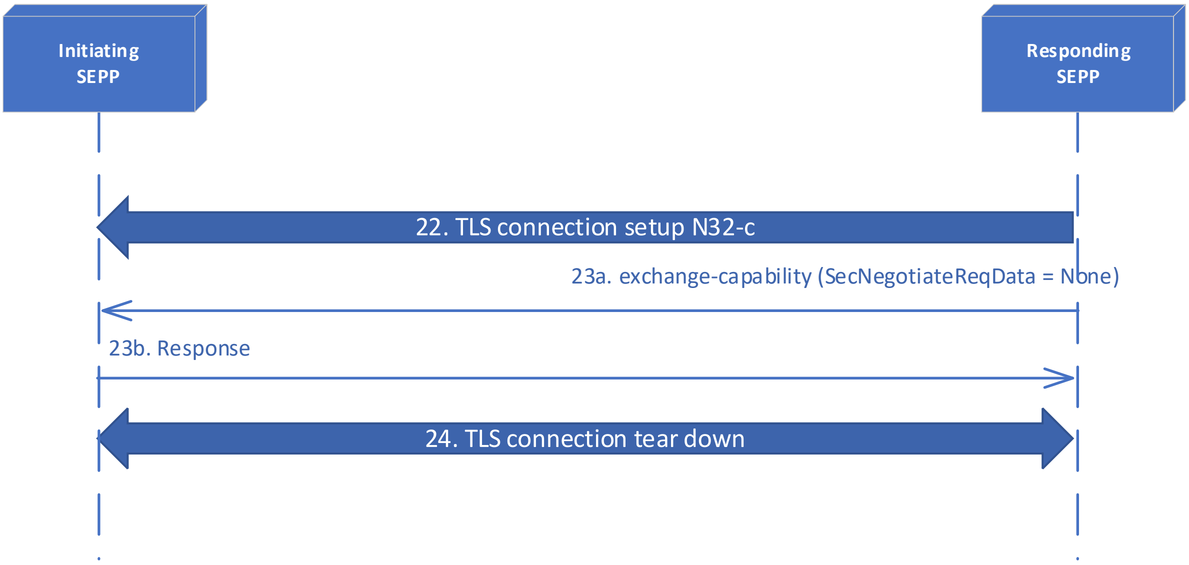

Initiating SEPP
Responding SEPP
22. TLS connection setup N32-c
23a. exchange-capability (SecNegotiateReqData = None)
23b. Response
24. TLS connection tear down

Figure 43 - N32 connection termination

Either side can terminate the context and associated n32-f TLS connections.

22. The SEPP wishing to terminate the context opens a short-lived TLS connection according to B.3.3.

    Correlation of the N32-f connection to the N32-c context shall be done following B.3.4.2.1.

23. The SEPP initiates an N32-c handshake. The SecNegotiateReqData shall contain “supported security capability” set to NONE (Ref.: TS 29.573 [10] section 5.2.2). This triggers each SEPP to release the N32-f context and tear down the corresponding n32-f connections.

    The 3gpp-Sbi-N32-Handshake-Id header shall be set to the n32HandshakeId returned by the peer SEPP during the N32-c handshake.

24. The N32-c TLS connection is torn down.

B.3.4.4 Race Conditions and Recovery

This section describes two situations. First when two peer SEPPs send an N32 exchange capability message at the same time to each other (Race condition). Second when a SEPP receives a new N32 exchange capability exchange message for a previously established N32-f context (Recovery).

It is assumed that between any pair of SEPPs there will only be one N32-f context.

B.3.4.4.1 Race Condition

If a SEPP sends an N32 exchange capability message and receives an N32 exchange capability message before it receives a response, it shall compare the FQDNs in the Sender IEs. The SEPP whose FQDN lexicographically precedes the FQDN of the other SEPP shall proceed with the initiated procedure and reject the incoming exchange capability message with the appropriate error cause (Ref: 3GPP 29.573 [10], section 5.2.2). The SEPP where the FQDN does not precede the FQDN of the other SEPP shall stop its initiated connection establishment and proceed by responding to the incoming exchange capability message.

B.3.4.4.2 Recovery

If a SEPP receives an N32 exchange capability message from a peer SEPP for which it already has an active N32-f context, it will:

- Stop sending any new messages on the related N32-f connection
- Delete the existing context and close any N32-f connections related to this context.
- Process the received N32 exchange capability request

(Ref: 3GPP 29.573 [10], section 5.2.2)

B.3.4.5 N32-f Lifetime

Editor's Note: This section is for further study.

The N32-f lifetime is under control of the client initiating the N32-f connection. It is expected that N32-f is a long-lived connection which is kept active even if there is no traffic to be sent.

Several methods are available to keep the connection alive when there is no traffic to be sent. Since TCP Keep-alive uses standard TCP/IP functionality nothing specific is needed from a server to respond to TCP keep-alive packets. Other methods can optionally be used to monitor the connection if supported by both peers.

- TCP keep-alive. (Mandatory)
- TLS Heartbeat (Optional)
- HTTP2 PING Frame (Optional)

If the peer SEPP does not acknowledge a packet before the timeout expires, the following actions should be taken.

a) Re-initialization of the N32-f TLS connection only

b) If this fails, re-initialization of N32-f context

If any of the optional heartbeat methods are used, the recovery actions to be taken are not defined in this document and are subject to operator policy and mutual agreement between peers.

B.4 Trust Anchors

Ref: 3GPP TS 33.501 [19] section 13.1.2

The SEPP shall maintain a set of trust anchors, each entry consisting of a list of trusted root certificates and a list of corresponding PLMN-IDs. Lists of PLMN IDs and lists of root certificates are related by the trust anchor they belong to. Any given PLMN ID can only appear in one trust anchor. Root certificates can appear in multiple trust anchors.

```
{

Trust Anchor A :

(PLMN ID 1, PLMN ID 2, …..)

(Root CA 1 certificates, Root CA 2 certificates,…..)

,

Trust Anchor B:

(PLMN ID 3, PLMN ID 4, …..)

(Root CA 1 certificates, Root CA 4 certificates,…..)

,

…

}
```

Annex C Detailed design for inter-PLMN connection with Hosted or Group SEPP

This detailed design is introduced by this document. It is based on an extension of the N32 protocol developed in the GSMA.

C.1 Introduction

This annex describes the N32s connection setup between a PLMN SEPP and a Service Provider (SP) SEPP, acting as a Hosted or Group SEPP on behalf of the PLMN. Refer to Hosted or Group SEPP (model 2) in sections 4.2.3 and 4.3.2. This annex covers the deployment scenario with dynamic SEPP discovery, N32s-c handshake and N32s-f connection setup and termination. For the sake of clarity, the call flows do not show all parameters but only certain examples where relevant.

The N32s connection setup between the PLMN SEPP and a Hosted or Group SEPP deviates from the bilateral direct N32 connection setup by the fact that the Hosted or Group SEPP does not represent the roaming destinations but is used as a route to get there.

C.2 Call Flows

C.2.1 N32s Connection Setup

The N32s connection setup passes the following subsequent steps with sample call flows in subsections C.2.2 – C.2.5.

- Dynamic SEPP discovery
- TLS connection setup and N32s-c handshake
- N32s-f connection setup

- N32s-f connection termination

C.2.2 Dynamic SEPP discovery

Both PLMN SEPP and SP SEPP can start the process to discover each other. The FQDN used for dynamic SEPP discovery will however be different from the well-known FQDN constructed using PLMN IDs (mcc and mnc):

- The PLMN SEPP may use an agreed-upon FQDN from the Service Provider's domain which is unique to the PLMN. This shall yield the hosted SEPP's private N32 interface (SP or n32s reference point in NG.113 Hosted or Group SEPP model).
- The Hosted or Group SEPP may use an agreed-upon FQDN from the PLMN's domain which is unique to the Service Provider. This shall yield the PLMN SEPP's private N32 interface (n32s).

Note that SEPP discovery by the PLMN's roaming partners using the well-known FQDN constructed with PLMN's ID shall yield the Hosted or Group SEPP's public N32 interface (HS or Group SEPP).

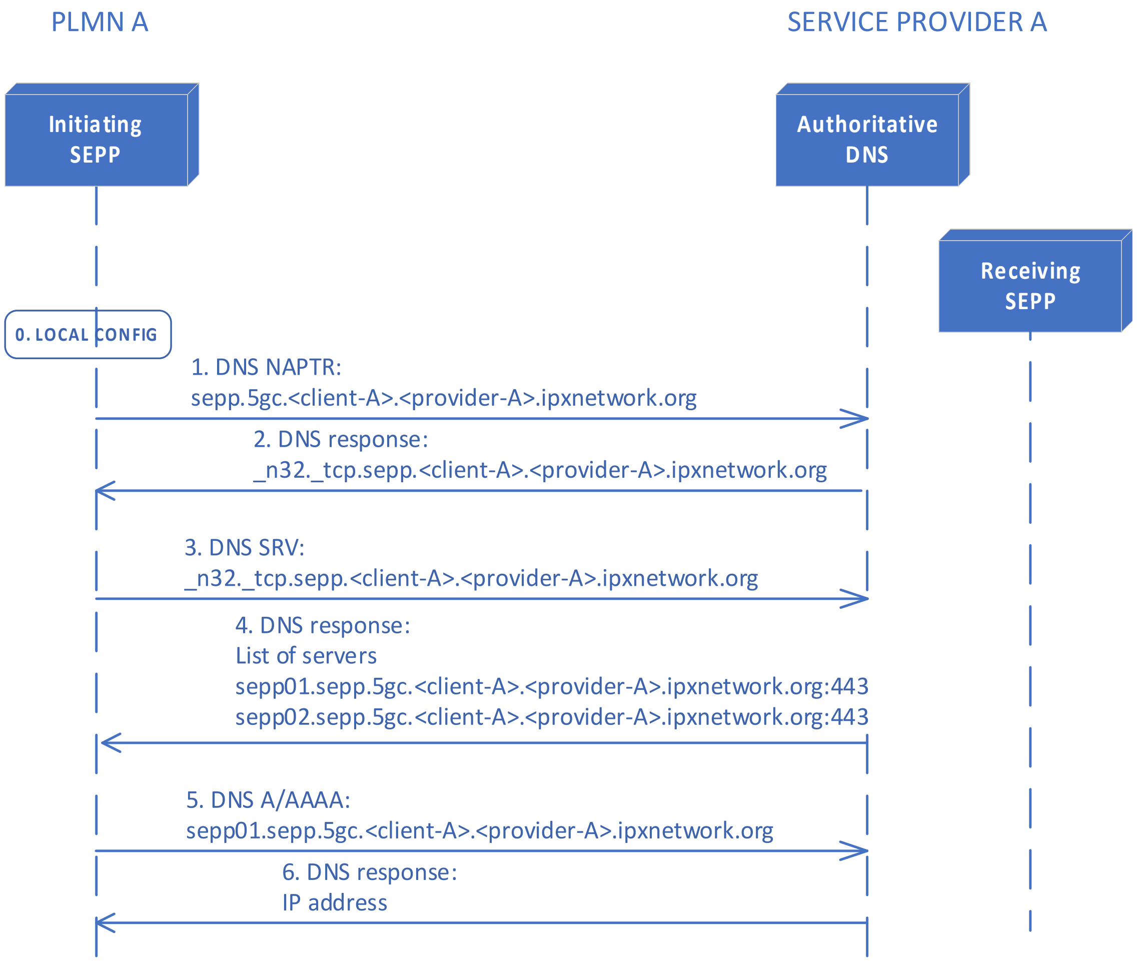

PLMN A
SERVICE PROVIDER A
Initiating SEPP
Authoritative DNS
Receiving SEPP
0. LOCAL CONFIG
1. DNS NAPTR:
sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org
2. DNS response:
_n32._tcp.sepp.<client-A>.<provider-A>.ipxnetwork.org
3. DNS SRV:
_n32._tcp.sepp.<client-A>.<provider-A>.ipxnetwork.org
4. DNS response:
List of servers
sepp01.sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org:443
sepp02.sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org:443
5. DNS A/AAAA:
sepp01.sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org
6. DNS response:
IP address

Figure 44 - Dynamic SEPP Discovery of Hosted or Group SEPP

In the call flow above, it is assumed that PLMN A SEPP acts as initiating SEPP (i-SEPP) and performs the SEPP discovery process. A DNS client within the i-SEPP takes care of the DNS queries either directly or through a local DNS cache. The DNS client does not make any decisions on next steps but returns the result of each query up to the SEPP application layer. The SEPP application layer decides on the next DNS query to be sent. (Also see section 4.19 of IR.67 [8])

0. It is assumed the initiating SEPP (i-SEPP) has local config for the PLMN ID of the roaming destination, indicating the next hop FQDN. The 3gpp-Sbi-Target-ApiRoot header in a received NF service request message is used to derive the PLMN ID. The next hop FQDN points to the Service Provider's Hosted or Group SEPP instance for PLMN A. Example:

   3gpp-Sbi-Target-ApiRoot: nrf.5gc.mnc002.mcc001.3gppnetwork.org

   Local configuration (pre-provisioned):

PLMNID	Next hop FQDN
001002	sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org

1. The i-SEPP sends a DNS NAPTR query using the next-hop FQDN from local config to the authoritative DNS of Service Provider A. Interaction with a carrier DNS to determine the authoritative DNS of Service Provider A is not shown for simplicity's sake.

2. The DNS server returns one or more NAPTR records containing the domain name of the N32 service. Note that the domain name of the N32 service should match the original service provider's domain (i.e. <provider-A>.ipxnetwork.org).

```
sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org.  14400  IN  NAPTR   50  100  "s"  "x-3gpp-sepp:x-n32c"    ""  _n32._tcp.sepp.5gc.<client-A>.<provider-
A>.ipxnetwork.org
```

3. The i-SEPP selects one of the records received in step 2 based on the needed service and sends a DNS SRV query to the authoritative DNS using the selected domain. (i.e., _N32._tcp.sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org).

NOTE: If the DNS cache contains an entry for the selected record, the DNS SRV query is skipped.

4. The DNS returns one or more SRV records indicating the available SEPPs of Service Provider A. The SRV records contain a priority and weight to allow the i-SEPP to select a responding SEPP (r-SEPP) (Ref.: RFC 2782 [16]), and the FQDN and ports to be used to establish N32-c to each r-SEPP.

```
                                                TTL class SRV priority weight port target.

_n32._tcp.sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org.  600 IN    SRV 10       60     443  sepp1.sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org.

_n32._tcp.sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org.  600 IN    SRV 10       20     443  sepp2.sepp.5gc.<client-A>.<provider-A>.ipxnetwork.org.
```

5. The i-SEPP selects one or multiple r-SEPPs based on the received SRV records. If multiple r-SEPPs are selected, the i-SEPP shall set up N32s connections to each

selected r-SEPP to allow load balancing of traffic. The i-SEPP sends a DNS A/AAAA query to resolve the IP address of the selected r-SEPP or r-SEPPs. In the example call flow it is assumed only one r-SEPP is selected.

NOTE: If the DNS cache contains an entry for the selected FQDN, the DNS A/AAAA query is skipped.

6. The DNS returns an A/AAAA record with the correct IP address.

NOTE: Glue records can be used in the DNS so that the IP addresses are already returned in step 4 avoiding the need for steps 5 and 6.

NOTE: If the DNS server is configured so that the IP addresses are already returned in step 4 then step 6 can be skipped.

C.2.3 TLS Connection Setup for n32s-c

Once the service provider's SP SEPP FQDN, IP and port are obtained from the dynamic SEPP discovery process, the mTLS handshake procedure can be initiated.

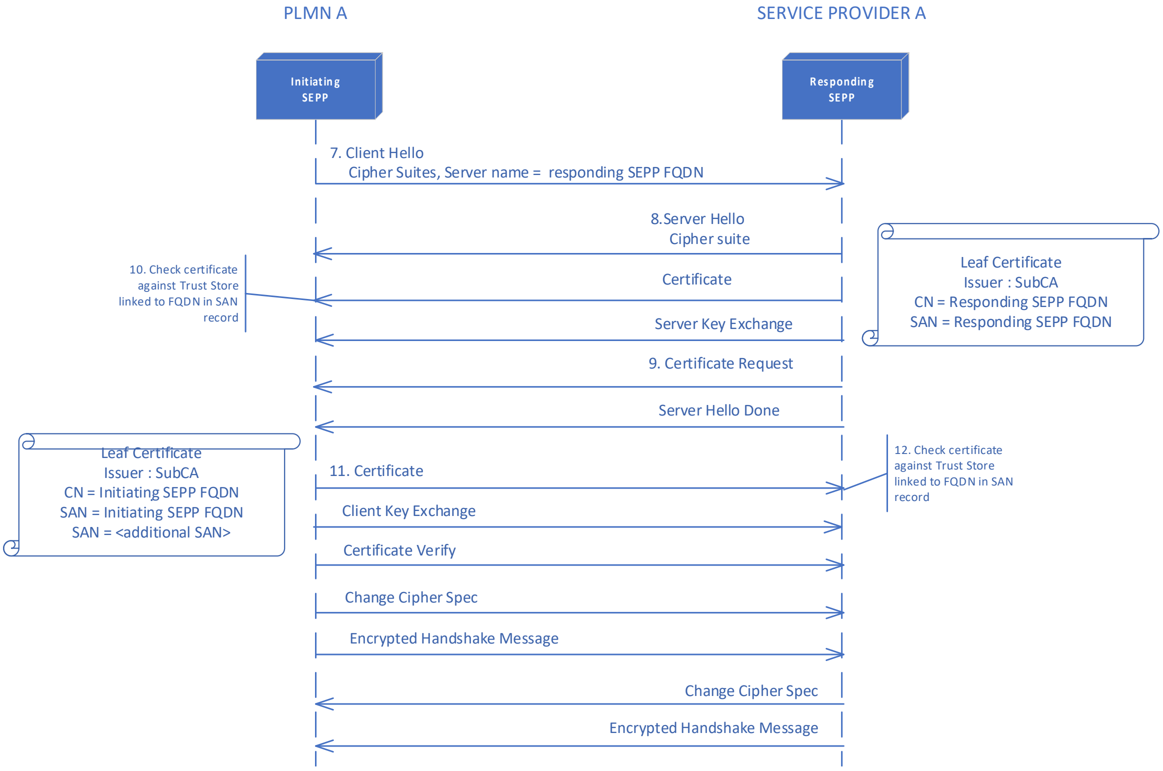

PLMN A
SERVICE PROVIDER A
Initiating SEPP
Responding SEPP
7. Client Hello
Cipher Suites, Server name = responding SEPP FQDN
8.Server Hello
Cipher suite
Leaf Certificate
Issuer : SubCA
CN = Responding SEPP FQDN
SAN = Responding SEPP FQDN
10. Check certificate against Trust Store linked to FQDN in SAN record
Certificate
Server Key Exchange
9. Certificate Request
Server Hello Done
Leaf Certificate
Issuer : SubCA
CN = Initiating SEPP FQDN
SAN = Initiating SEPP FQDN
SAN = <additional SAN>
12. Check certificate against Trust Store linked to FQDN in SAN record
11. Certificate
Client Key Exchange
Certificate Verify
Change Cipher Spec
Encrypted Handshake Message
Change Cipher Spec
Encrypted Handshake Message

Figure 45 - TLS Handshake

7. The PLMN SEPP (i-SEPP) sets up a TCP connection to service provider SP SEPP (r-SEPP) by sending a TLS client Hello to initiate the TLS handshake. The i-SEPP indicates the supported cipher suites and adds the selected r-SEPP FQDN(s) to the SNI extension.

8. The r-SEPP responds by selecting the appropriate TLS server certificate – if it has multiple certificates it uses the SNI field to select one – and sends it to the i-SEPP.

The leaf (server) certificate contains the r-SEPP FQDN in the Common Name and the Subject Alternative Name (SAN) record. Since the r-SEPP belongs to a service provider, no additional SAN records are required.

9. The r-SEPP proceeds with the TLS handshake and requests the client's certificate. The r-SEPP may indicate which Root CAs it trusts. At this stage the r-SEPP has no knowledge yet about the identity of the i-SEPP.

10. The i-SEPP uses the trailer of the FQDN from the SAN record to find the corresponding trust anchor in the set of trust anchors. The way a search for trust anchor is implemented may be vendor specific. The trust anchor could also be linked to the local configuration of the peer. The certificate chain received from the r-SEPP shall be verified against the list of Root CAs in the trust anchor.

    If chain verification fails, the TLS handshake fails with error code 48 (unknown_ca). (Ref.: 3GPP TS 33.501 [19] chapter 13.1.2)

11. The i-SEPP sends its TLS client certificate to the r-SEPP with its FQDN in the SAN records. The SAN records can contain additional FQDNs with alternative PLMN IDs if the i-SEPP belongs to a PLMN with multiple PLMN IDs.

    Only from this moment the r-SEPP is aware of the identity of the i-SEPP.

    The i-SEPP shall send its keys and the certificate verification result to the r-SEPP.

12. The r-SEPP shall perform the same validation as described in step 10. The bidirectional Change Cipher Spec and Encrypted handshake completes the mTLS handshake.

The N32s-c handshake is used to establish a N32s context (i.e. connection) between 2 endpoints represented as FQDN. An N32s context consists of a pair of endpoints represented by FQDN of i-SEPP and FQDN of r-SEPP).

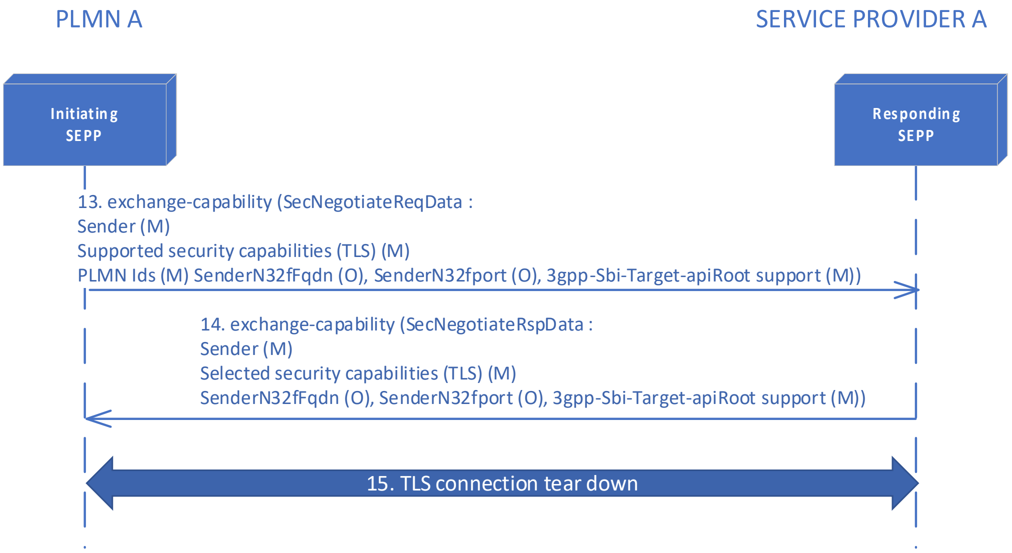

PLMN A
SERVICE PROVIDER A
Initiating SEPP
Responding SEPP
13. exchange-capability (SecNegotiateReqData :
Sender (M)
Supported security capabilities (TLS) (M)
PLMN Ids (M) SenderN32fFqdn (O), SenderN32fport (O), 3gpp-Sbi-Target-apiRoot support (M))
14. exchange-capability (SecNegotiateRspData :
Sender (M)
Selected security capabilities (TLS) (M)
SenderN32fFqdn (O), SenderN32fport (O), 3gpp-Sbi-Target-apiRoot support (M))
15. TLS connection tear down

Figure 46 - N32s-c Handshake

13. Within the previously established mTLS connection, the i-SEPP sends an http/2 n32s-c exchange capability message to the r-SEPP. The ":authority" header is set to the r-SEPP FQDN.

    The SecNegotiateReqData contains the FQDN of the i-SEPP in the Sender IE and indicates TLS in the Supported security capability IE. Assuming that the following checks succeed, the Sender IE shall be used by the r-SEPP to uniquely identify the i-SEPP and to build an N32s context consisting of the i-SEPP FQDN and r-SEPP FQDN pair.

    The sender PLMN IDs (IE = plmnIdList) shall be sent.

    If the plmnIdList IE is missing, the r-SEPP shall respond with an appropriate 4xx/5xx status code. If any of the PLMN IDs does not match the PLMN Ids in the TLS certificate of the i-SEPP, further actions can be taken based on service provider policy.

    The i-SEPP can also add the n32HandshakeId. If supported by the r-SEPP it shall be used by the r-SEPP in all N32-f forwarded messages.

14. The SecNegotiateRspData from the r-SEPP contains the FQDN of the r-SEPP in the Sender IE and TLS in the Selected security capability. The Sender IE shall be used by the i-SEPP to uniquely identify the r-SEPP and to build an N32s context consisting of the i-SEPP FQDN and r-SEPP FQDN pair.

    The plmnIdList IE is not included by the r-SEPP as it is not applicable.

    The r-SEPP can also add the n32HandshakeId. If supported by the i-SEPP it shall be used by the i-SEPP in all N32-f forwarded messages.

15. The mTLS connection is torn down when the n32s-c exchange is concluded.

C.2.4 TLS Connection Setup for n32s-f

This step is the same as for the direct TLS design (see B.3.4.2).

After DNS resolution of the respective Sender IE or SenderN32fFqdn exchanged via n32s-c, mTLS connections for n32s-f can be setup in both directions.

C.2.5 N32s Termination

This step is the same as for the direct TLS design (see B.3.4.3).

Any TLS client can actively terminate the n32s connection.

The server side of a TLS connection may silently drop the connection in absence of any traffic, including TCP keep-alive from the client.

C.2.6 Trust Anchors

Ref: 3GPP TS 33.501 [19] clause 13.1.2

The SEPP shall maintain a set of trust anchors, each consisting of a list of trusted root certificates and a list of corresponding Domain Names. Lists of Domain Names and Lists of

Root certificates are related by the trust anchor they belong to. Any given Domain Name can only appear in one trust anchor. Root certificates can appear in multiple trust anchors.

{

Trust Anchor A :

(PLMN FQDNs)

(Root CA 1 certificates, Root CA 2 certificates,…..)

,

Trust Anchor B:

(Service Provider FQDNs)

(Root CA 1 certificates, Root CA 4 certificates,…..)

,

…

}

Annex D Detailed design for inter-PLMN connection using PRINS

This detailed design is following 3GPP specifications.

D.1 Introduction

This annex describes the inter-PLMN connection setup using the PRINS security mechanism for inter-PLMN connection between a pair of SEPPs. It covers deployment scenarios with dynamic SEPP discovery via DNS, TLS connection setup for n32-c as pre-requisite for the HTTP/2 n32-c handshake, and TLS connection setup for n32-f for the HTTP/2 n32-f message transfer. Note that, while clause 13.1.2 of TS 33.501 [19] stipulates that NDS/IP can also be used, this annex only describes the TLS connection alternative for N32-f.

This design is a generic description for the PRINS architecture, as specified by 3GPP, and applies to deployment models involving Service Hubs and/or Roaming Hubs.

For the sake of clarity, the call flows do not show all parameters but only certain examples where relevant.

The following figure illustrates the security architecture for hubbing when application layer security is applied as described by the high level security architecture in section 4.3.3.

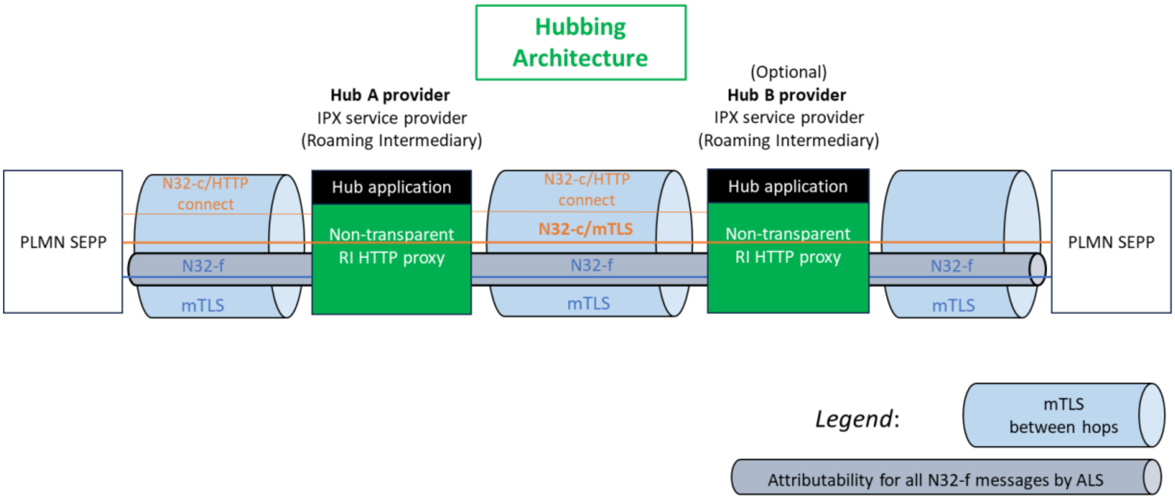


Figure 47- Security architecture for hubbing with application layer security

D.2 High Level Description

An NF in PLMN A wants to send a request to an NF in PLMN B and receive a response from that NF in PLMN B. The SEPPs on either side are responsible to set up and secure the connection between them. The scenario also covers requests sent by PLMN B after connection setup.

In all the described steps and diagrams, it is assumed that PLMN A on the left side initiates the connection setup to PLMN B on the right side, unless explicitly stated otherwise.

The connections between SEPPs and IPX nodes (c/pIPX) rely on the N32 API using the PRINS security method.

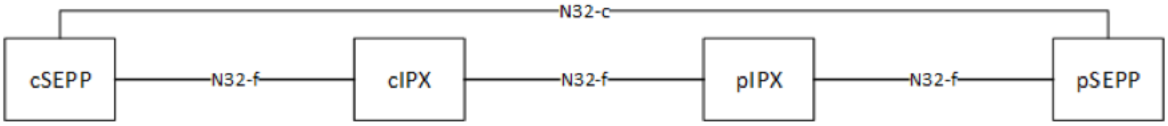


Figure 48 - PRINS Architecture with n32-c and n32-f

It is assumed that SEPPs and IPX nodes setup N32 connections at time of provisioning, rather than on reception of the first NF request towards a target PLMN.

The i-SEPP is the SEPP initiating the N32-c connection. The r-SEPP is the responding SEPP. Depending on the scenario, cSEPP and pSEPP can play both roles: NF requests can flow in both directions, regardless of who initiated the connection.

NOTE 1: PLMN A and PLMN B may have the same IPX provider. In this case the IPX provider has both cIPX and pIPX functional roles. In practice this could mean that the same IPX provider is responsible for the cIPX and pIPX set of patches, according to the service agreement with the respective PLMNs.

NOTE 2: In this Annex, the term "IPX provider" is used synonymously with the term "roaming intermediary”.

D.3 Peering Link

The peering relationship between the two Roaming Intermediaries is not bound to any particular PLMN, but rather to the entire set of PLMNs that are interconnected through the chain. While it is theoretically possible for all PLMNs that are customers of two Roaming Intermediaries of a chain to be pairwise interconnected via the chain, this theoretic maximum is not reached in practice due to contractual reasons. Typically, a given PLMN/customer of an intermediary contracts roaming interconnections only for a subset of other PLMNs that are reachable via the chain, for example because certain territories are already covered by direct (not mediated) roaming connections or via a different intermediary.

The subset of roaming relations that are contractually “enabled” via a chain of two Roaming Intermediaries are said to be “opened” at any given point in time. These roaming relations are not necessarily symmetric: while the subscribers of one PLMN may be allowed to roam in a given network via the chain of the intermediaries, the converse may be (contractually) prohibited.

The set of opened roaming relations changes over time and a consistent view over which relations should be opened and closed requires continuous coordination. The nature of this coordination depends on the type of contractual framework that exists between the PLMNs and the Roaming Intermediaries and is usually different for IPX service providers and for Roaming hub service providers.

More precisely, if the intermediaries are not tasked with managing roaming relations for their customers (PLMNs), then the roaming relations are opened and closed directly between the PLMNs. If, however, the intermediaries are tasked with roaming relation management (as is the case with roaming hubs), then they need to coordinate between themselves as well as their customers and proxy information to the other PLMN, since in this case,

- PLMNs do not coordinate directly between themselves, and
- a roaming relation remains open only for as long as both concerned PLMNs agree to this.

The procedures and mechanisms applied for the peering connection between the two intermediaries differs depending on their role/type.

Prerequisites in all cases

- the intermediaries have populated their DNS servers with entries that enable discovery of their PRINS proxies by means of their FQDNs. Load balancing may be implemented through DNS.
- each intermediary has created a trust anchor for the unique identifier of the other intermediary (e.g. FQDN) and has populated it with the corresponding root certificates, to be used for mTLS.
- (Optional) The intermediaries have exchanged, out of band, their public keys that they use in order to sign PRINS patches. This exchange facilitates that they can verify the signatures over such patches. It is recommended that the public keys to be

embedded within a public key certificate. The details of how exactly to exchange public keys or to verify such a certificate are currently not specified.

- (Optional) The intermediaries agree on whether they would like to use aggregation of N32-f traffic and, if so, which type of aggregation model (see section below).

Additional prerequisites in case the intermediaries are tasked with the management of roaming relations.

- Each intermediary in the chain sets up and maintains a table, called the roaming relations table, that indicates, for each of the PLMN IDs of its customers, and for each of the directions (inbound, outbound), which roaming relations (as identified by the PLMN ID of the roaming partner) via the other intermediary are open, and which are closed.

NOTE: Inconsistencies between the tables of the roaming intermediaries are possible and represent attack surface, as such inconsistencies may lead to unwanted signalling. Security controls must be able to detect unwanted traffic that may be due to such inconsistencies. Such security controls must be deployable both at an intermediary as well as at a PLMN.

D.3.1 N32-c processing on the peering link

The following description assumes that N32-c is established between by means of the HTTP CONNECT method using the intermediaries as HTTP proxies.

D.3.1.1 N32-c handling towards PLMNs

When an HTTP CONNECT request arrives at the first intermediary in the chain over an interface dedicated to the communication with PLMNs for N32-c, it assumes that this is an attempt to establish an N32-c connection to the PLMN as indicated in the relevant header and consults its roaming relations table in order to decide the next steps (details about this check are described in the next chapter). If the roaming relation is not open, it responds with an appropriate error code. Otherwise one of the following two situations can occur.

Situation 1: If it pertains to an open roaming relation via the second intermediary in the chain, then it first resolves that intermediary’s IP address via DNS, and then forwards the message there. A particular header is added to this second HTTP CONNECT message that includes the PLMN IDs of the two roaming partners. This enables the second intermediary to also check whether this relation is open also from its own perspective.

Situation 2: If the roaming relation pertains to another PLMN, i.e. one that is not mediated through another intermediary, then the intermediary resolves the FQDN via DNS and follows the HTTP CONNECT procedure towards the resolved IP address and the indicated port.

D.3.1.2 N32-c handling over the peering link

When an HTTP CONNECT request arrives at an intermediary over an interface dedicated to the communication with another intermediary (peering link), then it is assumed that this is an attempt to setup an N32-c connection where the initiator SEPP belongs to one of the other intermediary’s customers and the responder SEPP belongs to one of this intermediary’s customers. In this case, the processing is analogous as described above (i.e. a particular header which includes the PLMN IDs of the two roaming partners is used to check whether this relation is open).

D.3.2 N32-f processing

If a request to setup an mTLS connection arrives at an intermediary at an interface dedicated to the communication with PLMNs for N32-f, then it is assumed that this is an attempt to setup an N32-f connection with PRINS. The detailed processing is described in the next sections.

If a request to setup an mTLS connection arrives at an interface dedicated to the communication with another intermediary (peering link), then it is assumed that this is a request to setup a PRINS leg for an N32-f connection where the initiator SEPP belongs to one of the other intermediary's customers and the responder SEPP belongs to one of the current intermediary’s customers. The detailed processing is described in the next sections.

D.3.3 Aggregation aspects

On the peering link between the two intermediaries there are multiple levels of aggregation conceivable for N32-f traffic. It is conceivable, for example, that there exists a single TLS/PRINS connection that carries the N32-f traffic of all PLMNs that are connected via the chain.

Another level of conceivable aggregation is on PLMN level. That is, the intermediaries maintain a separate TLS/PRINS connection for each pair of customers with an open roaming relation in a given direction. This corresponds to aggregation because, a given pair of roaming partners, may setup multiple N32-f connections, each serving a separate subset of PLMN IDs or purposes.

Finally, an intermediary may choose to not use aggregation at all. In this case, it would create a separate mTLS connection towards the other intermediary for each incoming N32-f mTLS connection it receives from its customers.

D.4 N32 Connection Setup and Message Transfer

The N32 connection setup and message transfer passes the following steps.

- Preliminary Key exchange
- Dynamic SEPP discovery
- TLS connection setup
    - For n32-c
    - For n32-f
- N32-c protocol
    - N32-c capability exchange
    - N32-c parameter exchange

    - N32-f error reporting
    - N32-f context termination
- N32-f message transfer
    - N32-f message reformatting
    - N32-f message forwarding and patching

Sample call flows are shown in the respective chapters.

As part of the onboarding process, the PLMN A uses the cIPX’s implementation guide in order to define a PRINS protection policy with PLMN B. The implementation guide describes the requirements for this policy depending on the contracted services, and a suitable policy from a set of “popular” policies may be selected (e.g. "integrity-only"). It is important to note that also B's interests, and in particular the requirements for the services that B has agreed with pIPX, are also reflected in the policy. Note, that the policy needs to be specified in a way that is compatible with all services by intermediaries that have been contracted by A and B, even if multiple N32 connections are setup, possibly for different purposes. This is because, for a given roaming relation, intermediaries cannot differentiate different parallel N32 connection types and therefore apply a different policy to each.

Moreover, cIPX provides A with its certificates or public keys that are to be used to verify PRINS modifications attributable to cIPX (see next section preliminary key exchange).

A configures its SEPP with the following:

- It stores the public keys or certificates received by cIPX in order to use them in N32-c exchanges. Depending on policy, this material
    - may be signed by a SubCA selected by A,
    - may be used as raw public keys (i.e. without being embedded in a certificate), or
    - if provided in the form of a certificate that was issued by a SubCA of cIPX's choice, may be used in that form.
- It creates a trust anchor for B and populates it with B’s PLMN IDs and the corresponding root CA certificate(s) from the RAEX tool.
- It creates a trust anchor for cIPX and populates it with its unique identifier (e.g. FQDN) and the corresponding root certificates for TLS.
- It selects and configures a PRINS protection policy to be used with B, as described above.
- It configures its SEPP to only offer PRINS in N32-c negotiation when the remote entity is B.
- It configures its SEPP to use cIPX’s FQDN or IP address (as agreed with cIPX) as the HTTP proxy for N32 (both N32c and N32f).

cIPX configures the following:

- It creates a trust anchor for A and populates it, using the RAEX tool or using a direct channel, with A's PLMN IDs and the corresponding root certificates for TLS.

D.4.1 Dynamic SEPP discovery

In principle, multiple options exist for the dynamic discovery of the target SEPP IP address. One option is for the last hop, i.e. pIPX to resolve the well-known FQDN, and for all previous hops (i.e. iSEPP and the PRINS node at cIPX) to use the well-known FQDN. Another option is for the iSEPP to resolve the "final" FQDN (i.e. to select one from the ones offered in the SRV response). This last option is described below.

Dynamic SEPP discovery by the iSEPP may not be possible in case PLMN B is not willing to open its IP firewalls for IP addresses of PLMN A. In that case, the only options are either for the pIPX to do the discovery, or for PLMN A to statically configure the target SEPP FQDNs that would normally be returned in SRV records. In both case, N32-f traffic is simply forwarded to the appropriate cIPX with the target SEPP FQDN populated in the authority header.

In this design, it is assumed that DNS queries from PLMN A are accepted by PLMN B, implying that IP firewalls are opened up.

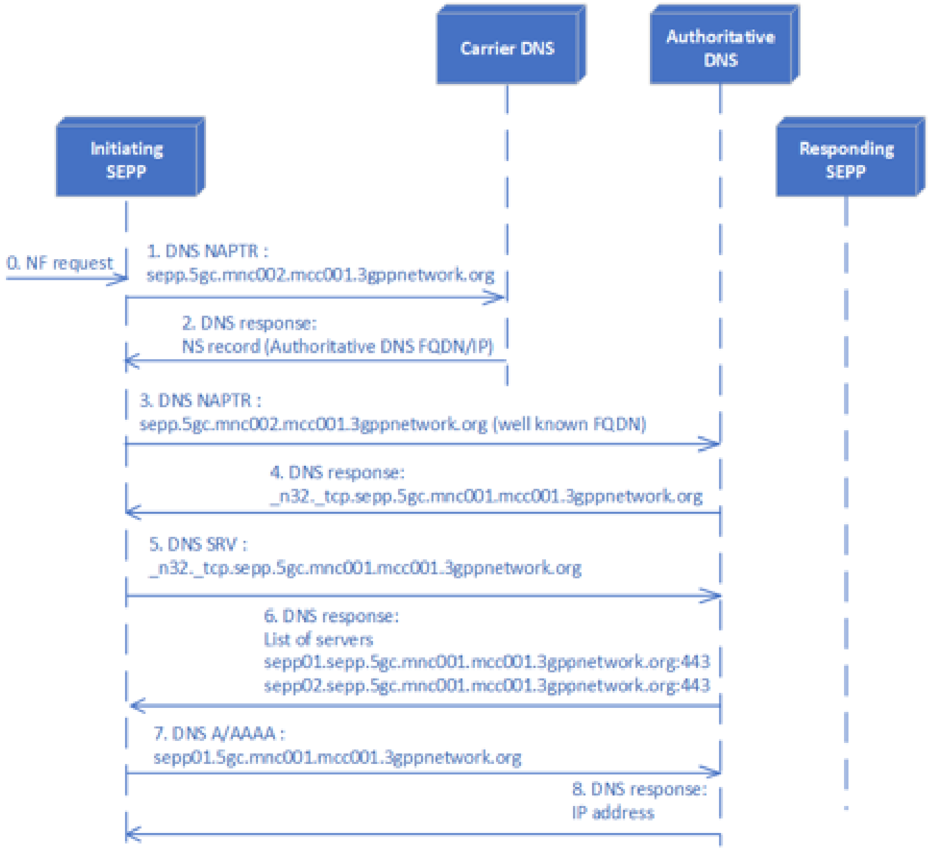

Carrier DNS
Authoritative DNS
Initiating SEPP
Responding SEPP
0. NF request
1. DNS NAPTR : sepp.5gc.mnc002.mcc001.3gppnetwork.org
2. DNS response: NS record (Authoritative DNS FQDN/IP)
3. DNS NAPTR : sepp.5gc.mnc002.mcc001.3gppnetwork.org (well known FQDN)
4. DNS response: _n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org
5. DNS SRV : _n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org
6. DNS response: List of servers sepp01.sepp.5gc.mnc001.mcc001.3gppnetwork.org:443 sepp02.sepp.5gc.mnc001.mcc001.3gppnetwork.org:443
7. DNS A/AAAA : sepp01.5gc.mnc001.mcc001.3gppnetwork.org
8. DNS response: IP address

Figure 49 - Dynamic SEPP Discovery

It is assumed that a DNS client within the SEPP takes care of the DNS queries either directly or through a local DNS cache. The DNS client does not make any decisions on next steps but returns the result of each query up to the SEPP application layer. The SEPP application layer decides on the next DNS query to be sent. (Also see section 4.19 of IR.67 [8]). If the FQDN and port of the peer SEPP are locally configured steps 0 to 6 can be skipped.

0. The i-SEPP obtains from its local configuration the well-known FQDN of PLMN B. If the connection is established on the first message towards PLMN B, the 3gpp-Sbi-Target-ApiRoot header in the message is used to construct a well-known FQDN based on the PLMN ID within the 3gpp-Sbi-Target-ApiRoot header. In addition, the PLMN ID is used to select a trust anchor for verifying the TLS server certificate chain.

   Example

3gpp-Sbi-Target-ApiRoot	Well-known FQDN
nrf.5gc.mnc002.mcc001.3gppnetwork.org	sepp.5gc.mnc002.mcc001.3gppnetwork.org

1. The i-SEPP sends a DNS NAPTR query to the IPX Secondary Root DNS (carrier DNS) (IR.67 2.2 [4]) using the well-known FQDN (i.e. sepp.5gc.mnc002.mcc001.3gppnetwork.org).

NOTE 1: if the DNS cache contains an entry for the well-known FQDN, steps 1 – 4 can be skipped.

NOTE 2: This step is optional and only used to discover the DNS of the target PLMN. The DNS of the target PLMN can also be obtained from IR.21

NOTE 3: If the DNS cache contains an entry for the well-known FQDN, steps 1 – 4 can be skipped.

2. The IPX Secondary Root DNS returns an NS record containing the FQDN and IP of the authoritative DNS.

3. The i-SEPP sends the same DNS NAPTR query as in step 1 to the authoritative DNS of PLMN B.

4. The DNS server returns one or more NAPTR records containing the domain name of the N32 service. Note that the mnc/mcc value of the returned domain can be different from the mnc/mcc in the well-known FQDN. The goal is to allow the PLMN to use the same SEPP (FQDN) for different PLMN IDs.

```
sepp.5gc.mnc002.mcc001.3gppnetwork.org. 14400 IN NAPTR  50 100 “s” “x-3gpp-sepp:x-n32c”  “” _n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org
```

5. The i-SEPP selects one of the records received in step 4 based on the needed service and sends a DNS SRV query to the authoritative DNS using the selected domain. (i.e., _n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org).

NOTE: If the DNS cache contains an entry for the selected record, the DNS query is skipped.

6. The DNS returns one or more SRV records indicating the SEPP topology of PLMN B. The SRV records contain a priority and weight to allow the i-SEPP to select a responding SEPP (r-SEPP) (Ref.: RFC 2782 [8]), and the FQDN and ports to be used to establish N32-c to each r-SEPP.

```
                                                 TTL class SRV priority weight port target.
_n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org.  600 IN    SRV 10       60     443  sepp1.sepp.5gc.mnc001.mcc001.3gppnetwork.org.
_n32._tcp.sepp.5gc.mnc001.mcc001.3gppnetwork.org.  600 IN    SRV 10       20     443  sepp2.sepp.5gc.mnc001.mcc001.3gppnetwork.org.
```

7. The i-SEPP selects one or multiple r-SEPPs based on the received SRV records. If multiple r-SEPPs are selected the i-SEPP shall set up N32 connections to each selected r-SEPP to allow load balancing of traffic.

NOTE 1: The details on how and when peer SEPPs are discovered and how traffic can be load-balanced is described in detail in IR.67.

The i-SEPP sends a DNS A/AAAA query to resolve the IP address of the selected r-SEPP or r-SEPPs. For this document it is assumed one r-SEPP is selected.

NOTE 2: If the DNS cache contains an entry for the selected FQDN, the DNS query is skipped.

8. The DNS returns an A/AAAA record with the correct IP address.

NOTE 1:If the DNS server is configured so that the IP addresses are already returned in step 6 then step 7 and 8 can be skipped.

NOTE 2: For NF service requests to be sent from PLMN B to PLMN A the SEPP in PLMN B also has to discover the SEPPs in PLMN A using the same procedure, and execute the N32c Handshake if there is no pre-existing context for the discovered peer SEPPs

Instead of static (IP) configuration of c/pIPX, a DNS-based discovery mechanism could be used.

D.4.2 TLS Connection setup

The mTLS connection setup is the pre-requisite for initiating N32-c and N32-f. The TLS handshake procedure (RFC) is used both for N32-c and N32-f. The TLS connection for n32-c is established between i-SEPP and roaming intermediaries using HTTP CONNECT in order to establish the mTLS between i-SEPP and r-SEPP via IPX proxies (c/pIPX), in case the roaming intermediary agrees on the TLS setup for N32-c.

The HTTP CONNECT establishment method requires SEPPs to be compliant to 3GPP Release 16 or above.

Local configuration is required per roaming relation to decide whether TLS or PRINS is to be offered.

D.4.2.1 TLS Connection setup for n32-c via IPX proxies

The i-SEPP sets up a TCP connection to its IPX proxy (c/pIPX). The i-SEPP uses the HTTP CONNECT method to instruct the IPX proxy to establish a TCP connection towards the r-

SEPP, uniquely identified by its FQDN. The c/pIPX selects a p/cIPX from local configuration and uses the HTTP CONNECT method to instruct the next IPX proxy to establish a TCP connection to the r-SEPP. Once the r-SEPP is reached the mTLS tunnel is established and the IPX proxies only forward TCP packets.

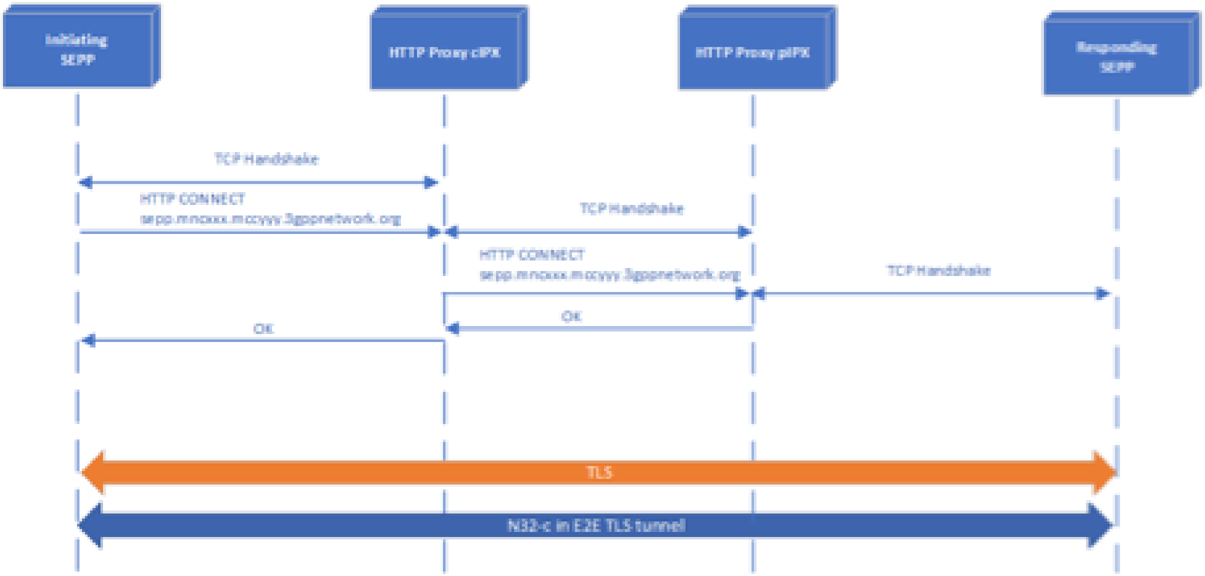


Figure 50 - N32-c mTLS connection using HTTP CONNECT

When an HTTP CONNECT request arrives at IPX proxy X over an interface dedicated to the communication with another IPX proxy, then it is assumed that this is an attempt to setup an N32-c connection where the initiator SEPP belongs to one of the other proxy's customers and the responder SEPP belongs to one of X's customers.

After a TCP proxy connection via HTTP CONNECT has been established, X forwards the traffic over this connection according to standard processing.

HTTP CONNECT shall be supported.

NOTE: The details on HTTP connect are provided in TS 29.573 Rel-18 [10] with Note 2 in clause 5.5.1 stating its applicability from Release 16 onwards.

D.4.2.2 TLS Connection setup for n32-f

It is assumed that mTLS connections for n32-f message forwarding are established at the time of provisioning, in both directions between c-SEPP and cIPX; cIPX and pIPX; pIPX and pSEPP respectively. It is also assumed that the same TLS connections can be used for multiple roaming relations. Dynamic discovery of SEPPs and IPX proxies was discussed in Section D.4.1.

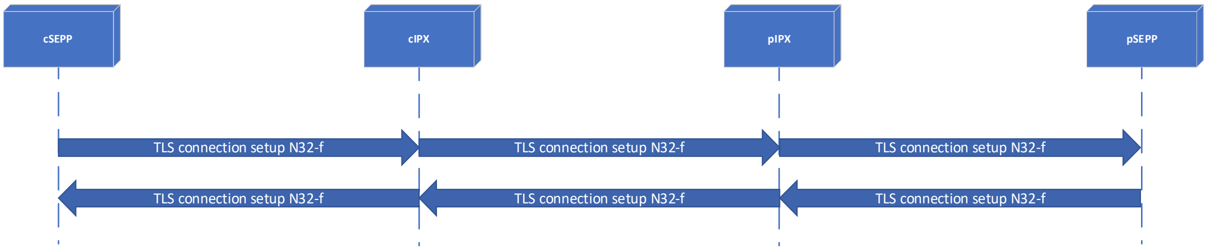

cSEPP
cIPX
pIPX
pSEPP
TLS connection setup N32-f
TLS connection setup N32-f
TLS connection setup N32-f
TLS connection setup N32-f
TLS connection setup N32-f
TLS connection setup N32-f

Figure 51 - N32-f mTLS connections

IPX proxy nodes do not partake in n32-c negotiation, therefore TLS connections for n32-f between IPX proxies are “context-agnostic”. In case of aggregation, they may carry traffic for multiple roaming relations and purposes.

Figure 51 shows the mTLS establishment procedure for the connection between the cSEPP and cIPX. All mTLS connections depicted in Figure 51 follow the same procedure. One difference compared to the N32-c TLS setup is the Servername in the ClientHello, which contains the FQDN of the next hop, and the SAN fields in the respective certificates.

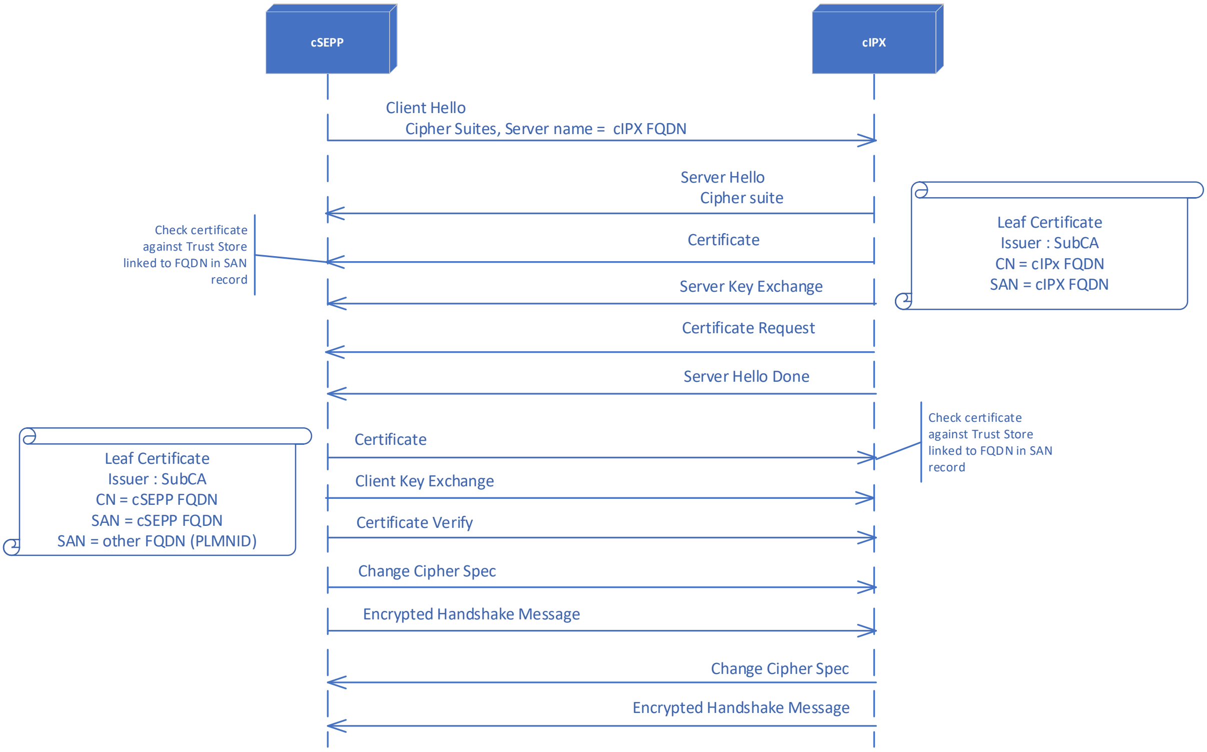


Figure 52 - N32-f mTLS connection establishment

D.4.3 N32-c Protocol

D.4.3.1 N32-c Capability Exchange

In PRINS, an N32-f context between 2 endpoints (SEPPs represented by FQDN:PORT) is explicitly negotiated through the capability exchange procedure.

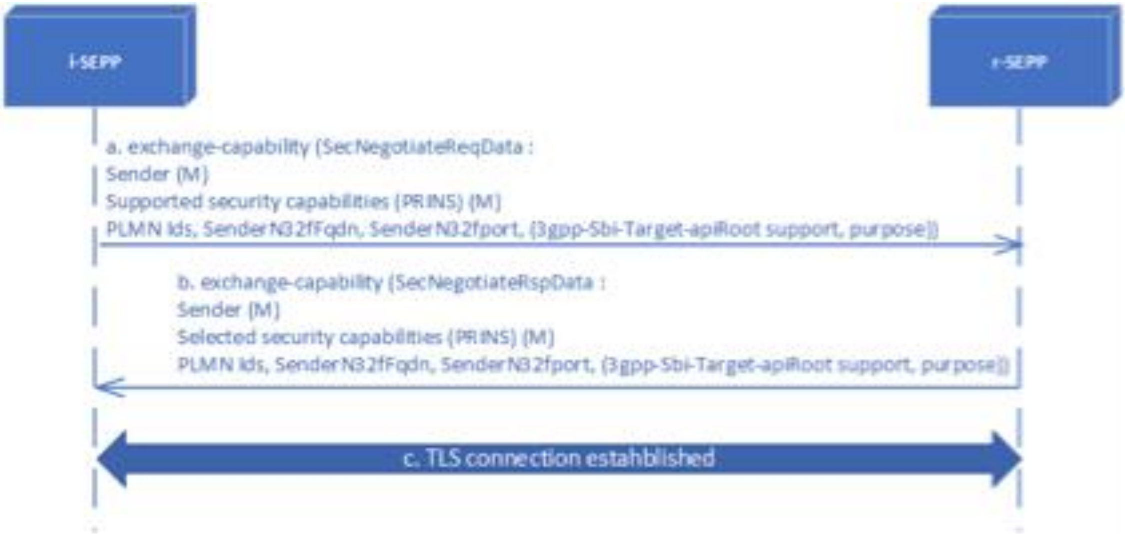

i-SEPP
r-SEPP
a. exchange-capability (SecNegotiateReqData :
Sender (M)
Supported security capabilities (PRINS) (M)
PLMN Ids, SenderN32fFqdn, SenderN32fport, (3gpp-Sbi-Target-apiRoot support, purpose))
b. exchange-capability (SecNegotiateRspData :
Sender (M)
Selected security capabilities (PRINS) (M)
PLMN Ids, SenderN32fFqdn, SenderN32fport, (3gpp-Sbi-Target-apiRoot support, purpose))
c. TLS connection estahblished

Figure 53 - N32-c Handshake

a) Within an established mTLS tunnel for n32-c , the i-SEPP sends an http/2 n32-c exchange capability message to the r-SEPP. The ":authority" header is set to the r-SEPP FQDN.

The SecNegotiateReqData contains the FQDN of the i-SEPP in the Sender IE (sepp01.sepp.5gc.mnc888.mcc999.3gppnetwork.org) and indicates PRINS in the Supported security capability IE.

If the plmnIdList IE is missing, the r-SEPP shall respond with an appropriate 4xx/5xx status code. If any of the PLMN IDs in the plmnIdList IE or the Sender IE does not match the PLMN IDs in the SAN records of the TLS certificate of the i-SEPP, then further actions shall be taken according to operator policy. Likewise, if the PLMN IDs in the plmnIdList IE or the Sender IE do not belong to the same and correct organisation according to IR.21 information, further action shall be taken according to operator policy.

If the i-SEPP wants incoming N32-f connections to be set up to a different FQDN and/or port, the i-SEPP can indicate this in the SenderN32fFqdn and/or SenderN32fPort IEs as specified in Release 18 of 3GPP TS 29.573 [10].

b) The SecNegotiateRspData from the r-SEPP contains the FQDN of the r-SEPP in the Sender IE and PRINS in the Selected security capability. The Sender IE shall be used by the i-SEPP to uniquely identify the r-SEPP and to build an N32 context consisting of the i-SEPP FQDN and r-SEPP FQDN pair.

The r-SEPP shall include a plmnIdList IE. If the plmnIdList is missing, the TLS connection shall be torn down.

NOTE: The i-SEPP cannot respond with an error code since it is the HTTP client.

If any of the PLMN IDs in the plmnIdList IE or the Sender IE does not match the PLMN IDs in the SAN records of the TLS certificate of the r-SEPP, then further actions shall be taken according to operator policy. Likewise, if the PLMN IDs in the plmnIdList IE or the Sender IE do not belong to the same and correct organisation according to IR.21 information, further action shall be taken according to operator policy. If the r-SEPP wants incoming N32-f connection to be set up to a different FQDN and/or port, it can indicate this in the SenderN32fFqdn and/or SenderN32fPort IEs as specified in Release 18 of 3GPP TS 29.573 [10].

All the received IEs are stored within the N32 Context on the i-SEPP and the r-SEPP.

c) Once the n32-c handshake has concluded the mTLS connection shall be reused for the parameter exchange procedures. When the parameter exchange procedures have been executed, the SEPPs may decide to keep the TLS connection for n32-c active, and the r-SEPP may create a TLS connection for n32-c in the other direction. These connections can be used for n32-f error reporting and termination procedures.

D.4.3.2 N32-c Parameter Exchange

This procedure consists of 3 parts that use the same N32-c message (exchange-params).

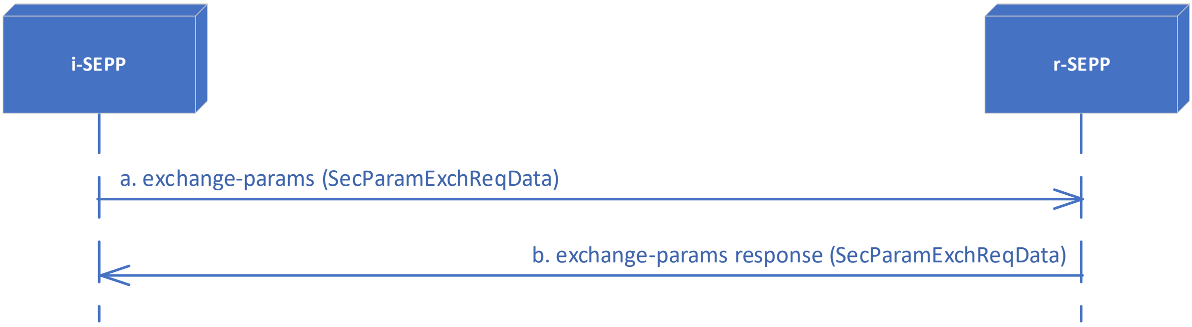

i-SEPP
r-SEPP
a. exchange-params (SecParamExchReqData)
b. exchange-params response (SecParamExchReqData)

Figure 54 - N32-c Parameter Exchange

D.4.3.2.1 Cipher Suite Negotiation

a) The i-SEPP sends an exchange-params message to the r-SEPP providing a prioritised list of supported cipher suites, and an N32fContexId to be used by the r-SEPP for messages initiated in the r-SEPP network.

b) The r-SEPP shall compare the provided cipher suites with its own list and select a cipher suite according to local policy. The r-SEPP shall respond with the selected cipher suite and will provide an N32fContextId to be used by the i-SEPP for messages initiated in the i-SEPP network. In case of failure the r-SEPP shall respond with an appropriate 4xx/5xx error code, as specified in TS 29.573 [10] clause 6.1.6.

D.4.3.2.2 Protection Policy Exchange (optional)

a) The i-SEPP sends an exchange-params message to the r-SEPP with the protection policy information containing a mapping of all APIs and corresponding IEs with an indication if the IE is modifiable by the cIPX and a list of IEs that are to be protected (encrypted).

b) The r-SEPP send an exchange-params response message to the i-SEPP with the selected protection policy information containing a mapping of all APIs and corresponding IEs with an indication if the IE is modifiable by which specific pIPX. In case of failure the r-SEPP shall respond with an appropriate 4xx/5xx error code.

This step is optional, because the 3GPP specifications (3GPP TS 33.501 [19] clause 13.2.3.6) assume that the policy is decided upfront between the roaming partners. This step can then optionally be executed as a means to verify the configurations on both ends – which have to match.

D.4.3.2.3 Security Information List Exchange

a) The i-SEPP shall send an exchange-params message to the r-SEPP with the IPX Provider Security Info List containing the identifier of the cIPX and a list of associated raw public keys or certificates of the cIPX.

b) The r-SEPP shall send an exchange-params response message to the i-SEPP with the IPX Provider Security Info List containing the identifier of the pIPX and a list of associated raw public keys or certificates of the pIPX.

It is assumed that only the IPX identifiers of the intermediaries used for the roaming relation are included in this exchange, and take the form of an FQDN as specified in TS 29.573 [10]. If an IPX has multiple nodes for load balancing and redundancy, then multiple identifiers and public keys may be exchanged, or multiple public keys using the same (shared) IPX identifier.

Editor's note: FQDN format to be clarified by 3GPP.

D.4.3.3 N32-f Error Reporting

If an n32-f message cannot be processed by the receiving SEPP it shall report the error to the sending SEPP using the n32-f error reporting procedure. If there is no active n32-c TLS connection, the receiving SEPP shall create one. The receiving SEPP derives the sending SEPP FQDN from the locally stored context information. Either side can initiate the error reporting procedure, regardless of which side initiated the first n32-c handshake. In the following diagram the i-SEPP is the SEPP initiating the error reporting procedure, the r-SEPP is the SEPP which sent the original n32-f message.

Certain errors may not be subject to error reporting. How such errors are handled may depend on whether the system is in testing or production phase. In case of testing, errors that are not reported using the method above should raise a troubleshooting ticket.

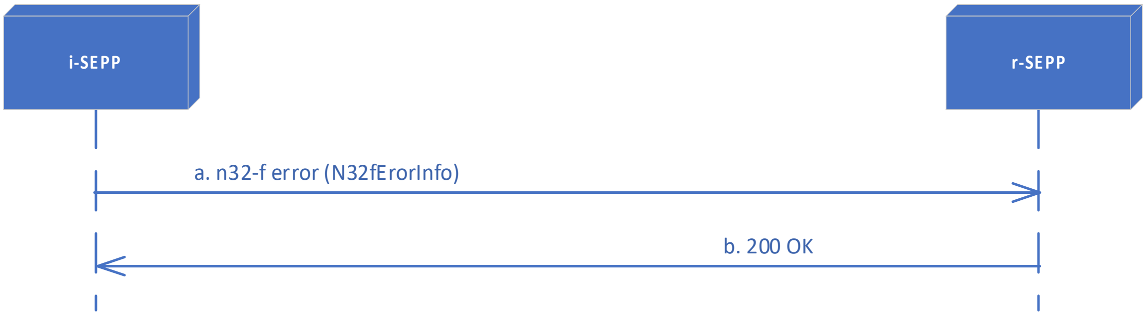


Figure 55 - N32-f Error Reporting

a) The i-SEPP uses the n32-f error message to inform the r-SEPP of the error and error details. It shall add the n32fMessageId from the reformatted N32 message, n32fErrorType and the n32fContextId provided by the r-SEPP during cipher suite negotiation. If the error is related to failure of modification patches, the ErrorInfo shall contain information on which modification from which IPXs failed.

b) The r-SEPP responds with 200 OK or with an appropriate 4XX/5XX error in case of error.

D.4.3.4 N32-f Termination

Either side can terminate n32-f contexts. The SEPP initiating the termination procedure is called the i-SEPP.

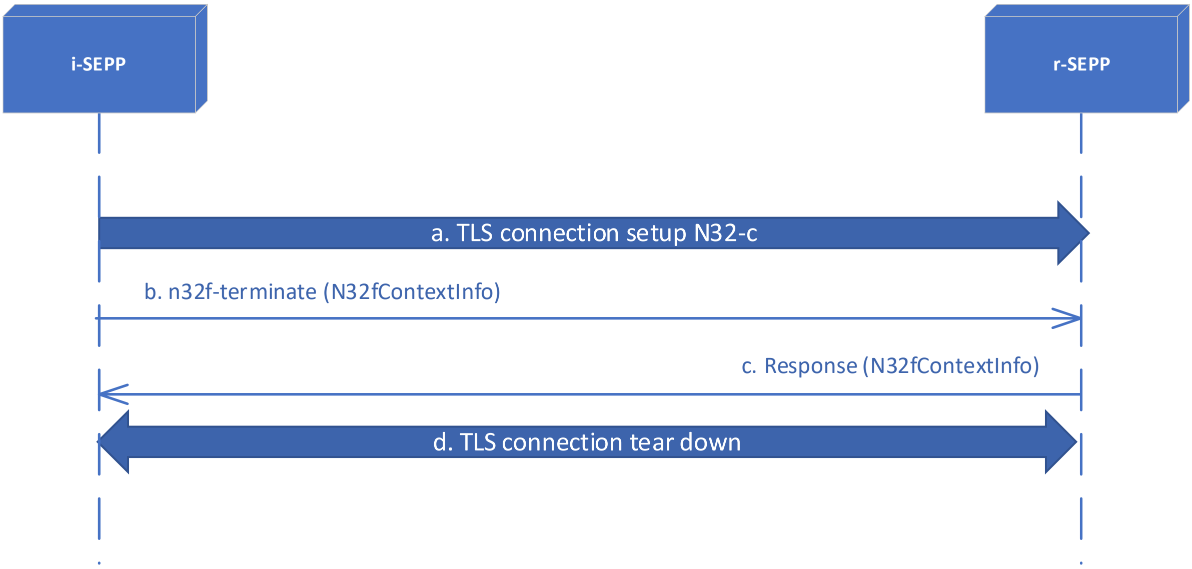

i-SEPP
r-SEPP
a. TLS connection setup N32-c
b. n32f-terminate (N32fContextInfo)
c. Response (N32fContextInfo)
d. TLS connection tear down

Figure 56 - N32-f Context Termination

a) The SEPP wishing to terminate the context opens a short-lived TLS connection according to Section D.4.2.

b) The i-SEPP sends an n32f-terminate message to the r- SEPP. The N32fContextInfo IE shall contain the N32fContextId of the r-SEPP.

c) The r- SEPP response shall contain the N32fContextInfo IE with the N32fContextId of the i-SEPP.

d) The N32-c TLS connection is torn down.

D.4.4 N32-f message transfer

D.4.4.1 N32-f reformatting

NF service requests and responses are reformatted into JSON objects according to the procedures described in 3GPP TS 33.501 [19] clause 13.2.4.3. using the encryption policy as exchanged in Section D.4.3.2.2f.

The metadata object contains the following parameters:

- The N32fMessageId containing a unique randomly generated identifier.

- The N32fContextId containing the N32fContextId provided during the cipher suite negotiation procedure.
- The authorisedIPX containing the FQDN of the first hop IPX or NULL if there is no authorised IPX.

The JSON objects are used to generate a JWE object using a symmetric key derived from the TLS connection (Note that there will be a different encryption key per N32 Connection).

The resulting JWE object is sent as payload in the N32-f HTTP request (or response) message sent to the peer SEPP as described in in Section D.4.3.2.2f.

D.4.4.2 N32-f forwarding and patching

NF service requests are forwarded by the cSEPP to the pSEPP using the N32-f mTLS connections pre-established in 3.4.3. (This is a summary of 3GPP TS 33.501 [19] clause 13.2.4.8 with additional information).

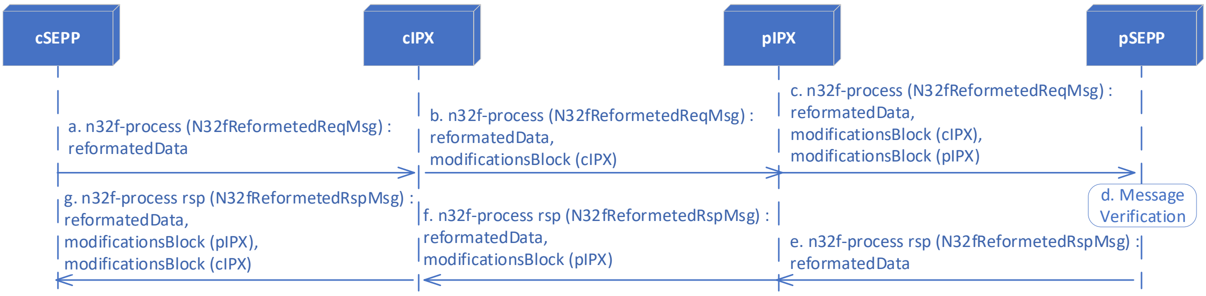

cSEPP
cIPX
pIPX
pSEPP
a. n32f-process (N32fReformetedReqMsg) : reformatedData
b. n32f-process (N32fReformetedReqMsg) : reformatedData, modificationsBlock (cIPX)
c. n32f-process (N32fReformetedReqMsg) : reformatedData, modificationsBlock (cIPX), modificationsBlock (pIPX)
d. Message Verification
e. n32f-process rsp (N32fReformetedRspMsg) : reformatedData
f. n32f-process rsp (N32fReformetedRspMsg) : reformatedData, modificationsBlock (pIPX)
g. n32f-process rsp (N32fReformetedRspMsg) : reformatedData, modificationsBlock (pIPX), modificationsBlock (cIPX)

Figure 57 – N32-f Forwarding and Patching

a) The cSEPP uses the n32f-process message to send the JWE object constructed in 3.4.4.1. The :authority header will be set to the pSEPP FQDN. The HTTP request shall not contain any 3gpp-Sbi-Target-ApiRoot header (3GPP TS 29.573 [10] Section C.3.2.3).

b) The cIPX unpacks the payload of the n32f-process message and parses the unprotected IEs. The cIPX creates a JSON operations patch to be applied by the pSEPP. The cIPX will add its identity (FQDN – generic or node-specific?) to the JSON patch and create a JWS using the private key from (3.1) to integrity protect the patch. Note that a JWS object has to be created even if no modifications are required. The cIPX appends the JWS object to the n32f-process payload and forwards it to the next hop keeping the :authority header from step a.

c) The pIPX unpacks the payload of the n32f-process message and parses the unprotected IEs. The pIPX applies the JSON patch attached by the cIPX and creates a second JSON operations patch, taking into account modifications by cIPX, to be applied by the pSEPP. The pIPX will add its identity (FQDN) to the JSON patch and create a JWS using the private key from (3.1) to integrity protect the patch. The pIPX appends the JWS object to the n32f-process payload and forwards it to the next hop keeping the :authority header from step b.

d) The pSEPP shall check the integrity and authenticity of the original reformatted message and decrypt it to reconstitute the original NF service request payload (Ref 33.501 clause 13.2.4.7). The pSEPP shall verify the integrity and authenticity of the JSON patches appended by the cIPX and pIPX. The pSEPP shall verify that the modifications provided by the cIPX are permitted according to the policy exchanged and the modifications provided by the pIPX are permitted according to the locally configured policies for the pIPX. If any of these checks and verifications fail, the pSEPP shall use the error reporting procedure to report the error to the cSEPP. The pSEPP shall verify that the modifications are plausible. The pSEPP shall apply the patches in order to create a new NF service request to be forwarded to the NF as provided in the 3gpp-Sbi-Target-ApiRoot header. The pSEPP shall remove the 3gpp-Sbi-Target-ApiRoot header before forwarding the NF service request.

e) – g) follow the same procedure as a) to d) but for NF service request responses received from the pNF.

D.4.4.3 Race Conditions and Recovery

This section describes two situations. First, when two peer SEPPs send an N32 exchange capability message at the same time to each other (Race condition). Second when a SEPP receives a new N32 exchange capability exchange message for an already established N32 context (Recovery).

D.4.4.3.1 Race Condition

If a SEPP sends an N32 exchange capability message, and receives an N32 exchange capability message before it receives a response, it shall compare the FQDNs in the Sender IEs. The SEPP whose FQDN lexicographically precedes the FQDN of the other SEPP shall proceed with the initiated procedure and reject the incoming exchange capability message with the appropriate error cause (Ref: 3GPP TS 29.573 [10] clause 5.2.2). The SEPP where the FQDN does not precede the FQDN of the other SEPP shall stop its initiated connection establishment and proceed by responding to the incoming exchange capability message.

D.4.4.3.2 Recovery

If a SEPP receives an N32 exchange capability message from a peer SEPP for which it already has an active N32 context, it will:

- Stop sending any new messages related to the context
- Delete the existing context Process the received N32 exchange capability request

(Ref: 3GPP TS 29.573 [10] clause 5.2.2)

D.4.4.3.3 Backup Routing

If there is a communication issue between pIPX and pSEPP (selected by cSEPP by means of authority header), then the N32-f connection breaks because each pair of SEPPs have agreed their own encryption keys. Upon reception of an HTTP error code, the cSEPP may attempt to re-establish the connection via the same or a different cIPX, in the hope that a functioning path is selected at this time. However, such a communication cannot be initiated by the cIPX without the involvement of the cSEPP.

In any case, if a high-availability backup routing mechanism is required, it is assumed that any high-availability fail-over solution does not impact application layer mechanisms and is implementation specific.

D.4.4.4 N32-f TLS Lifetime

The N32-f TLS connection is under control of the client initiating the N32-f TLS connection. It is expected that the TLS connection is a long lived connection which is kept active even if there is no traffic to be sent.

Several methods are available to keep the connection alive when there is no traffic to be sent. Since TCP Keep-alive uses standard TCP/IP functionality nothing specific is needed from a server to respond to TCP keep-alive packets. Other methods can optionally be used to monitor the connection if supported by both peers.

- TCP keep-alive. (Mandatory)
- TLS Heartbeat (Optional)
- HTTP2 PING Frame (Optional)

If the peer node does not acknowledge a packet before the timeout expires, the TLS connection shall be re-initialised.

If any of the optional heartbeat methods are used, the recovery actions to be taken are not defined in this document and are subject to operator policy and mutual agreement between peers.

D.5 Considerations for Roaming and Service Hub

This chapter describes the applicability of PRINS to Roaming and Service Hub business models, and whether further modifications to PRINS should be considered.

D.5.1 Roaming Relation Management

The peering relationship between the two Roaming Intermediaries is not bound to any particular PLMN, but rather to the entire set of PLMNs that are interconnected through the chain. From cIPX’s point of view, the PLMNs that it can reach via pIPX are covered by the peering relation, and vice versa for pIPX.

TLS connections between hubs work solely with hub certificates, and therefore hubs shall also register their CA in RAEX DB.

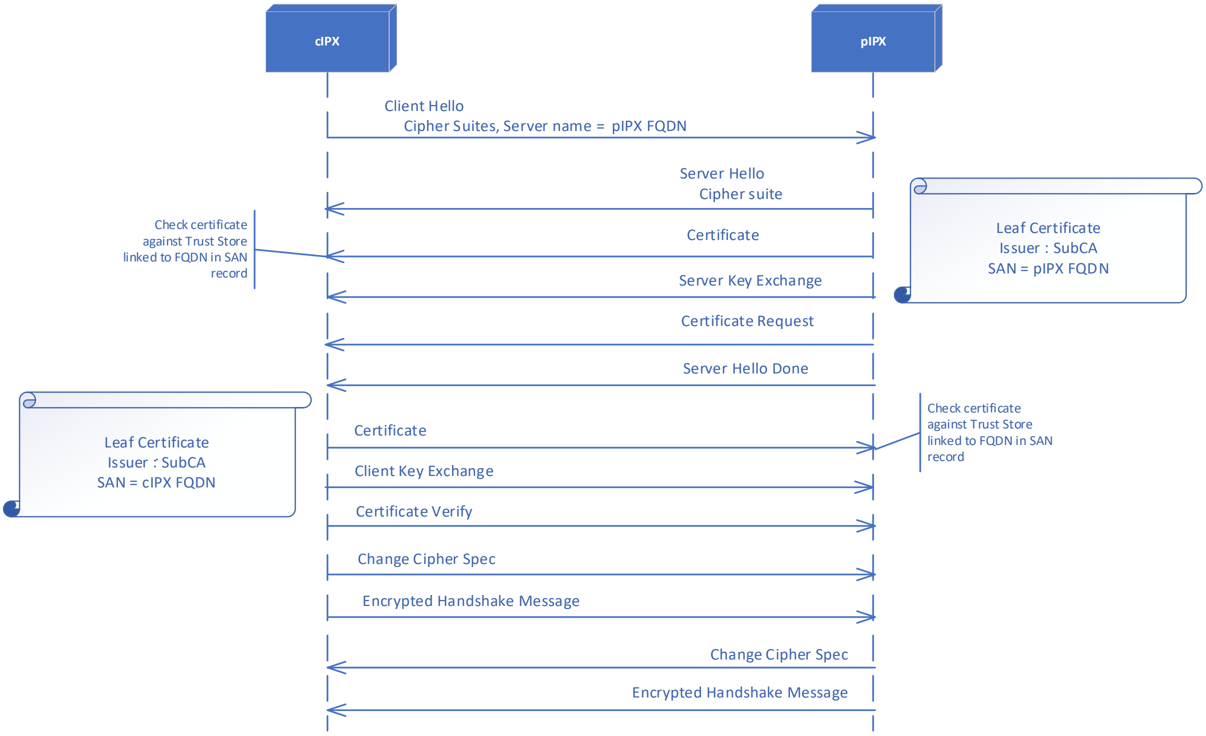


Figure 58 - TLS Connection Setup between hubs

Hubs must know from local configuration which PMNs are reachable via which hub (in business jargon: peering partner). They must also know from local configuration which roaming relations are open, and in which direction (uni-directional i.e. inbound only/outbound only, or both i.e. bi-directional).

Likewise, PMN SEPPs must know which destinations (roaming partner PMNs) are reachable via which hubs. The way local configuration is set up is vendor-specific, but no matter the implementation, it is assumed this knowledge is available and pre-provisioned in all nodes involved, i.e. the SEPPs at the respective PMNs and the IPX proxies at the respective hub service providers.

It is important to keep in mind that only a subset of roaming relations that are theoretically possible via the chain of two IPXs (Roaming Intermediaries) are opened at any given point in time. Moreover, roaming relations are not symmetric: while PMN A’s subscribers may be allowed to roam in PMN B’s network via the chain of intermediaries, the converse may be prohibited.

Also, the set of opened roaming relations changes over time and that a consistent view over which relations should be opened and closed requires continuous coordination. The nature of this coordination depends on the type of contractual framework that exists between the PLMNs and the Roaming Intermediaries and is usually different for IPX service providers and for Roaming Hubs. The latter usually assume more financial reliability than the former.

More precisely, if the intermediaries are not tasked with managing roaming relations for their customers, then the roaming relations are opened and closed directly between the PLMNs.

If, however, the intermediaries are tasked with roaming relation management (as is the case with roaming hubs), then they need to coordinate between their customers as well as themselves and proxy information to the other PLMN since, in this case,

- PLMNs do not coordinate directly between themselves, and
- a roaming relation remains open only for as long as both concerned PLMNs agree to this.

The procedures and mechanisms applied for the peering connection between the two intermediaries differs depending on their role/type. The following apply to roaming hubs as prerequisites.

- cIPX (roaming hub) sets up and maintains a table, called the roaming relations table, that indicates, for each of the PLMN IDs of its customers, and for each of the directions (inbound, outbound), which roaming relations (as identified by the PLMN ID of the roaming partner) via pIPX are open, and which are closed. Moreover, cIPX also knows which PLMN IDs belong to the same PLMN, both for cIPX's own customers, as well as for pIPX's customers. This information is used for filtering.
- Likewise, pIPX (roaming hub) maintains a similar table.
- The hubs agree on a method to identify each other's customers uniquely by means of some unique identifier. This is important in order to agree on the opening and closing of relations and for deciding on whether N32c traffic is allowed or blocked.

NOTE: Inconsistencies between the tables of the hubs are possible and may lead to unwanted signalling. Security controls must be able to detect unwanted traffic that may be due to such inconsistencies. Such security controls must be deployable both at a RH as well as at a PLMN.

- The hubs have populated their DNS servers with entries that enable discovery of their PRINS boxes by means of their FQDNs. Load balancing may be implemented through DNS.
- cIPX has created a trust anchor for the unique pIPX identifier (e.g. FQDN) and has populated it with the corresponding root certificates, to be used for mTLS.
- pIPX has created a trust anchor for the unique cIPX identifier (e.g. FQDN) and has populated it with the corresponding root certificates, to be used for mTLS

N32-c on the peering link

When an HTTP CONNECT request arrives at a cIPX roaming hub over an interface dedicated to communication with PLMNs for N32-c, the hub assumes that this is an attempt to establish an N32-c connection to B (i.e. TLS) and consults its roaming relations and routing tables in order to decide the next steps. If the roaming relation is not open, it responds with an appropriate error code. If it pertains to an open roaming relation via pIPX roaming hub, then cIPX first resolves pIPX's IP address via DNS, and then forwards the message to pIPX.

In order to enable pIPX to conduct the same checks with respect to its own state, it must be put into a position to know the identities of both PLMN A and PLMN B. This is done by the inclusion of an HTTP header within the HTTP CONNECT message (Release 18 onwards).

If the roaming relation pertains to another PLMN, i.e. one that is not mediated through another intermediary, then cIPX resolves the FQDN via DNS and follows the HTTP CONNECT procedure towards the resolved IP address and the indicated port.

When an HTTP CONNECT request arrives at cIPX over an interface dedicated to communication with pIPX, then cIPX assumes that this is an attempt to setup an N32-c connection where the initiator SEPP belongs to one of pIPX's customers and the responder SEPP belongs to one of X's customers. In this case, cIPX uses the HTTP header to check whether the relation is open, analogous to the above description.

After a TCP proxy connection via HTTP CONNECT has been established, cIPX forwards the traffic over this connection according to standard processing.

The processing is for pIPX is analogous.

Aggregation aspects

On the peering leg between cIPX and pIPX there are multiple levels of aggregation conceivable. It is conceivable, for example, that there exists a single TLS/PRINS connection that carries the N32-f traffic of all PLMNs that are connected via the chain. Such a TLS connection would have to be setup without being associated with any particular roaming relation or even PLMN. There would be no identifiers of PLMNs encoded in SNI values or certificates, and the demultiplexing of messages would have to be based on HTTP header information.

Another level of conceivable aggregation is on PLMN level. That is, cIPX and pIPX maintain a separate TLS/PRINS connection for each pair of customers with an open roaming relation in a given direction. This corresponds to aggregation because, a given pair of roaming partners, e.g. A and B, may setup multiple N32-f connections, each serving a separate subset of PLMN IDs or purposes.

However, it is unclear whether the above aggregation approaches work in all cases because there exists no way for cIPX to tell pIPX to open an additional TLS/PRINS connection towards B in case A and B have negotiated an additional N32-f context and they now expect to be used for a specific subset of PLMN IDs or N32Purposes. That is, aggregation on the peering link must be supported by the SEPPs as well.

D.5.2 Other operational aspects

Preliminary Certificate Exchange

IPX providers may need to be involved in order to identify and address any mistakes made on the level of N32-c, e.g. ensuring that the SEPP is configured correctly. For such cases, a suitable procedure may need to be defined by the GSMA.

An alternative to the out-of-band key exchange between PMN and IPX (hub service provider) could also be defined, if required.

TLS Connections

The Roaming Hub shall filter the traffic on N32-f connections according to open roaming relations (ensuring no misallocated traffic, e.g. for closed roaming relations, is forwarded). This is necessary because a single N32-f connection may serve multiple roaming relations.

N32-c Policies

Editor’s Note: move to Peering Link section (to be re-introduced).

A PRINS policy needs to be agreed up-front between 4 stakeholders in each roaming relationship: PMN A, IPX A, IPX B and PMN B. It is hereby assumed that PMN A and B outsource services per roaming relation to only one IPX provider, and that any others are merely providing IP transport.

Policies are agreed up-front as part of the roaming agreement. This has a practical consequence: if PMN A considers outsourcing any service to IPX A which involves a change in policy, this may need to be reflected with all of PMN A’s roaming partners and their respective IPX providers.

If the IPX needs to distinguish between in- and out-bound roaming, this needs to be implemented by the IPX as there is no inherent support for indicating this in N32.

Annex E Detailed design for inter-PLMN connection using hop-by-hop TLS

This detailed design is introduced by this document. It is based on an extension of the N32 protocol developed in the GSMA.

E.1 Introduction

This annex describes the inter-PLMN connection between 2 PLMNs using service providers as intermediate hops. Refer to NG.113, Roaming models, Service and Roaming Hub (models 3 and 4). It uses the N32s profile between PLMN and Service Provider and the N32p profile between Service Providers (“peering”). It covers dynamic SEPP discovery, TLS connection setup for n32s/p-c with n32s/p-c handshake, and TLS connection setup for n32s/p-f.

This design is a generic description for any Hop-by-Hop architecture using TLS only.

The terms Initiating SEPP (i-SEPP) a Responding SEPP (r-SEPP) refer to the endpoints in a direct connection between hops. In the scope of this annex i-SEPP/r-SEPP can be PLMN SEPP, Service Hub SEPP or Roaming Hub SEPP (SP SEPP).

For the sake of clarity, the call flows do not show all possible parameters but only examples where relevant.

E.2 High Level Description

An NF in PLMN A wants to send a request message to an NF in PLMN B and receive responses from that NF in PLMN B. The SEPPs of PLMN A and PLMN B are not directly connected but instead use service providers as intermediate hops deploying their own, intermediate, SEPPs.

The connections between the PLMN and service providers and between service providers relies on the N32 API using the TLS security method.

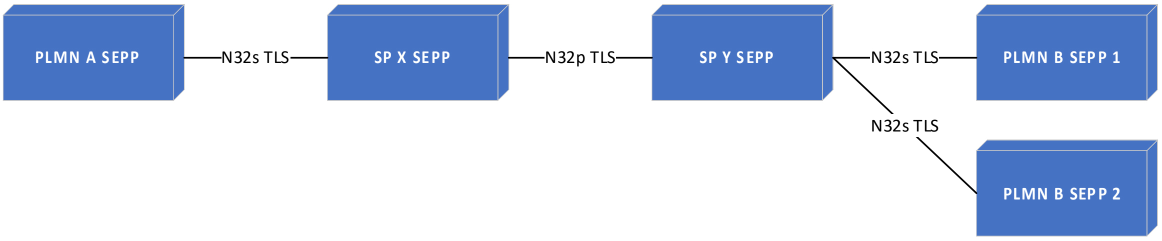


Figure 59 - TLS Hop-by-hop Connections

Because PLMNs have to manage which roaming relations use which interconnect model (direct or via a service provider), it is assumed that PLMN SEPPs have local configurations for one or more service providers and are able to setup connections and route traffic via the correct provider or directly based on the target PLMN. Likewise, it is assumed that intermediate SEPPs (SH or RH SEPP) have local configurations for other intermediates (for peering) as well as PLMNs.

Between a PLMN and the SP SEPP of the service provider, and between SEPPs of service providers, traffic for multiple roaming relations (target PLMN destinations) can be sent over the same N32s/p connection. This document provides recommendations for the connections between PLMN and service provider and the connections between service providers.

N32s and N32p are GSMA variants of the N32 reference point. They consist of variants of n32-c and n32-f called n32s-c/f and n32p-c/f respectively. N32s and N32p are used as described in the following 3 hops.

There are 3 hops to be considered:

1. Connection between PLMN and service provider (N32s): chapter E.3.
2. Connection between two service providers (N32p): chapter E.4.
3. Connection between service provider and PLMN (N32s): chapter E.5.

E.3 Connection between PLMN and service provider

E.3.1 N32s Connection Setup

The N32s connection setup passes the following steps with sample call flows in subsections E.3.2 – E.3.4. It is similar to C.2.1. The trigger for a PLMN SEPP to start the N32s connection setup process will be triggered by local configuration upon (re)start, recovery, etc. Once n32s-f connection to the service provider has been setup, all traffic to target destinations managed via the same service provider can make use of this established connection. There can be multiple n32s-f connections for traffic separation. The below process does not have to be repeated. The case of using multiple n32s-f connections for e.g., load sharing is not further detailed.

- Dynamic SP SEPP discovery via DNS
- TLS connection setup for n32s-c with n32s-c handshake
- TLS connection setup for n32s-f

E.3.2 Dynamic SP SEPP discovery

A PLMN can decide to statically configure a service provider's SP SEPPs. However, it is recommended to use a "well-known" service provider FQDN, of the form "sepp.5gc.<service-provider-unique-name>.ipxnetwork.org. Dynamic discovery of a service provider's SP SEPPs then follows the same procedure as described for bilateral N32 connections (see Annex B), as shown in the next Figure, with PLMN A as initiating party.

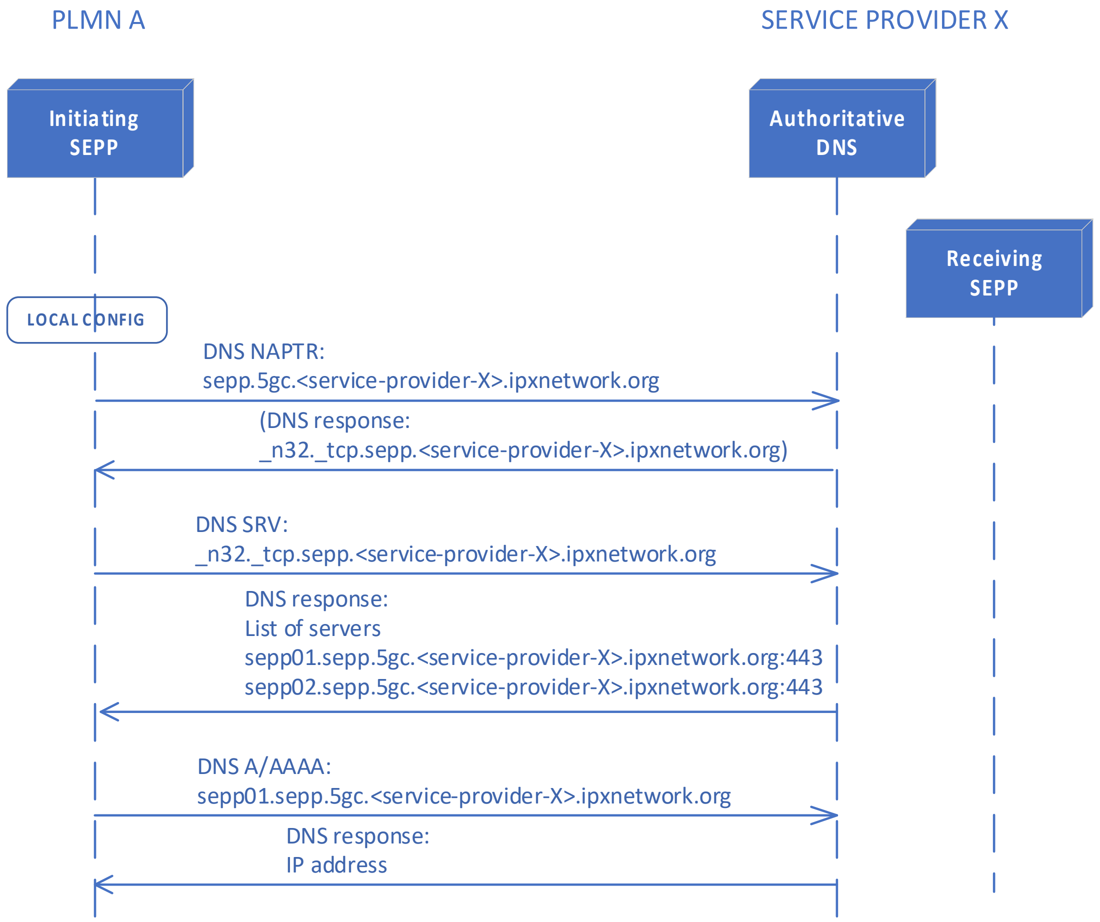

PLMN A
SERVICE PROVIDER X
Initiating SEPP
Authoritative DNS
Receiving SEPP
LOCAL CONFIG
DNS NAPTR:
sepp.5gc.<service-provider-X>.ipxnetwork.org
(DNS response:
_n32._tcp.sepp.<service-provider-X>.ipxnetwork.org)
DNS SRV:
_n32._tcp.sepp.<service-provider-X>.ipxnetwork.org
DNS response:
List of servers
sepp01.sepp.5gc.<service-provider-X>.ipxnetwork.org:443
sepp02.sepp.5gc.<service-provider-X>.ipxnetwork.org:443
DNS A/AAAA:
sepp01.sepp.5gc.<service-provider-X>.ipxnetwork.org
DNS response:
IP address

Figure 60 - Dynamic SP SEPP Discovery

E.3.3 TLS Connection Setup for n32s-c

E.3.3.1 TLS Connection setup

Once the service provider's SEPP FQDN, IP and port are obtained from the previous discovery step, the mTLS handshake procedure can be initiated for n32s-c.

This procedure is as described in Annex C.2.3.

The following table illustrates the format of the domain of the FQDN in the SAN records depending on the owner of the SEPP node.

SEPP owner	Primary SAN	additional SAN
PLMN	.5gc.<PLMN-ID>.3gppnetwork.org	.5gc.<ALT-PLMN-ID>.3gppnetwork.org
Intermediate	.5gc.<service-provider-unique-name>.ipxnetwork.org	N/A

E.3.3.2 N32s-c handshake

The n32s-c handshake is as presented in C.2.3, with the difference that r-SEPP belongs to a service provider and its plmnIdList IE is not relevant.

- The r-SEPP does not include the plmnIdList IE.

E.3.4 TLS Connection Setup for n32s-f

Once a successful n32s-c handshake has been executed, a long lived mTLS connection can be initiated from i-SEPP to r-SEPP and another long lived mTLS connection can be initiated from r-SEPP to i-SEPP for NF service requests in the other direction. This procedure is as described in Annex C.2.4.

E.4 Connection between service providers

E.4.1 N32p Connection Setup

The N32p connection setup passes the following steps with sample call flows in subsections E.4.2 – E.4.4. It is recommended to be triggered by local configuration upon (re)start, recovery, etc. In case of a hub model, once n32p-f connection to the peer service provider has been setup, all traffic to target destinations managed via the peer service provider can make use of this established connection and the below process does not have to be repeated.

- Dynamic peer SP SEPP discovery via DNS
- TLS connection setup for n32p-c with n32p-c handshake
- TLS connection setup for n32p-f

E.4.2 Dynamic Peer SP SEPP Discovery

When originating and target PLMN make use of a service or roaming hub provider, a peering setup is a prerequisite. Service providers can decide to statically configure each other's SEPPs. However, also in this case it can be recommended to use a "well-known" service provider FQDN, of the form "sepp.5gc.<service-provider-unique-name>.ipxnetwork.org". Dynamic discovery of a service provider's SEPPs then follows the same procedure as described for bilateral N32 connections (See Annex B), as shown in the next Figure 61, with service provider X as initiating party.

Notice in this case there is no uniqueness per served PLMN and the N32p connection can be used to carry traffic for any roaming relation between a PLMN served by provider X and a

PLMN served by provider Y. This has specific consequences for handling n32p-f, as discussed in chapter E.4.4.

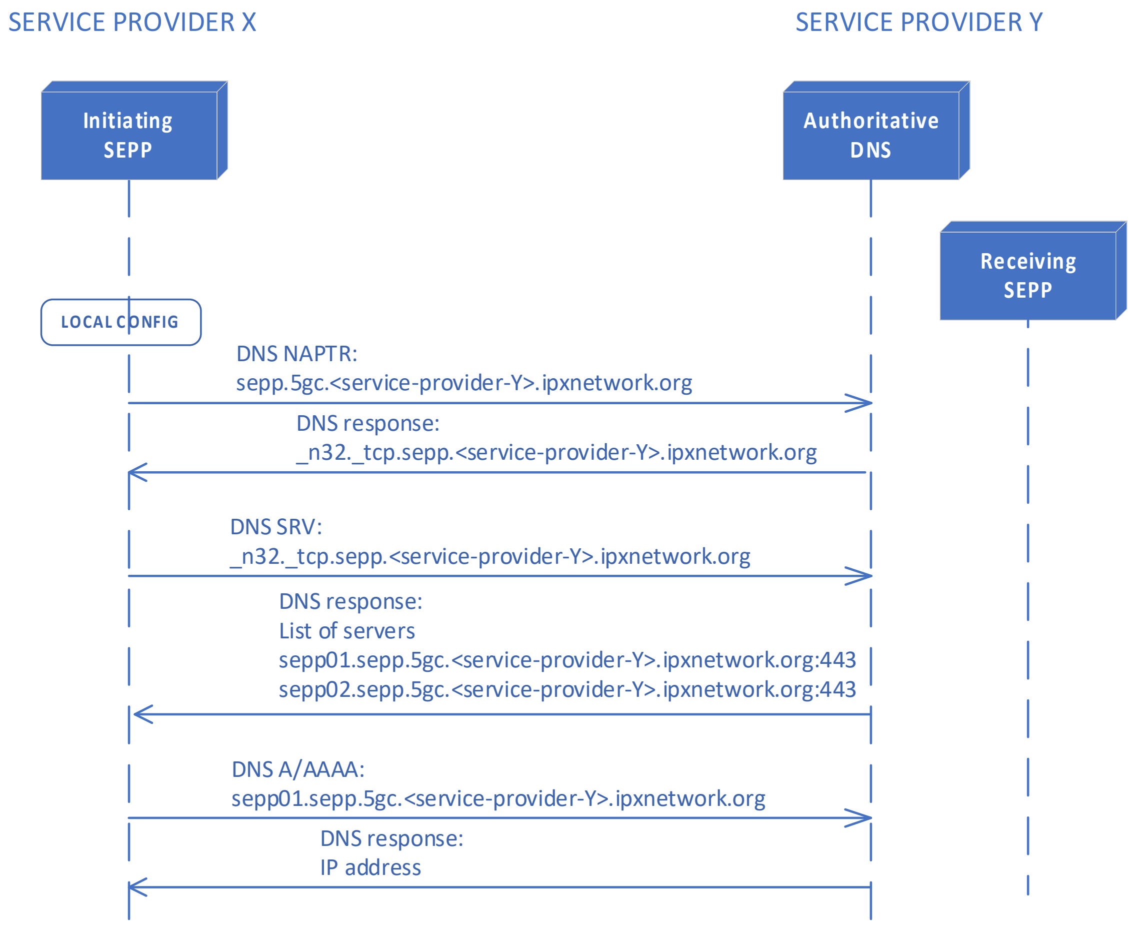

SERVICE PROVIDER X
SERVICE PROVIDER Y
Initiating SEPP
Authoritative DNS
Receiving SEPP
LOCAL CONFIG
DNS NAPTR:
sepp.5gc.<service-provider-Y>.ipxnetwork.org
DNS response:
_n32._tcp.sepp.<service-provider-Y>.ipxnetwork.org
DNS SRV:
_n32._tcp.sepp.<service-provider-Y>.ipxnetwork.org
DNS response:
List of servers
sepp01.sepp.5gc.<service-provider-Y>.ipxnetwork.org:443
sepp02.sepp.5gc.<service-provider-Y>.ipxnetwork.org:443
DNS A/AAAA:
sepp01.sepp.5gc.<service-provider-Y>.ipxnetwork.org
DNS response:
IP address

Figure 61 - Dynamic Peer SP SEPP Discovery

E.4.3 TLS Connection Setup for n32p-c

E.4.3.1 TLS Connection setup

Between peer service providers, the mTLS handshake procedure is essentially the same as presented in C.2.3, with the difference that both i-SEPP and r-SEPP belong to service providers and only primary SAN records are expected in the TLS certificates.

E.4.3.2 N32p-c Handshake

The n32p-c handshake is as presented in C.2.3, with the difference that both i-SEPP and r-SEPP belong to service providers and plmnIdList IE are not relevant. This is indicated in the corresponding steps.

- The i-SEPP does not include the plmnIdList IE.
- The r-SEPP does not include the plmnIdList IE.
- Once the n32p-c handshake has concluded the mTLS connection shall be torn down.

E.4.4 TLS Connection Setup for n32p-f

Once a successful n32p-c handshake has been executed, a long lived mTLS connection can be initiated from i-SEPP to r-SEPP and another long lived mTLS connection can be initiated from r-SEPP to i-SEPP for NF service requests in the other direction.

Support of SenderN32fFQDN and SenderN32fPort is indicated during the N32-c handshake procedure by setting the relevant flag for the SNDN32F in the supported Features attribute. If either SEPP does not support the feature the same FQDN as for the N32-c handshake and, the default destination port (443) or locally configured port, is used to set up the TLS connection for N32-f. See also section 4.1.1.

NOTE: The use of SenderN32fFQDN and SenderN32fPort was introduced in Rel.18.

a) If the SenderN32fFqdn and/or SenderN32Port were provided by the r-SEPP, different from the FQDN and/or Port used for n32p-c, the i-SEPP shall initiate a new DNS A/AAAA query to the authoritative DNS to retrieve the corresponding IP address.

   Otherwise, the same FQDN and/or port as used for the n32p-c handshake shall be used by the i-SEPP.

b) The same procedure and security checks as defined in Annex C shall be used to set up a long lived mTLS tunnel from i-SEPP to r-SEPP. If any of the checks fail, the N32-f context and associated n32p-f connections shall be torn down.

   Additionally, if the n32p-f certificate SAN records contain any FQDN domain which is not present in the corresponding n32p-c certificate, then the certificate shall be rejected.

   Correlation of the N32-f connection to the N32-c context shall be done following B.3.4.2.1.

c) NF service requests are forwarded within the mTLS connection unchanged. The :authority header will be set to the r-SEPP FQDN (or SenderN32fFQDN if exchanged in the n32p-c handshake). The 3gpp-Sbi-Target-ApiRoot header shall be kept as received from the PLMN. The 3gpp-Sbi-Originating-Network-Id header shall be included to identify PLMN A.

   The 3gpp-Sbi-N32-Handshake-Id header shall be set to the n32HandshakeId return by the peer SEPP during the N32-c handshake.

d) If the SenderN32fFqdn and/or SenderN32Port were provided by the i-SEPP, different from the FQDN and/or Port used for n32p-c, the r-SEPP shall initiate a new DNS A/AAAA query to the authoritative DNS to retrieve the corresponding IP address.

   Otherwise, the same FQDN and/or port as used for the n32p-c handshake shall be used by the r-SEPP.

e) The same procedure and security checks as defined in Annex C shall be used to set up a long-lived TLS tunnel from r-SEPP to i-SEPP. If any of the checks fail the N32-f context and associated n32p-f connections shall be torn down.

Additionally, if the n32p-f certificate contains any FQDN domain which is not present in the corresponding n32p-c certificate, then the certificate shall be rejected. (Ref : 3GPP TS 33.501 [19]).

Correlation of the N32-f connection to the N32-c context shall be done following B.3.4.2.1.

f) NF service requests are forwarded within the mTLS connection unchanged. The :authority header will be set to the i-SEPP FQDN (or SenderN32fFQDN if exchanged in the n32p-c handshake). The 3gpp-Sbi-Target-ApiRoot header shall be kept as received from the PLMN. The 3gpp-Sbi-Originating-Network-Id header shall be included to identify PLMN B.

The 3gpp-Sbi-N32-Handshake-Id header shall be set to the n32HandshakeId return by the peer SEPP during the N32-c handshake.

E.5 Connection between service provider and PLMN

E.5.1 N32s Connection Setup

The N32s connection setup passes the following steps with sample call flows in subsections E.5.2– E.5.4. It is recommended that connections are setup by the PLMN instead of the service provider, but under some conditions such as mutual agreement, (re)start, recovery, etc, it may be required for the service provider to initiate the setup. The N32 connection shall only be used for traffic concerning the PLMN.

- Dynamic PLMN SEPP discovery via DNS
- TLS connection setup for n32s-c with n32s-c handshake
- TLS connection setup for n32s-f

E.5.2 Dynamic PLMN SEPP discovery

Dynamic PLMN SEPP discovery by the service provider shall use a private FQDN of the target PLMN (See C.2.2).

E.5.3 TLS Connection Setup for n32s-c

E.5.3.1 TLS Connection setup

The mTLS handshake procedure is essentially the same as presented in C.2.3, with the difference that i-SEPP belongs to a service provider (SP SEPP) and only a primary SAN record is expected in its TLS certificates.

E.5.3.2 N32s-c Handshake

The n32s-c handshake is as presented in C.2.3, with the difference that i-SEPP belongs to a service provider and its plmnIdList IE is not relevant.

- The i-SEPP does not include the plmnIdList IE.

E.5.4 TLS Connection Setup for n32s-F

Once a successful n32s-c handshake has been executed, a long lived mTLS connection can be initiated from i-SEPP to r-SEPP and another long lived mTLS connection can be initiated from r-SEPP to i-SEPP for NF service requests in the other direction.

Support of SenderN32fFQDN and SenderN32fPort is indicated during the N32-c handshake procedure by setting the relevant flag for the SNDN32F in the supportedFeatures attribute. If either SEPP does not support the feature the same FQDN as for the N32-c handshake and, the default destination port (443) or locally configured port, is used to set up the TLS connection for N32-f. See also section 4.1.1.

NOTE: The use of SenderN32fFQDN and SenderN32fPort was introduced in Rel.18.

a) If the SenderN32fFqdn and/or SenderN32Port were provided by the r-SEPP, different from the FQDN and/or Port used for n32s-c, the i-SEPP shall initiate a new DNS A/AAAA query to the authoritative DNS to retrieve the corresponding IP address.

   Otherwise, the same FQDN and/or port as used for the n32s-c handshake shall be used.

b) The same procedure and security checks as defined in 3.3.1 shall be used to set up a long lived mTLS tunnel from i-SEPP to r-SEPP. If any of the checks fail the N32-f context and associated n32s-f connections shall be torn down.

   Additionally, if the n32s-f certificate SAN records contain any FQDN domain which is not present in the corresponding n32s-c certificate, then the certificate shall be rejected.

   Correlation of the N32-f connection to the N32-c context shall be done following B.3.4.2.1.

c) NF service requests are forwarded within the mTLS connection unchanged. If 3gpp-Sbi-Target-apiRoot header is used between the i-SEPP and r-SEPP, then the :”authority” header will be set to the r-SEPP FQDN (or SenderN32fFQDN if exchanged in the n32s-c handshake) and the 3gpp-Sbi-Target-ApiRoot header shall be kept as received from the PLMN or peer service provider. If 3gpp-Sbi-Target-apiRoot header is not used between SEPPs, the “:authority” header will be set to the pNF FQDN and the 3gpp-Sbi-Target-ApiRoot header shall be removed. The 3gpp-Sbi-Originating-Network-Id header shall be included to identify PLMN A, or kept as received from peer service provider A.

   The 3gpp-Sbi-N32-Handshake-Id header shall be set to the n32HandshakeId return by the peer SEPP during the N32-c handshake.

d) If the SenderN32fFqdn and/or SenderN32Port were provided by the i-SEPP, different from the FQDN and/or Port used for n32s-c, the r-SEPP shall initiate a new DNS A/AAAA query to the authoritative DNS to retrieve the corresponding IP address.

   Otherwise, the same FQDN and/or port as used for the N32s-c Handshake shall be used.

e) The same procedure and security checks as defined in 3.3.1 shall be used to set up a long-lived TLS tunnel from r-SEPP to i-SEPP. If any of the checks fail the N32-f context and associated n32s-f connections shall be torn down.

   Additionally, if the n32s-f certificate contains any FQDN domain which is not present in the corresponding n32s-c certificate, then the certificate shall be rejected.

   Correlation of the N32-f connection to the N32-c context shall be done following B.3.4.2.1.

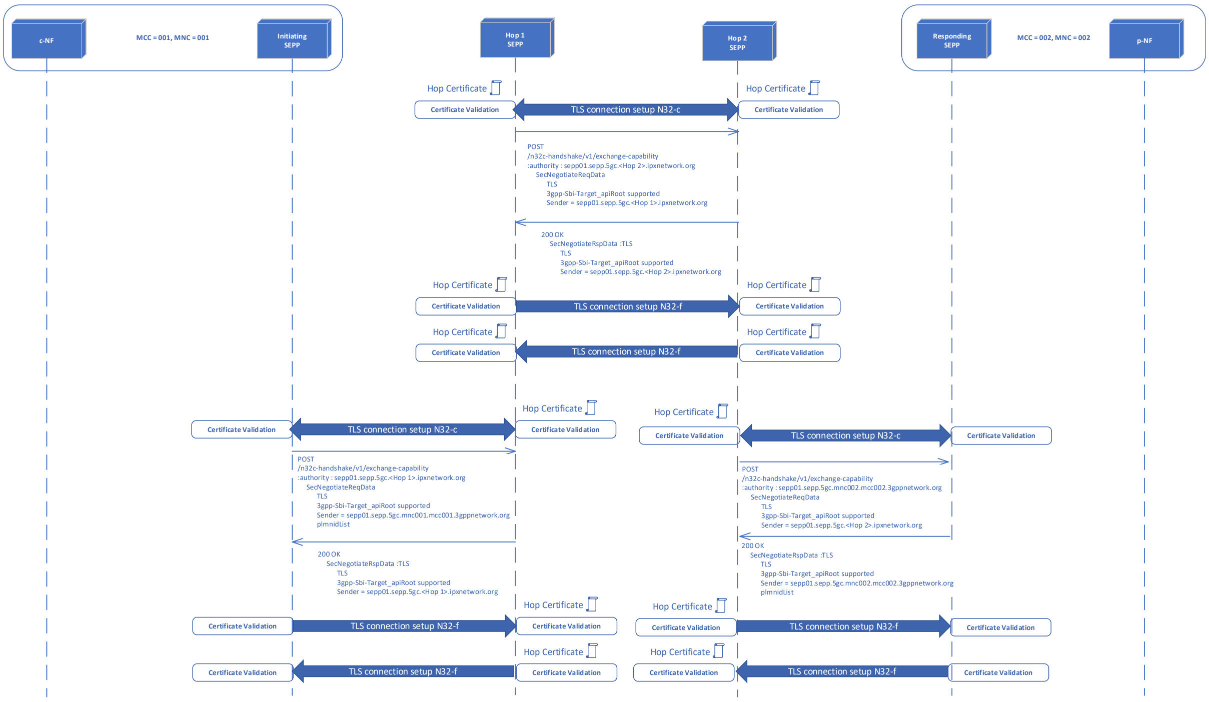
f) NF service requests are forwarded within the mTLS connection unchanged. The “:authority” header will be set to the i-SEPP FQDN (or SenderN32fFQDN if exchanged in the n32s-c handshake). The 3gpp-Sbi-Target-ApiRoot header shall be kept as received from the NF (Ref.: 3GPP TS 29.573 [10] Section C.2.) or shall be inserted by the r-SEPP if not provided by the NF. The 3gpp-Sbi-Originating-NetworkId header shall be kept as received from the NF or included by the r-SEPP if not included by the NF (3GPP TS 29.500 [20] clause 5.2.3.2).

   The 3gpp-Sbi-N32-Handshake-Id header shall be set to the n32HandshakeId return by the peer SEPP during the N32-c handshake.

E.6 N32 Termination

Either side can terminate the N32s/p context and associated n32s/p-f connections. The procedure is the same as described in B.3.4.3.

E.7 E2E Connectivity establishment example



```
POST
/n32c-handshake/v1/exchange-capability
:authority : sepp01.sepp.5gc.<Hop 2>.ipxnetwork.org
   SecNegotiateReqData
      TLS
      3gpp-Sbi-Target_apiRoot supported
      Sender = sepp01.sepp.5gc.<Hop 1>.ipxnetwork.org
```

```
200 OK
   SecNegotiateRspData :TLS
      TLS
      3gpp-Sbi-Target_apiRoot supported
      Sender = sepp01.sepp.5gc.<Hop 2>.ipxnetwork.org
```

```
POST
/n32c-handshake/v1/exchange-capability
:authority : sepp01.sepp.5gc.<Hop 1>.ipxnetwork.org
   SecNegotiateReqData
      TLS
      3gpp-Sbi-Target_apiRoot supported
      Sender = sepp01.sepp.5gc.mnc001.mcc001.3gppnetwork.org
      plmnidList
```

```
200 OK
   SecNegotiateRspData :TLS
      TLS
      3gpp-Sbi-Target_apiRoot supported
      Sender = sepp01.sepp.5gc.<Hop 1>.ipxnetwork.org
```

```
POST
/n32c-handshake/v1/exchange-capability
:authority : sepp01.sepp.5gc.mnc002.mcc002.3gppnetwork.org
   SecNegotiateReqData
      TLS
      3gpp-Sbi-Target_apiRoot supported
      Sender = sepp01.sepp.5gc.<Hop 2>.ipxnetwork.org
```

```
200 OK
   SecNegotiateRspData :TLS
      TLS
      3gpp-Sbi-Target_apiRoot supported
      Sender = sepp01.sepp.5gc.mnc002.mcc002.3gppnetwork.org
      plmnidList
```

Figure 62 - E2E Connectivity establishment

E.8 E2E Traffic flow example

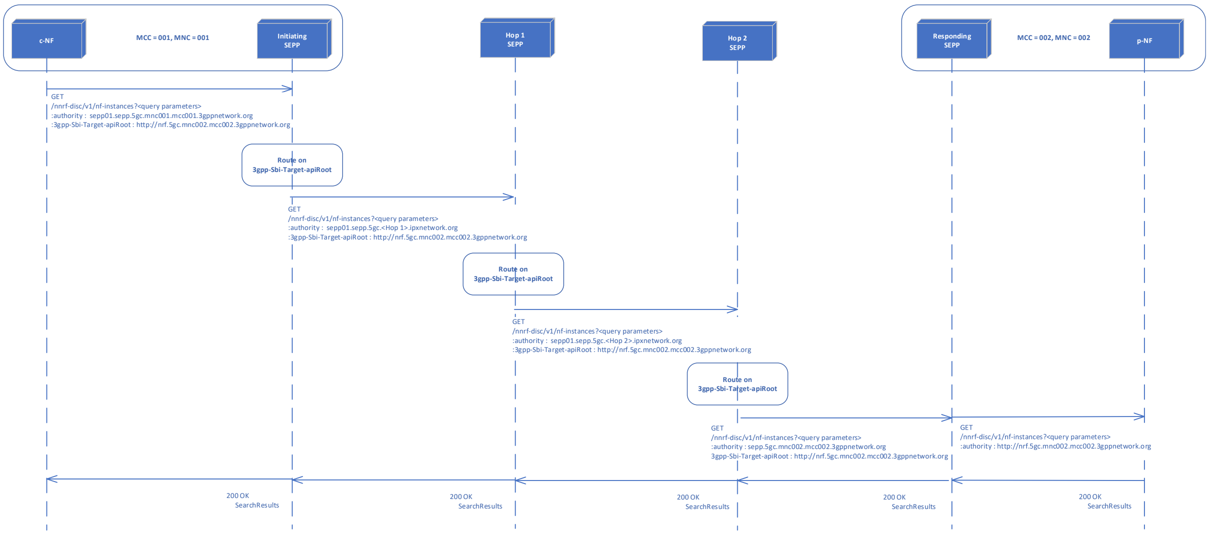

c-NF
MCC = 001, MNC = 001
Initiating SEPP
Hop 1 SEPP
Hop 2 SEPP
Responding SEPP
MCC = 002, MNC = 002
p-NF
GET
/nnrf-disc/v1/nf-instances?<query parameters>
:authority : sepp01.sepp.5gc.mnc001.mcc001.3gppnetwork.org
:3gpp-Sbi-Target-apiRoot : http://nrf.5gc.mnc002.mcc002.3gppnetwork.org
Route on 3gpp-Sbi-Target-apiRoot
GET
/nnrf-disc/v1/nf-instances?<query parameters>
:authority : sepp01.sepp.5gc.<Hop 1>.ipxnetwork.org
:3gpp-Sbi-Target-apiRoot : http://nrf.5gc.mnc002.mcc002.3gppnetwork.org
Route on 3gpp-Sbi-Target-apiRoot
GET
/nnrf-disc/v1/nf-instances?<query parameters>
:authority : sepp01.sepp.5gc.<Hop 2>.ipxnetwork.org
:3gpp-Sbi-Target-apiRoot : http://nrf.5gc.mnc002.mcc002.3gppnetwork.org
Route on 3gpp-Sbi-Target-apiRoot
GET
/nnrf-disc/v1/nf-instances?<query parameters>
:authority : sepp.5gc.mnc002.mcc002.3gppnetwork.org
3gpp-Sbi-Target-apiRoot : http://nrf.5gc.mnc002.mcc002.3gppnetwork.org
GET
/nnrf-disc/v1/nf-instances?<query parameters>
:authority : http://nrf.5gc.mnc002.mcc002.3gppnetwork.org
200 OK SearchResults
200 OK SearchResults
200 OK SearchResults
200 OK SearchResults
200 OK SearchResults

Figure 63 - E2E Traffic flow example

Annex F Security Profiles

F.1 Motivation

For N32 E2E security at application layer (implemented with PRINS), encryption and modification policies are established at IE level of granularity. There are a few thousands of IEs being used in the RESTful APIs used in 3GPP 5G SA roaming interfaces. Every roaming partner using PRINS needs to negotiate prior to the setup of the connectivity, whether IEs are confidentiality protected or readable in the clear, or also modifiable.

In order to make this task operationally manageable, 3GPP provides the option that the initiating SEPP indicates PRINS Security Profiles Support (see TS 29.573 [10], clause 6.1.7) in the parameter exchange request message towards the responding SEPP, which allows to include a candidate list of security profiles instead of detailed protection policy information. While 3GPP has defined the support, it is under the authority of GSMA to define a set of IE security policy templates, namely security profiles.

The standardisation of those security profiles aims to:

- avoid MNO's time and efforts in reviewing all relevant roaming APIs at IE level of granularity, and accordingly drafting the corresponding individual policies.
- streamline the policy negotiation time between MNOs (and roaming intermediaries) consolidated information on which IEs will be visible and may be modified, so as to consider what services can be provided.

NOTE 1: In the following an initial, limited set of templates is defined, which can be enhanced in the future. It is important to keep track per 3GPP Release of all service messages, which use the identified IE Data Types and need to be protected.

F.2 Security profile details

Security policy templates are a possible implementation of security profiles. Each security profile implemented by the corresponding template contains a list of ‘Protected’ IE Data Types and potentially a list of 'Modifiable' IE Data Types.

The term ‘Protected IEs’ refers to IEs that shall be encrypted, i.e. not available in clear text to roaming intermediaries. All other IEs are visible to the roaming intermediaries. In addition, a template can indicate 'Modifiable IEs’. These are allowed to be modified by roaming intermediaries as specified by 3GPP by adding signed patches with the modification needed.

3GPP has listed seven IE data types for ‘Protection’ policy (see clause 6.1.5.3.5, TS 29.573 [10]):

- UEID
- LOCATION
- KEY_MATERIAL
- AUTHENTICATION_MATERIAL
- AUTHORISATION_TOKEN
- OTHER
- NONSENSITIVE

NOTE 1: Since integrity protection cannot be deactivated, “protected” means encryption as well as protected against modification by means of JSON patching.

NOTE 2: Even though those are defined in the context of application layer security (i.e., PRINS), they can easily be generalized as ‘security data types’ independently of the selected security protocol as long as the MNO SEPPs have the N32-f context established and the necessary key material exchanged.

NOTE 3: FS.36 (annex A) [41] provides a data risk classification. Regular updates to align that classification with 3GPP APIs per release are required.

Profile A encrypts all IE data types identified above (except NONSENSITIVE which are visible, i.e. in the clear) and does not allow any modification of IEs. Profile B allows in addition for visibility (but not modification) of user identity, location, and other sensitive IE. Profile C allows for visibility and modification of all IEs except key material, authentication material, and authorisation token which are protected.

The following Table 7 summarises an initial set of profiles. The IE Data Types can be categorized as [encrypted,clear] and [modifiable,non-modifiable].

NOTE 4: An encrypted IE is by default non-modifiable.

Security profile	Profile A	Profile B	Profile C	Profile D	Profile E
UEID (Data of the type 'SUPI')	encrypted non-modifiable	clear non-modifiable	clear modifiable	clear non-modifiable	clear modifiable
LOCATION (location data)	encrypted non-modifiable	clear non-modifiable	clear modifiable	clear non-modifiable	clear modifiable
KEY_MATERIAL (cryptographic material)	encrypted non-modifiable	encrypted non-modifiable	encrypted non-modifiable	clear non-modifiable	clear modifiable
AUTHENTICATION_MATERIAL (authentication vector)	encrypted non-modifiable	encrypted non-modifiable	encrypted non-modifiable	clear non-modifiable	clear modifiable
AUTHORISATION_TOKEN	encrypted non-modifiable	encrypted non-modifiable	encrypted non-modifiable	clear non-modifiable	clear modifiable
OTHER	encrypted non-modifiable	clear non-modifiable	clear modifiable	clear non-modifiable	clear modifiable
NONSENSITIVE	clear non-modifiable	clear non-modifiable	clear modifiable	clear non-modifiable	clear modifiable

Table 10 - Security profiles

A profile describes the policy specific per roaming partner. The policy shall contain a policy identifier and a release number referring to the release it is applicable for. Encryption policies in the two MNO SEPPs shall be equal to enforce a consistent ciphering of IEs on N32-f.

For profiles A, B and C, a mapping between IE Data Types as indicated in the table and individual IEs is needed and is work in progress. Until this is completed, these profiles cannot be activated. Since no such mapping is required for Profile D and E, these profiles can be activated immediately. Similar to the hop-by-hop TLS architecture, the end-to-end application layer architecture (PRINS) with profile D and E provides roaming intermediaries with visibility to all information. But in contrast to hop-by-hop TLS, using PRINS with these profiles allows for attributability for both N32 endpoints and for intermediaries that introduce modifications via JSON patching. It should be noted that, while Profile E allows modification of the security material, such modifications, even though attributable, will lead to the inability of subscribers to connect to the visiting network.

Profile D shall be therefore the default for immediate activation.

F.3 Guidance on selection of protection level

Different criteria may be applied to decide on which protection level is needed, based on the particular use case, the trust level on intermediaries or contractual obligations among others.

For end to end security protection between two roaming peers, a minimum security profile with protection of key material, authentication vector and authorisation token and integrity protection of any other IE (called visible, not modifiable in above table) should be supported by the MNO SEPPs.

Any other profile with modification option allows the MNO to stay informed on who changed which IE in the path.

For full protection it is recommended to use roaming intermediaries as routing proxy only, thus protecting all the path between the roaming peers via direct bilateral TLS, i.e., in this case all IEs are by default confidentiality and integrity protected by TLS established between the two MNO SEPPs.

NOTE 1: PRINS can use these profiles in model 3 and model 4. Hop-by-hop TLS utilized as another security architecture for these models cannot use such profile, unless the N32-c handshake is done between both MNO SEPPs.

F.4 Reformatted message details

From the protection policy information (N32-f context), the SEPP knows the IE Data Types which need encryption and which are modifiable. The SEPP needs to identify per API the IEs, i.e. all service messages, in which the IE Data Type is used that needs specific handling.

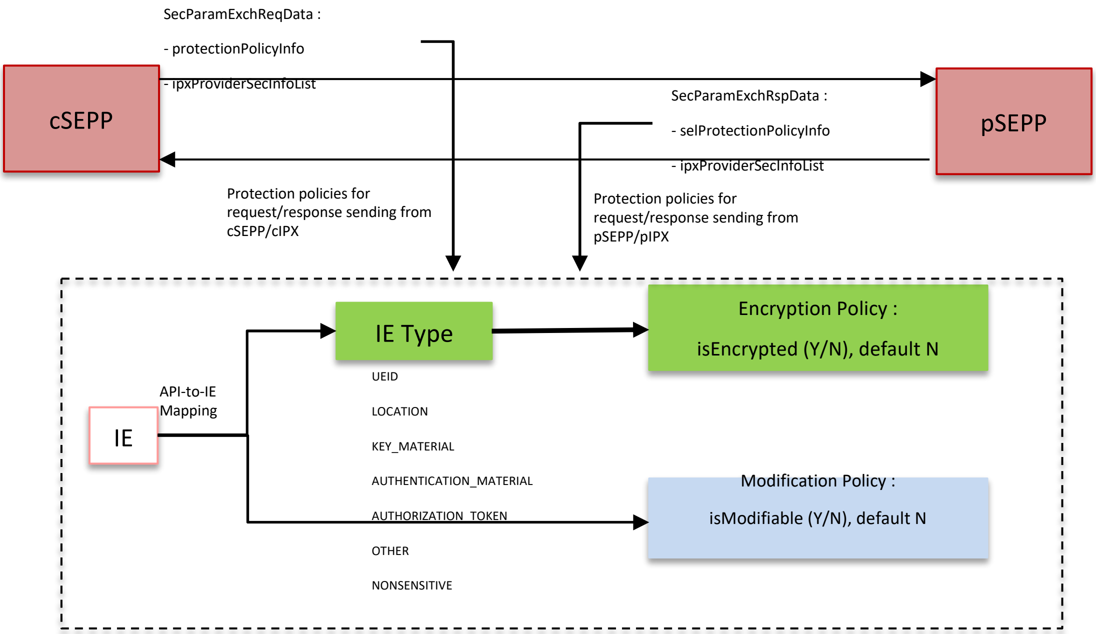


Figure 64 – Illustration of API to IE mapping

A SEPP on the sending side PMN applies the message reformatting as described in clause 5.3.2 of TS 29.573 [10]; Figure 5.3.2.3-1 is added here for illustration.

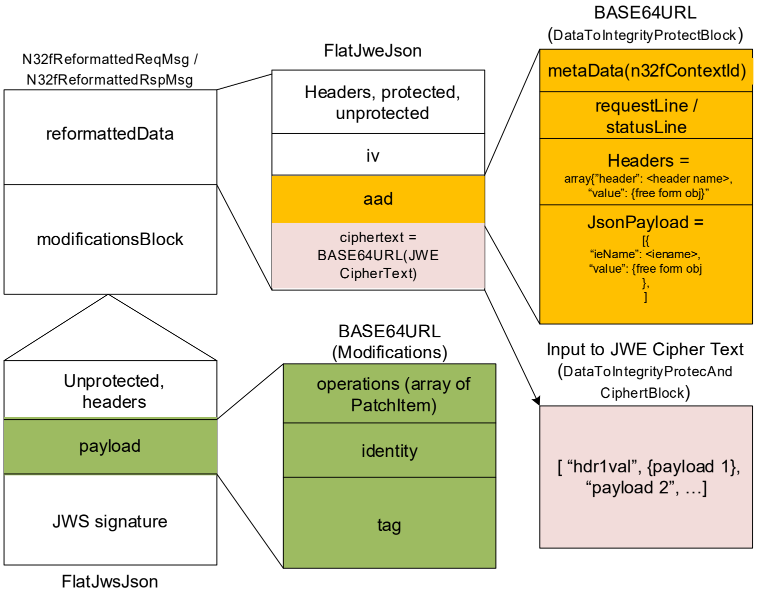

N32fReformattedReqMsg /
N32fReformattedRspMsg
reformattedData
modificationsBlock
Unprotected, headers
payload
JWS signature
FlatJwsJson
FlatJweJson
Headers, protected, unprotected
iv
aad
ciphertext = BASE64URL(JWE CipherText)
BASE64URL (Modifications)
operations (array of PatchItem)
identity
tag
BASE64URL (DataToIntegrityProtectBlock)
metaData(n32fContextId)
requestLine / statusLine
Headers = array{"header": <header name>, "value": {free form obj}"
JsonPayload = [{ "ieName": <iename>, "value": {free form obj },]
Input to JWE Cipher Text (DataToIntegrityProtecAnd CiphertBlock)
["hdr1val", {payload 1}, "payload 2", …]

Figure 65 – From clause 5.3.2.3-1, TS 29.573 [10]

Annex G Specific detailed design for inter-PLMN connection with Group SEPP

G.1 Introduction

The Group SEPP will appear to the roaming partner as a dedicated MNO SEPP that aggregates the PLMN IDs of all group affiliates.

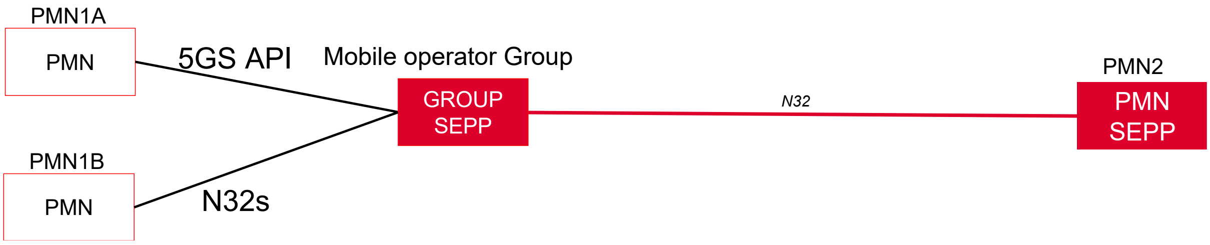


Figure 66 – Operator Group architecture

The Group SEPP can connect to an affiliate PLMN using one of the following interfaces:

- 5GS API: A direct connection to the affiliate's SCP or NF, following the same design principles as a PLMN SEPP, as defined in Annex B.
- N32s: A connection to the affiliate's SEPP*, using the N32s interface initially introduced in the Hosted SEPP architecture. This is detailed in Section 4.3.2.2.4 and Annex C.

This annex provides additional design considerations specific to the Group SEPP architecture.

G.2 Call Flows

G.2.1 N32 Dynamic SEPP discovery

The discovery of the Group SEPP on the N32 interface by the roaming partner follows the same principle as the direct case described in Section B.3.2. The roaming partner uses the well-known FQDN format sepp.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org to discover the Group SEPP FQDN via DNS.

G.2.2 TLS Connection Setup

The TLS connection for N32 will follow the same approach as the direct case described in Section B.3.2.

The Group SEPP's TLS certificates include all the group's PLMN IDs in the Subject Alternative Name (SAN) field.

The roaming partner's SEPP can validate the Group SEPP's leaf certificate using the Root CA or Sub-CA certificate provided by the Group SEPP provider. This certificate can be obtained via the RAEX certificate management tool, as defined in GSMA PRD FS.34 [37].

G.2.3 N32 Connection

The N32 connection follows the same approach as the direct case described in Section B.3.4.

However, a single N32 connection will be used by the roaming partner SEPP to connect to the Group SEPP, enabling access to all group affiliates.

The Group SEPP's TLS leaf certificate is also used to extract the list of PLMN IDs from the SAN field. These PLMN IDs are used to select the trust anchor and are compared against those sent over the N32-c interface.

G.2.4 Roaming route openings

The roaming partner will gradually enable 5G Standalone (SA) roaming with all affiliates of the Group. As a result, 5G SA roaming may be active with one affiliate while remaining inactive with others.

In order to prevent 5G SA roaming while there is not yet an agreement with a specific Group affiliate, certain blocking mechanisms can be applied based on the following scenarios:

Case 1: Group affiliate as the Home Network:

- Since there is no agreement yet, the roaming partner would not forward roaming traffic that would otherwise be generated at the visited AMF for the Group affiliate. In this case, no N32 signalling is initiated towards the Group SEPP.
- The Group affiliate (as Home Network) can also block the registration procedure by disabling roaming with the specific roaming partner in the UDM configuration. In this scenario, N32 signalling is initiated by the roaming partner towards the Group SEPP, and the Group SEPP forwards this to the affiliate even though the roaming agreement is not yet in place.

- The Group SEPP can be configured to reject registration requests coming from the roaming partner if no 5G SA roaming agreement exists. In this approach, no traffic enters the affiliate core.

Case 2: Group affiliate as the Visited Network

- Since there is no agreement yet, the group affiliate would not forward roaming traffic attempts at the visited AMF. In this case, the affiliate initiates no N32 signalling towards the roaming partner via the Group SEPP.
- The roaming partner (as Home Network) can also block the registration procedure by disabling roaming with the group affiliate in its UDM configuration. Here, N32 signalling is initiated by the group affiliate towards the roaming partner via the Group SEPP.
- The Group SEPP can be configured to reject registration requests originating from the group affiliate if the 5G SA roaming agreement is not in place.

NPTE: In some of the above scenarios the Group SEPP forwards signalling into the core of an affiliate without a roaming agreement being in place with that particular affiliate. However, this only happens if there is a roaming agreement with another affiliate, and in anticipation of the missing roaming agreement being established. Forwarding traffic without first the agreement in place comes with security implications since the role of SEPP is to ensure only legitimate traffic is forwarded.

Annex H Hybrid cases between MNO, HS and Group SEPP

H.1 Introduction

The following figure illustrates a hybrid case in which, for the same MNO, roaming partners can be connected to different SEPPs using different models.

- roaming partner 1 will be connected to PMN SEPP (using model 1),
- roaming partner 2 will be connected to Hosted or Group SEPP (using model 2.2 or 2.3). In this example, the larger number of roaming partners will be on model 2.

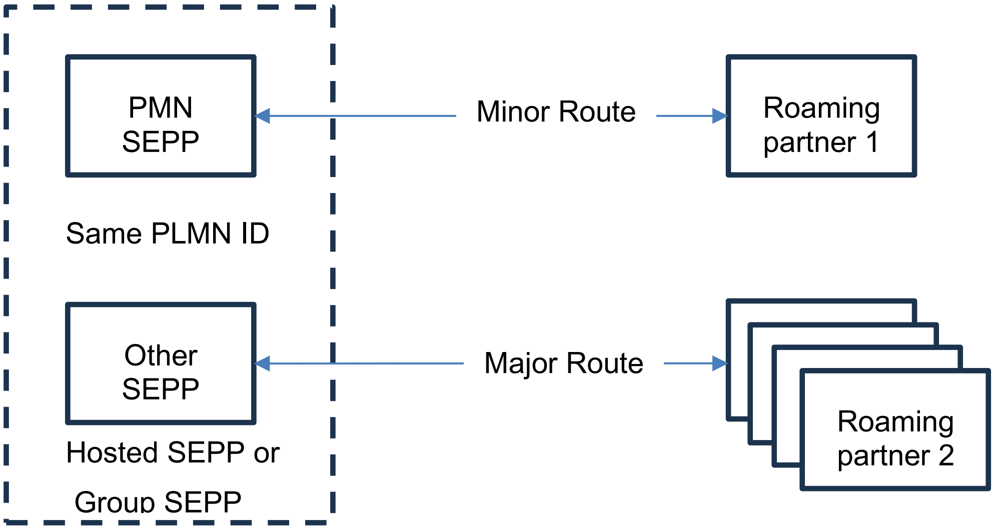


Figure 67– Hybrid case

Several options could be defined to resolve such hybrid cases, especially for the SEPP discovery procedure:

- Static configuration
- DNS resolution based on origin
- HTTP redirect

H.2 Static configuration

This solution will reuse the basic DNS SEPP discovery procedure for the major route (route with the larger number of roaming partners).

For the minor route, static configuration will be implemented in the initiating SEPP to discover always the SEPP related to minor route. Two options can be used:

- Static configuration of the SEPP FQDN
- Static configuration of a predefined FQDN (identifying the SEPP model), enabling DNS procedure to discover the one or several SEPP FQDN

H.3 DNS resolution based on origin

Another solution is to configure the authoritative DNS to provide different SEPP FQDNs based on the origin of the DNS query (roaming partner).

This solution requires a DNS Server with specific function (origin based) and the knowledge of IP ranges of the originating roaming partner.

H.4 HTTP redirect

A third option is to use the HTTP redirect function defined in Section 4.4.4.

One of the two SEPPs will be defined as the result of the standard DNS procedure to discover the SEPP.

This SEPP will receive all the N32-c and could redirect some of them to the other SEPP, depending on the roaming partner initiating the N32-c.

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	26 Sept 2019	PRD First Draft	TG	Mark McGinley, 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	Mark McGinley, AT&T
2.0	21 August 2020	Implementation of NG.113 CR1007	TG	Mark McGinley, 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	Mark McGinley, AT&T
4.0	11 May 2021	Implementation of approved CRs: NG.113 CR1023_rev5 NG.113 CR1024 NG.113 CR1025 NG.113 CR1026 NG.113 CR1027 NG.113 CR1028 NG.113 CR1029 NG.113 CR1030 NG.113 CR1031 NG.113 CR1032 NG.113 CR1033	TG	Mark McGinley, AT&T

5.0	13 December 2021	Implementation of approved CRs: NG.113 CR1034 NG.113 CR1035 NG.113 CR1036 NG.113 CR1037 NG.113 CR1038 NG.113 CR1039 NG.113 CR1040	TG	Mark McGinley, AT&T
6.0	11 May 2022	Implementation of approved CRs: NG.113 CR1041 NG.113 CR1042 NG.113 CR1043	TG	Mark McGinley, AT&T
7.0	29 November 2022	Implementation of approved CRs: NG.113 CR1044 NG.113 CR1045	TG	Mark McGinley, AT&T
8.0	June 2023	NG.113 CR1047 NG.113 CR1048 NG.113 CR1049 NRG 017_006 NG.113 guideline on gating NG.113 CR1050 NG.113 CR1052	ISAG	Javier Sendin, GSMA
9.0	February 2024	NG.113 CR1055 NG.113 CR1051 NG.113 CR1053	ISAG	Javier Sendin, GSMA
10	May 2024	Implementation of NG.113 CR1046, NG.113 CR1056, NG.113 CR1057, NG.113 CR1058, NG.113 CR1059, NG.113 CR1060, NG.113 CR1061, NG.113 CR1062	ISAG	Sandra Ondrusova, CK Hutchison
11	September 2024	Implementation of NG.113 CR1064, CR1065, CR1066, CR1069, CR1071, CR1073,	ISAG	Sandra Ondrusova, CK Hutchison
12	December 2024	Implementation of NG.113 CR1063, CR1074, CR1075, CR1076, CR1077, CR1078, CR1079, CR1080, CR1082, CR1083, CR1084, CR1086, CR1087, CR1088, CR1089, CR1090, CR1091.	ISAG	Sandra Ondrusova, CK Hutchison
13	June 2025	Implementation of NG.113 CR1094, CR1095, CR1096, CR1097, CR1098, CR1099, CR1101, CR1103, CR1104	ISAG	Sandra Ondrusova, CK Hutchison
14	December 2025	Implementation of NG.113 CR1100, CR1102, CR1105, CR1106, CR1107 CR1108, CR1109, CR1110, CR1111 CR1112, CR1114	ISAG	Sandra Ondrusova, CK Hutchison

Other Information

Type	Description
Document Owner	GSMA NG
Editor / Company	Sandra Ondrusova, CK Hutchison

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.