Report 5G Mobile Roaming Revisited (5GMRR)

Version 4.0

12 June 2023

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

Copyright © 2023 GSM Association

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 5
1.1 Overview 5
1.2 5GMRR Task Force 5
1.3 Scope 5
1.4 Phases of 5GMRR work 6
1.5 Abbreviations 6
1.6 References 7
1.7 Definitions 9
2 5G roaming architecture 9
2.1 Definitions 9
2.1.1 General 9
2.1.2 IP Exchange (IPX) 10
2.1.3 Roaming Value Added Service (RVAS) 10
2.1.4 Roaming Hub (RH) 10
2.2 Regulatory Considerations and Outsourcing 11
2.3 Control Plane and User Plane 11
2.3.1 Roaming 5G System Architecture 11
2.3.2 Roaming 5G Reference Points 12
2.3.3 Roaming 5G User Plane Aspects 12
2.3.4 Roaming Services 13
3 Requirements 13
3.1 Business/operational requirements 13
3.2 Technical Requirements 14
3.3 Security and Privacy Requirements 15
3.4 Assessment of the Requirements 15
4 State of the art 5GS roaming solutions 15
4.1 Background 15
4.2 PRINS 16
4.3 Direct TLS 17
4.4 Incompatibility PRINS and Direct TLS 18
4.5 Comparison PRINS versus Direct TLS 18
4.5.1 Direct TLS 18
4.5.2 PRINS 19
4.5.3 TLS/PRINS characteristics 20
4.5.4 TLS/PRINS pro/cons 20
5 Key issues 22
5.1 Security 22
5.2 Normalisation of messages 22
5.2.1 Normalisation of messages in 2G/3G/4G inter-PLMN traffic 22
5.2.2 Normalisation of messages in 5G inter-PLMN traffic 22
5.3 SEPP Security Configuration Criteria 23
5.4 When using SEPP and when using SCP? 23
5.5 How to secure SCP to SEPP? 23

5.6 Support of multiple PLMN IDs 23
5.7 Usage of TLS and PRINS between SEPPs 24
5.8 Originating network identification 25
5.8.1 Issues 25
5.8.2 3GPP Rel-17 defined HTTP custom header 3gpp-Sbi-Originating-Network-Id 25
5.8.3 Bilateral case 26
5.8.4 Hubbing case 26
6 Use cases 26
7 Roaming VAS 27
8 Naming, Addressing and Routing for 5G SA Roaming 27
8.1 SEPP Discovery 27
8.2 Naming scheme for non-MNO entities on the IPX Network 29
8.2.1 Introduction 29
8.2.2 Domain names and identifiers for MNOs 29
8.2.3 Domain names and identifiers for non-MNOs 29
8.2.4 Registration procedure 29
9 Mapping of Service Requirements and Defined Roles for the 5G SA Roaming Services outsourced to intermediaries 30
9.1 Introduction 30
9.2 Background of outsourced 5G SA Roaming Services 30
9.3 Mapping of Service Requirements for Roaming Hubbing to 5G SA Roaming Services 31
9.4 Requirements for Roaming Hubbing in relation to the Operators connected 34
10 Documentation 34
Annex A Guidelines for Inter-PLMN Connection 36
Annex B Considerations for SEPP Outsourcing 37
B.1 Overview 37
B.2 Outsourcing in 2G/3G/4G 38
B.3 Examples of Legal and Regulatory Requirements & Guidance 38
B.4 SEPP Selection Considerations 39
B.4.1 National Regulation 39
B.4.2 Regulatory Application 40
B.4.3 Supply Chain 41
B.4.4 Implementation 42
B.5 SEPP Outsourcing Conclusions 42
Annex C Considerations on PRINS for Roaming Hubs 44
C.1 Introduction 44
C.2 Solution details 44
C.3 Service Transparency 49
C.4 Evaluation 49
Annex D Hop-by-hop TLS Architecture 51
D.1 Introduction 51
D.2 Hop-by-hop TLS: Architecture Description for hosted SEPP 51

D.3 Hop-by-hop TLS: Architecture Description for hub SEPP 56
D.4 Hop-by-hop TLS: N32-f and N9 flows 58
Annex E Local PRINS (L-PRINS) for Roaming and Service Hubs 63
E.1 Introduction 63
E.2 End-to-end Attribution 63
E.3 Solution details 64
E.3.1 N32-c establishment using L-PRINS 64
E.3.2 Call Flow over N32-f using L-PRINS 65
E.4 Local PRINS Advantages 66
E.5 Evaluation 67
Annex F Security Profiles for PRINS 68
Annex G Document Management 70
G.1 Document History 70
G.2 Other Information 70

1 Introduction

1.1 Overview

This studt report provides the conclusions of the GSMA 5G Mobile Roaming Revisited (5GMRR) task force.

The report provides an outline of the 5GS roaming security architecture, how it is different from the roaming architecture in 4G/LTE, and how this architecture addressing the business, operational and security requirements.

A comparison of the existing 5GS roaming solutions as described in the 3GPP specifications (see TS 33.501 0, TS 23.501 0 and TS 29.573 0) is provided, followed by key issues, alternative potential solutions, and a decision criteria catalogue for the potential adaptation of solutions.

The report concludes with recommendations for the selected solution(s) and the follow-up actions in GSMA and 3GPP.

1.2 5GMRR Task Force

The role of the 5G Mobile Roaming Revisited (5GMRR) task force is to define realizable implementations using the 3GPP 5GS roaming security solution that optimally align the business needs, technical operation and security for 5G roaming. These requirement areas are present in 5GMRR Task Force through the participation of members of the following expert groups in GSMA, Wholesale Agreements and Solutions (WAS), Networks Group (NG) and Fraud and Security (FASG) as follows:

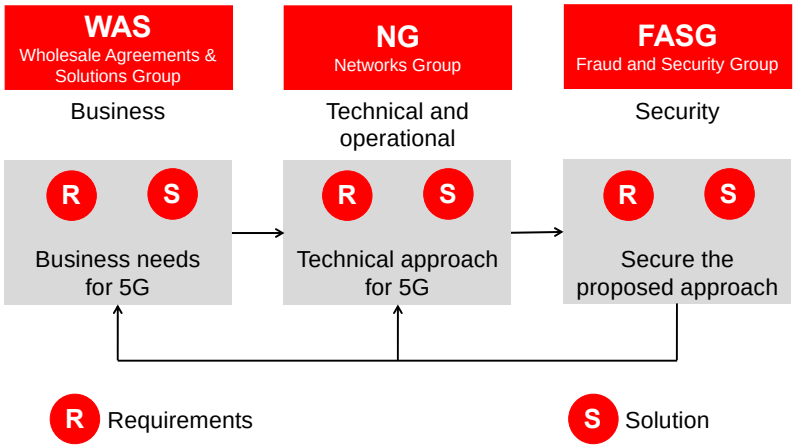


Figure 1 – Requirements & Solution Design

1.3 Scope

This document proposes a set of recommendations for the establishment of 5G roaming agreements between two MNOs both using 5GS Core considering the business needs of MNOs and intermediates.

1.4 Phases of 5GMRR work

In 5GMRR Phase 1 the use case descriptions are restricted to the bilateral inter-PLMN connections between two PLMNs. The detailed solution has been adopted in NG.113 Annex B 0 and is based on the following deployment principles and implementation restrictions:

- 5GS Roaming Architecture for bilateral inter-PLMN connections via Direct TLS connections between SEPPs typically via an IP routing, managed QoS service in the IPX network.
- Support of inter-PLMN Roaming Hub (RH) solutions for Operator Groups but without a description of the internal implementation details.
- Including support of PLMN solutions with Outsourced SEPP with a secure private interface between PLMN and Outsourced SEPP.
- The implementation details of the internal Roaming Value Added Services (RVAS) solution are not described.

In 5GMRR Phase 2 more 5GS roaming use cases are addressed with the involvement of intermediary service providers like by IPX, Hosted SEPP, Roaming VAS, and Roaming HUB incorporated in the roaming relations between v-PLMN and h-PLMN:

- Hosted SEPP…[description to be added in the process of 5GMRR Phase 2]
- Roaming Hub …[description to be added in the process of 5GMRR Phase 2]
- RVAS … [description to be added in the process of 5GMRR Phase 2]
- IPX … [description to be added in the process of 5GMRR Phase 2].

Further details are in … [to be added in the process of 5GMRR Phase 2].

1.5 Abbreviations

Term	Description
5GC	5G Core Network
5GMRR	5G Mobile Roaming Revisited
5GS	5G System
APT	Advanced Persistent Threat
B2BUA	Back-To-Back User Agent
CNI	Critical National Infrastructure
CoP	Codes of Practice
CP-SOR	Control Plane Steering Of Roaming
DEA	Diameter Edge Agent
DRC	Data Roaming Control
E2E	End-To-End
EECC	European Electronic Communications Code
ENISA	European Union Agency for Cybersecurity
EPC	Evolved Packet Core
GDPR	General Data Protection Regulation
HPLMN	Home Public Land Mobile Network

Term	Description
hSEPP	Home Secure Edge Protection Proxy
IMSI	International Mobile Subscriber Identity
IPUPS	Inter-PLMN User Plane Security
IPX	IP Exchange
L-PRINS	Local PRINS
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
NF	Network Function
PLMN	Public Land Mobile Network
PRD	Permanent Reference Document
PRINS	PRotocol for N32 INterconnect Security
pSEPP	Producer Security Edge Protection Proxy
RH	Roaming Hub
RVAS	Roaming Value Added Services
SBA	Service Based Architecture
SBI	Service Based Interfaces
SCP	Service Communication Proxy
SEPP	Secure Edge Protection Proxy
SLA	Service Level Agreement
SLO	Service Level Objective
SMSF	Short Message Service Function
SMSoIP	SMS over IP
SMSoNAS	SMS over 5G NAS
SOR-AF	Steering Of Roaming Application Function
SUPI	Subscription Permanent Identifier
TEID	Tunnel Endpoint ID
TLS	Transport Layer Security
TSR	Telecoms Security Requirements
UPF	User Plane Function
VAS	Value Added Services
VPLMN	Visited Public Land Mobile Network
vSEPP	Visited Secure Edge Protection Proxy

1.6 References

Ref	Doc Number	Title
	3GPP TS 33.501	Security architecture and procedures for 5G
	IETF RFC 7540	Hypertext Transfer Protocol Version 2 (HTTP/2)
	IETF RFC 793	Transmission Control Protocol (TCP)

Ref	Doc Number	Title
	IETF RFC 7159	The JavaScript Object Notation (JSON) Data Interchange Format
	GSMA PRD IR.73	Steering of Roaming Implementation Guidelines
	GSMA PRD NG.113	5GS Roaming Guidelines
	3GPP TS 23.501	System architecture for the 5G System (5GS)
	GSMA PRD FS.21	Interconnect Signalling Security Recommendations
	GSMA PRD FS.36	5G Interconnect Security
	3GPP TR 29.829	Technical Specification Group Core Network and Terminals; Service-based support for SMS in 5GC (Release 17)
	3GPP TS 23.122	Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode
	3GPP TS 29.550	Technical Specification Group Core Network and Terminals; 5G System; Steering of roaming application function services; Stage 3
	ENISA	Guideline on Security Measures under the EECC https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc
	ENISA	5G Supplement - to the Guideline on Security Measures under the EECC https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc
	EU Toolbox	The EU toolbox for 5G security https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security
	NCSC	Security analysis for the UK telecoms sector https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf
	UK Cabinet Office	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf
	GSMA PRD AA.51	IPX Definition
	GSMA PRD IR.34	Guidelines for IPX Provider networks
	GSMA PRD BA.60	Roaming Hubbing Handbook
	GSMA PRD BA.62	Roaming Hubbing Business Requirements Commercial Model
	GSMA PRD BA.63	Roaming Hubbing Hub to Hub Operational Procedures
	S3-212287	Change Request 33.501 CR 1080 rev 1 v16.6.0 “Clarification on the number of PLMN ID use by SEPP over N32”
	S3-212367	Change Request 33.501 CR 1105 rev 1 v15.12.0 “Clarify the usage of TLS and PRINS between SEPPs”
	3GPP TS 29.573	Technical Specification Group Core Network and Terminals; 5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3
	GSMA PRD FS.34	Key Management for 4G and 5G inter-PLMN Security

Ref	Doc Number	Title
	UK TSR	United Kingdom Telecom Security Requirements, not yet published.
	GSMA PRD IR.21	GSM Association Roaming Database, Structure and Updating Procedures
	GSMA PRD IR.67	DNS Guidelines for Service Providers and GRX and IPX Providers
	GSMA PRD IR.80	Technical Architecture Alternatives for Open Connectivity Roaming Hubbing Model
	GSMA PRD IR.85	Hubbing Provider Data, Structure and Updating Procedures
	GSMA PRD AA.73	Roaming Hubbing Client to Provider Agreement
	By Anand R. Prasad and others	3GPP 5G Security, 6 August 2018 https://www.3gpp.org/news-events/1975-sec_5g
	EC	Revised Directive on Security of Network and Information Systems (NIS2), 12 May 2019 https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2
	Cyprus DSA	The Security of Networks and Information Systems Law (law 89(I) of 2020) https://dsa.cy/images/pdf-upload/Decision-310-2021.pdf
	EU Regulation 2016/679	General Data Protection Regulation (GDPR) https://gdpr-info.eu
	UK Parliament	Telecommunications (Security) Act 2021 https://bills.parliament.uk/bills/2806
	UK Department for Digital, Culture Media & Sport	Draft Telecommunications Security Code of Practice https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1057446/Draft_telecoms_security_code_of_practice__accessible_.pdf
	Financial Times	The great hack attack: SolarWinds breach exposes big gaps in cyber security https://www.ft.com/content/c13dbb51-907b-4db7-8347-30921ef931c2
	3GPP TS 29.500	5GS; Technical Realization of Service Based Architecture; Stage 3

1.7 Definitions

Term	Description
Attribution	The principle of identifying and documenting the specific entity responsible for a particular action.

2 5G roaming architecture

2.1 Definitions

2.1.1 General

IP Exchange (IPX) providers and Roaming Value Added Services (RVAS) providers are important stakeholders in the IPX ecosystem and in the framework of the whole roaming

services ecosystem. In addition, Roaming Hubs (RH) offer a special deployment model in the IPX ecosystem that is typically suited to provide roaming services to two or more Mobile Network Operators (MNO) who have no roaming agreements with each other.

The IPX, RVAS and RH provider roles are independent of the legal entity that has these roles. A single legal entity can have multiple instances of these roles in parallel and can offer multiple services in parallel.

The following definitions only apply to the 5GS roaming traffic between a 5G Core network in the HPLMN and a 5G Core network in the VPLMN including the ongoing session context when PDU sessions are to be handed over to/from EPC and 5GC in LTE/5G interworking situations.

2.1.2 IP Exchange (IPX)

An IP Exchange (IPX) provider is an interconnect partner enabling transport of inter-PLMN traffic between operators on the IPX network. Service Level Agreements (SLAs), specific Service Level Objectives (SLOs), bandwidth guarantees, and latency guarantees may be part of the service provided.

A more elaborated list of IPX services and its supported roaming services is included in section 2.3.4. For further details of the IPX network and the IPX services please see:

- GSMA PRD AA.51 “IPX Definition” 0 that provides an overview of both the key components of the IPX network and a summary of the defined IPX services.
- GSMA PRD IR.34 “Guidelines for IPX Provider networks” 0 that gives guidelines and technical information on the IPX network consisting of the IP interconnection backbone of IPX Providers and GPRS Roaming eXchange of GRX Providers.

2.1.3 Roaming Value Added Service (RVAS)

A RVAS provider is an external entity, acting outside the perimeter of the MNO’s network domain, providing RVAS business services to an MNO. The services provided may include services that serve the subscriber (e.g. roaming control service, roaming welcome SMS), or those that serve the network (e.g. to solve interoperability issues, corrective actions). The use of RVAS is optional for MNOs.

For further details of the services and implementation guidelines for RVAS please see section 7.

2.1.4 Roaming Hub (RH)

The Roaming Hub (RH) provides a set of services to client MNOs to facilitate the deployment and operation of roaming and interworking services, often in a selectable ‘a la carte’ type set of options. Functions and operations like RVAS, routing, filtering, testing, troubleshooting, billing, invoicing, and dispute management will need to continue to be provided by RHs in 5GS roaming to preserve the range of services currently provided to client MNOs.

Within the roaming ecosystem , the RH is a separate entity that acts like a VPMN for HPMNs, and an HPMN for VPMNs. Client MNOs (clients of the roaming hub) have one

roaming hub agreement with the RH provider in order to have roaming relations with participating client MNOs.

In order to avoid fraud and to ensure consistency a RH does not manipulate content, format or any information related to the traffic transmitted through its solution, unless manipulation is explicitly required within GSMA specifications or required by local regulations and laws, or subject to arrangements made between two parties.

For further details of RH service offering and definitions please see:

- GSMA PRD BA.60 “Roaming Hubbing Handbook” 0 that provides an overview about Roaming Hubbing.
- GSMA PRD BA.62 “Roaming Hubbing Business Requirements Commercial Model” 0 summarizing the commercial high level commercial requirements on Roaming Hubs and their commercial relationships to Client Operators including mandatory requirements on the commercial relationship between Roaming Hub and Client(s).
- GSMA PRD BA.63 “Roaming Hubbing Hub to Hub Operational Procedures” 0 that defines the operational procedures for efficient interconnection, interworking and interoperability between Roaming Hubs.

2.2 Regulatory Considerations and Outsourcing

The 5GS roaming architecture and procedures allow the outsourcing of edge elements, i.e. SEPP to third parties, although this business scenario and its implications are thus far not specifically addressed in 3GPP specifications TS 33.501 0, TS 23.501 0 and TS 29.573 0.

There are different regulatory frameworks, such as the EU Toolbox 0 and the United Kingdom Telecom Security Requirements (TSR) [27], that describe specific conditions for outsourcing of functions and actions within a jurisdiction. It is the responsibility of all companies subject to the specific regulations to comply with local regulatory frameworks.

Please see Annex B for the results of a survey that was undertaken by the GSMA to identify the possible national approaches and regulations for outsourcing of the SEPP function in different regions and countries. Any position on SEPP Outsourcing will vary significantly with each individual country and potential outsource.

Further security considerations for SEPP outsourcing are given in section 14.4 in FS.21 0.

2.3 Control Plane and User Plane

2.3.1 Roaming 5G System Architecture

In the 5G System Architecture a clear separation is made between the Control Plane and User Plane network functions and reference points as outlined in 3GPP TS 23.501 0. Figure 2 shows this split between the N32-based Control Plane and the N9-based User Plane as part of the Roaming 5G System Architecture.

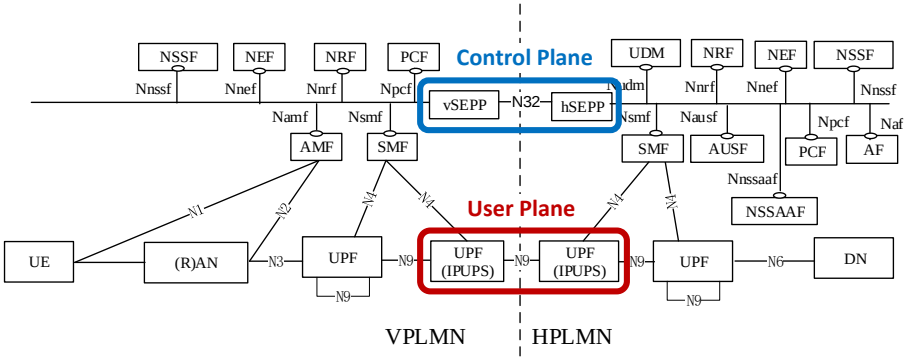


Figure 2 – Roaming 5G System Architecture

2.3.2 Roaming 5G Reference Points

Based on the list of reference points in 3GPP TS 23.501 0, Figure 3 provides an overview of the control plane reference points that can apply end-to-end (E2E) between the 5G Core network functions of roaming partners.

N32: Reference point between SEPP in the visited network and the SEPP in the home network.
N8: Reference point between the UDM and the AMF.
N10: Reference point between the UDM and the SMF.
N12: Reference point between AMF and AUSF.
N14: Reference point between two AMFs.
N15: Reference point between the PCF and the AMF in the case of non-roaming scenario, PCF in the visited network and AMF in the case of roaming scenario.
N16: Reference point between two SMFs, (in roaming case between SMF in the visited network and the SMF in the home network).
N24: Reference point between the PCF in the visited network and the PCF in the home network.
N27: Reference point between NRF in the visited network and the NRF in the home network.
N31: Reference point between the NSSF in the visited network and the NSSF in the home network.
N58: Reference point between AMF and the NSSAAF

E2E Control Plane
Indirect Control Plane via N32

Figure 3 – Roaming 5G Reference Points for the Control Plane

Please note that N32 is the only control plane reference point between the 5GC networks of roaming partners. All control plane interactions are exchanged via this N32 reference point.

In parallel, the N9-based User Plane signalling messages for the UPF (IPUPS) interactions are exchanged via the N9-based User Plane reference point.

2.3.3 Roaming 5G User Plane Aspects

Note – Postponed till 5GMRR Phase 2.

2.3.4 Roaming Services

The support of RVAS is considered a home operator internal deployment specific matter in 5GMRR Phase 1. As a result, the implementation details of the internal RVAS solution are not described in 5GMRR Phase 1.

For this phase RVAS are provided on behalf of the HPLMN. If and how RVAS could be provided by VPLMN could be envisaged for new 5G services at a later point in time. The only exception is 'welcome SMS', which service interaction needs to be aligned with HPLMN anyway (and not applicable when 'welcome SMS' will be based on IMS).

Note – Further RVAS descriptions are postponed till 5GMRR Phase 2.

For the support of RVAS with features like 'welcome SMS', the solution may depend on cross-generation access via previous mobile generation systems when the UE switches between 2G/3G/4G/5G within the VPLMN; note that the signalling between VPLMN and HPLMN switches from HTTP to Diameter to SS7 in case there are parallel links. This may involve security risks for 5G users during roaming as clarified in both NG.113 0 and FS.21 0 under "Risks from Interworking with Different Technology Generations and Signalling Protocols". Additional guidance on the use of correlation between protocol instances can be found in FS.21 0 under "Correlation Across Interconnect Signalling Protocols".

3 Requirements

3.1 Business/operational requirements

Global roaming is a key service offering for MNOs. From a service and customer satisfaction perspective, ensuring the reliability and security of international roaming services is important. The 3GPP security principles of the 5GS are strongly supported by the operator roaming community.

Considering the business models that have developed and flourished to support the global roaming ecosystem, there are several principles that the GSMA's roaming groups believe are vital requirements and need to be supported when considering 5G security deployment models.

Foremost across all requirements for 5G roaming security is the strong desire for a single 5G roaming deployment (architecture) model that would support the majority of MNOs and roaming ecosystem partners. In practice, this would mean that the security deployment model should be clearly defined so that it does not need to be a negotiating point per roaming agreement.

The industry has experienced significant delays and effort to deploy VoLTE roaming, with initial delays stemming from the availability of multiple deployment architectures and associated business cases. With this lesson learned, multiple security deployment model choices for each use case should be avoided for 5GS roaming, understanding there will be significant complexity associated with deploying these new security solutions and elements. Having multiple deployment options that require additional bi-lateral negotiation and agreement for every roaming partner will impact the timing and proliferation of global 5GS roaming.

Along with the deployment approaches, the GSMA roaming groups evaluated the 5G roaming security requirements against the following categories: contractual; flexibility, practicality, and business needs. From a contractual standpoint, the roaming partners and ecosystem partners will continue to operate using contract vehicles that hold each party accountable with clarity of role, responsibility, privacy, and liability at a minimum. As the baseline for enabling and opening roaming, the contract vehicle can be enhanced to support any new security requirements should that be needed, including the new security requirements in the roaming contract will support compliance.

The analysis of the requirements concluded that while implementing new 5G roaming security methods, the overall ecosystem partner functions need to continue to be supported as they are critical to enabling the global roaming products for all types of MNOs. However, while important to support the business and partner functions, the solution(s) should not compromise the security and privacy of the data exchanged. Some specific examples that illustrate the concept are the need to ensure support for the Roaming Hubbing Model and similarly the concept that some MNOs may need to delegate their 5G Roaming Security controls in order to engage in the 5G Roaming ecosystem. In addition, the solution will need to account for the regulatory requirements across different regions.

Roaming Value Added Services (RVAS) are an enabler to the roaming ecosystem and enhance the roaming experience for consumers and support their MNO customers with additional capabilities. These RVAS services need to be supported across 5G roaming, however their use should not break the security model designed or endorsed. While relying on many of these RVAS capabilities, the MNOs wish to maintain their independence and do not want the RVAS decisions of their roaming partners to impact their own operations. Visibility to the originating and terminating MNO is needed for a variety of applications/reasons, even when an MNO outsources a particular function. This requirement needs to be supported alongside the need to maintain the integrity and confidentiality of the message content from the terminating MNO. A clear example of this is steering of roaming.

To keep flexibility, the 5GS roaming solution should be designed in a transparent way that technical and security controls do not have to be adjusted to enable an RVAS. RVAS may change over time and new RVAS may come up in the future. Such innovation should not be hindered. However, changes to RVAS will always have to be in the bounds of the roaming agreements and meet the other requirements set out in this document.

Finally, having clear, detailed technical and business deployment guidelines will help ensure that secure 5G roaming is implemented with a high degree of interoperability, minimize deployment issues and support a robust global 5G ecosystem.

3.2 Technical Requirements

From the technical perspective, the 5GS roaming solution should consider the following:

- Signaling messages need to be exchanged between MNOs. As defined in the 3GPP 5GS standard, signaling messages are exchanged between roaming partners, as it is done for the previous mobile generations.
- An MNO may want to deploy multiple SEPPs for redundancy and load sharing purposes. The 5GS roaming architecture considers this and supports routing and load sharing accordingly.

- To have the least possible impact on the 3GPP specification, the overall number of network functions (NF), involved in 5G roaming should be minimal. Ideally, only the SEPP and the IPUPS perform all 5G roaming security controls for the roaming interface and no other NF is affected. This provides maximum transparency for other NF and simplifies implementation and operation.

From operational perspective, the additional effort for operating 5G roaming should only be slightly higher than existing roaming solutions. The overall 5GS roaming solution, its security controls and its key management procedures should add as minimal extra effort as possible.

The detailed solution is described in NG.113 Annex B 0.

3.2.1 Security and Privacy Requirements

As defined by 3GPP in TS 33.501 0, the following security and privacy requirements should be met by the 5GS roaming solution.

- The solution shall ensure that signaling messages cannot be manipulated, tampered, or injected by a malicious actor – authenticity and integrity, handled by the SEPP, are required.
- In 5GMRR Phase 1 with TLS connections used between SEPPs, both integrity and confidentiality protection apply to all attributes transferred over the N32 interface.
- IPUPS, as defined by 3GPP Release 16, shall be used. Likewise, a secure N9 message transfer shall be deployed between all MNOs. 3GPP requires the use of NDS/IP.
- The destination network shall be able to determine the authenticity of the source network that sent a signaling message.
- The solution shall prevent replay attacks, and cover algorithm negotiation and prevention of bidding down attacks.
- Standard security protocols should be used.
- Operational aspects of key management should be taken into account.

5GMRR identified that in addition to the above requirements, recipients of messages shall be able to determine the originating MNO.

Note: This should equally apply for the case, that a SEPP is outsourced and operated by another trusted entity on behalf of the origin MNO as in alignment with the specific security considerations for SEPP outsourcing in Annex B as well as in section 14.4 in FS.21 0.

3.3 Assessment of the Requirements

Note: Postponed till 5GMRR Phase 2 when the full solution for 5G SA Roaming is defined.

4 State of the art 5GS roaming solutions

4.1 Background

In previous generations of mobile networks inter-operator signalling security was difficult to achieve due to early telephony signalling legacy.

5G addresses the problem in the 3GPP specifications by enabling confidence in signalling integrity and confidentiality and gives the ability to establish authenticity through either:

- end-to-end communication security using Direct TLS, see section 4.3, or
- where intermediaries are used (Hubs, IPX carriers and Value Added Services) 3GPP PRINS to secure the interconnect, see section 4.2.

Additionally, 5GS was designed to ensure attribution as it is defined in section 1.7. Evaluation of the different deployment options for RH, described in Annexes C and D, include whether attribution can be ensured.

The following sections summarize the options for 5G Roaming with PRINS and Direct TLS at the start of the 5GMRR task force. It should be noted that this is an open, current discussion and requires further consultation and validation by WGs and membership as part of the work by this task force.

4.2 PRINS

The PRotocol for N32 INterconnect Security (PRINS) model for the support of 5G roaming is shown in Figure 4. The use of PRINS is negotiated via N32-c (not depicted).

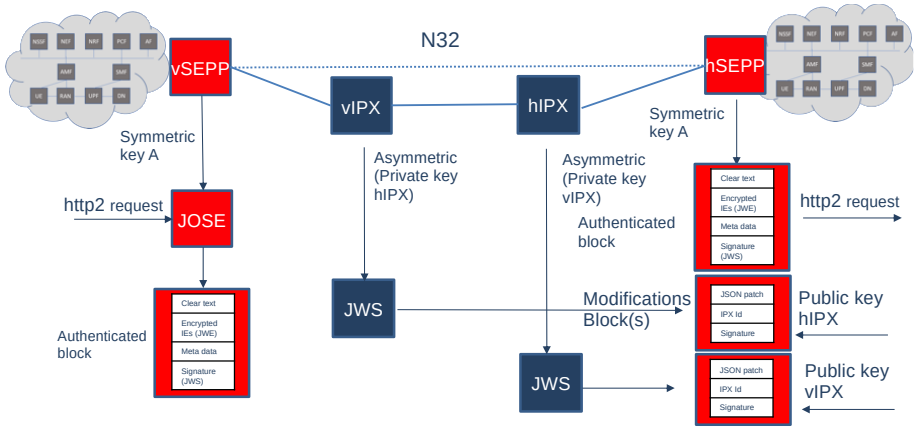


Figure 4 – PRotocol for N32 INterconnect Security (PRINS) model for 5G roaming

The PRINS model is designed to fulfil the following:

- Confidentiality and integrity of sensitive information elements during transport via vIPX and hIPX, while still allowing modifications and offering services. Sensitive information is secured end-to-end[1].

[1] A differentiation between non-/sensitive IEs is postponed till 5GMRR Phase 2.

- Traceability and attribution of potential changes and modifications to signalling between PLMNs.

However, when analysing PRINS, the following difficulties were detected when using PRINS with modifications by intermediaries:

- Creates operational complexity as signalling consuming MNO needs to perform extensive policy checks:
    - Protection Policies may vary per partner MNO
    - Roaming agreement may vary per partner MNO
    - JSON Patch control for both visited and home network IPX carriers
- Operators will need to be aware of which intermediary IPX is allowed to modify messages, as well as of public keys of these intermediaries.

As a result, introduction of the PRINS model would require solutions that address the complexity for Contracts, Operation and Security that it brings.

Annex C shows that PRINS can be applied for integrating Roaming Hubs, addressing the challenges pointed out above.

As a result, introduction of the PRINS model would require solutions that address the complexity for Contracts, Operation and Security that it brings.

In the interest of business continuity, Annex D presents the Hop-by-Hop TLS architecture that recognizes service provider relations that serve a collection of (international) roaming relations. This illustration covers the case where only one operator has outsourced services, the case where both operators have outsourced services, and covers the common part for both options.

Annex E shows a solution in which PRINS protocol is used as a single solution and combined approach for the Roaming Hub and Service Hub use cases by using PRINS as a local protocol between consecutive hops. This approach is called Local PRINS (L-PRINS).

This solution provides a hop-by-hop PRINS solution and a possible milestone towards end-to-end security as it is anticipated that end-to-end security could become mandatory in the future or desired by operators.

To facilitate and simplify the deployment and operation of PRINS, security profiles could be introduced. Annex F provides a proposal.

4.3 Direct TLS

The Direct TLS model for the support of 5G roaming is shown in Figure 5. The use of direct TLS is negotiated via N32-c (not depicted).

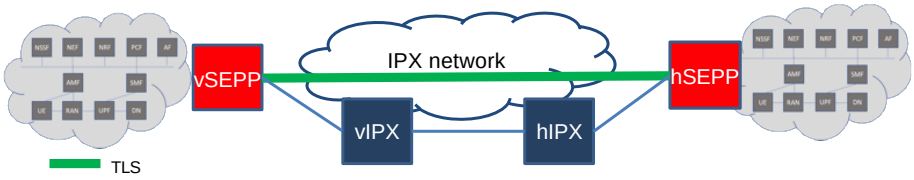


Figure 5 – Direct TLS model for 5G roaming

The Direct TLS model is characterised as follows:

- Signalling producing MNO in full control of HTTP/2 message content send to consuming MNO
- Operational simplicity as consuming MNO only needs policy checks for Roaming Agreements per producing MNO.
- Signalling information secured end-to-end between both MNOs
- Intermediaries not possible unless there is willingness to disclose all information including UE keying material and authentication tokens to the intermediary.

4.4 Incompatibility PRINS and Direct TLS

The 3GPP standard TS 33.501 0 prescribes that for N32-f either Direct TLS is to be used end-to-end for a roaming relation if intermediaries on the path are routed on IP layer only, or alternatively, PRINS, if intermediaries should be able to read and modify signalling messages in an operator controlled manner. If PRINS is used, the communication is end-to-end secured at application layer on top of TLS, which is applied hop-by-hop securing communication between intermediaries at the transport layer. From a deployment perspective, this is negotiated between both 5GS roaming partners in N32-c.

Note: In this context intermediaries according to 3GPP are network elements that can read a message and possibly also can add a modification. In the TLS end-to-end case, there is no possibility for an RVAS provider and/or IPX provider to intervene as the whole message content is confidentiality protected end-to-end. PRINS allows RVAS providers and IPX providers to intervene at the application layer according to the security policy applied to the underlying roaming agreement.

4.5 Comparison PRINS versus Direct TLS

In order to compare PRINS and Direct TLS, the following elements are taken into account:

- Three different cases (bilateral with MNO SEPP, bilateral with outsourced SEPP, roaming hubbing)
- VAS could be provided at different level (before/after the SEPP or in transit)

4.5.1 Direct TLS

SEPPs are connected directly via TLS using N32 interface which could be fully encrypted, see Figure 6.

N32-c connection: A TLS based connection between a SEPP in one PLMN and a SEPP in another PLMN. Used to negotiate TLS as security policy for N32-f.

N32-f connection: Logical connection that exists between a SEPP in one PLMN and a SEPP in another PLMN for exchange of protected HTTP messages via the same TLS connection as used for N32-c.

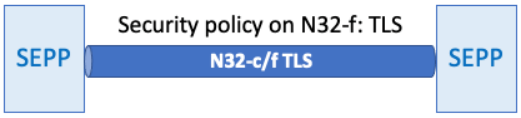


Figure 6 – Direct TLS Architecture

TLS offers end-to-end protection of full message content on the N32-f connection between both SEPPs.

MNO could use different approaches to connect the SEPP.

SEPP could be directly provided by the MNO, and VAS could be hosted by the MNO or a 3rd party.

SEPP could be outsourced by the MNO to IPX providers, and VAS could be also outsourced.

Roaming traffic could be managed by a Roaming Hub, based a SEPP connectivity.

4.5.2 PRINS

PRINS architecture combined the N32-c connection and N32-f connection to provide both transport and application level security, see Figure 7.

N32-c connection: A TLS based connection between a SEPP in one PLMN and a SEPP in another PLMN. Used to negotiate PRINS as security policy for N32-f and to negotiate the N32-f specific associated security configuration parameters required to enforce application layer security on HTTP messages exchanged between the SEPPs.

N32-f connection: Logical connection that exists between a SEPP in one PLMN and a SEPP in another PLMN, via two IPX providers, each associated with one of the PLMNs, for exchange of protected HTTP messages.

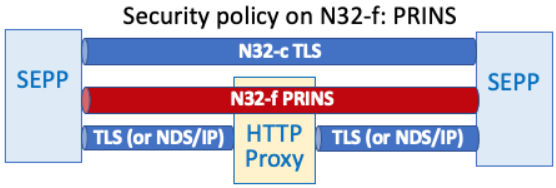


Figure 7 – PRINS Architecture

Full end-to-end protection on the N32-f connection is provided by the upper PRINS layer with sensitive IEs protected at the intermediate HTTP Proxy signalling hops. The underlying

TLS (or NDS/IP) layer offers hop-to-hop protection of full message content of the N32-f connections between the SEPP and HTTP Proxies.

Compared to Direct TLS, MNO could use RVAS provided by IPX in transit on the N32-f interface based on the non-encrypted fields.

4.5.3 TLS/PRINS characteristics

Table 1 summarises the major signalling characteristics and highlights the difference between direct TLS and PRINS.

	TLS	PRINS
N32-c IPX role	IP carrier (SEPP-SEPP)	IP carrier (SEPP-SEPP)
N32-f IPX role	IP carrier (SEPP-SEPP)	HTTP proxy (SEPP-IPX-IPX-SEPP)
5GC Signalling Security Transport layer	End-to-end (SEPP-SEPP) Integrity protection and encryption	Hop-by-hop (SEPP-IPX-IPX-SEPP) Integrity protection and encryption
5GC Signalling Security Application layer	Not protected	End-to-end (SEPP-SEPP) Integrity protection Partly Encrypted
Actors for Security keys	SEPP	SEPP / HTTP proxy
SEPP outsourcing	Possible	Possible
Coupling security/VAS	No	Yes
Hubbing	MNO like	MNO like

Table 1 – Differences between Direct TLS and PRINS

4.5.4 TLS/PRINS pro/cons

Table 2 summarises the pros/cons between direct TLS and PRINS in case of using intermediate hops (e.g. RH, IPX Provider).

With the model in Figure 8, TLS offers hop-by-hop protection of full message content between SEPPs, hop-by-hop security protection of full message content between SEPPs is provided. However, this concatenation of hop-by-hop TLS connections introduces additional risk by allowing 3rd parties to gain full access to signaling and allowing an intermediary node to hide the originator information.

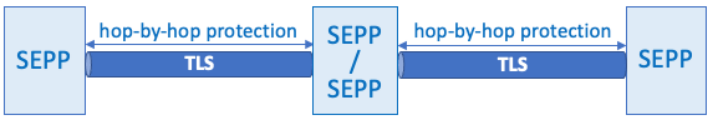


Figure 8 – Direct TLS used with intermediate hops

With the model as in Figure 9, PRINS provides end-to-end protection for sensitive IEs at signaling hops for the confidentiality protected IEs via the PRINS ALS layer.

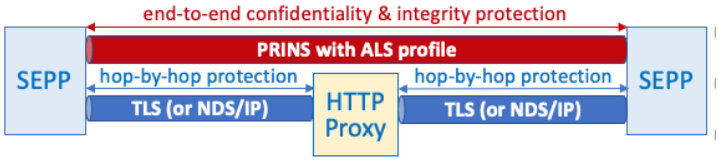


Figure 9 – PRINS used with intermediate hops

PRINS provides a more granular and flexible security handling of data transferred between SEPPs.

From a security point of view, who attaches or modifies a particular Information Element in the chain when an IPX is involved, may be controlled by one of the communicating parties. Thus, it should be kept as an option in designing a 5G security interconnect solution. Any operational burdens, in terms of human effort can be optimized with software options such as providing IPX providers with profiles on modification policies.

	Pros	Cons
Direct TLS	End-to-end encryption IPX usage for pure IP No audit trail is needed (all changes are within each operator's domain and no intermediate changes by IPX providers)	No transit VAS
PRINS	Transit VAS possible (for example signalling normalisation) End-to-end sensitive information element protection Traceability for modifications Most information elements accessible by IPX provider	IPX to provide http proxies for N32-f More actors for security keys (IPX providers) Security policy profiles per N32-f Coupling of security and (transit) VAS policies

Table 2 – Pros/Cons between Direct TLS and PRINS

Note: Transit VAS use cases are quite limited (not used for hubbing, sponsor IMSI or MVNO)

The comparison in Table 2 mixes transport and application security. N32-f HTTP/2 traffic in PRINS between Operator and the IPX provider is subject to be protected by NDS/IP. It can be done via TLS or even IPSec, of course hop by hop. It is just a transport security mechanism between networks.

5 Key issues

5.1 Security

For a description of security issues please refer to FS.21 0 section 14 “Holistic Security approach for Mobile Roaming services”. This is specifically developed and written in the context of 5GS roaming and addresses the following aspects:

- Security Considerations
- Security Recommendations
- Specific considerations SEPP Outsourcing.

In addition, please refer to FS.34 0 for considerations of Key Management.

5.2 Normalisation of messages

Normalisation in this context refers to modification of certain attributes in inter-PLMN traffic. This is typically needed to facilitate inter-operability of MNO’s network functions where problems arise due to different interpretation or implementation of standards or protocols.

5.2.1 Normalisation of messages in 2G/3G/4G inter-PLMN traffic

Control plane messages of inter-PLMN 2G/3G/4G traffic are primarily based on SS7, GTPv1/v2 and Diameter. Although these interfaces are defined in the respective RFC and 3GPP specifications, it is not uncommon that network equipment vendors have different interpretation or implementation of such interfaces in terms of message formatting, information element formats and their actual values. IPX providers are required to perform normalisation of such traffic to resolve such inter-operability issues. Some examples are:

- Uppercase / lowercase conversion of information element values. Usually Diameter host/realm names are case-insensitive, but some DEA/HSS require all their peer names be in lowercase but some MME are configured with uppercase names.
- Modifications of information element values. MME/MSC are programmed to map MAP/Diameter result codes to NAS codes for sending to UE. These NAS codes impacts UE behavior (such as selection of networks). In order to use certain NAS codes, MAP/Diameter result codes from HLRHSS are mediated to specific values.
- Setting/unsetting of information element values to cope with different versions of specifications. Some information element (such as feature bits) values defined in new 3GPP specifications are not available in network equipment with older generations. Mediation of such values are necessary to support certain use cases.

While some normalisation can be handled by MNO’s network functions (such as DEA in 4G), some MNO relies on external parties such as IPX provider to perform such normalization.

5.2.2 Normalisation of messages in 5G inter-PLMN traffic

In 5G inter-PLMN traffic is based on HTTP/2 protocol, and if using PRINS on N32-f, with JSON format for control plane. GTPv2 is used for user plane. Normalisation of messages in 5G inter-PLMN traffic for message compatibility / interoperability is not required due to the following reasons:

- JSON is a well-defined formatting and serialisation standard and shall facilitate interoperability of MNO's network functions. 3GPP has means for version handling of Service Based Interfaces (SBI) standardised, as well as mechanism for negotiating supported features within a given version, and these should be used, verified, and tested before launching of new roaming relations.
- Any incompatibility or interoperability issues shall be addressed by the MNO at SEPP with configuration, software patching or backward compatibility rules.
- Processing of user plane traffic is not required for normalization as user plane traffic based on GTPv2 is a simple and mature format that is widely used in 3G/4G.

5.3 SEPP Security Configuration Criteria

Note – Postponed till 5GMRR Phase 2.

5.4 When using SEPP and when using SCP?

Note – Postponed till 5GMRR Phase 2.

5.5 How to secure SCP to SEPP?

Note – Postponed till 5GMRR Phase 2.

5.6 Support of multiple PLMN IDs

As per update of TS 33.501 0 section 5.9.3.2 "Requirements for Security Edge Protection Proxy (SEPP)" for Rel.17 as in the Change Request S3-212287 0, the SEPP shall be able to use one or more PLMN IDs as follows:

1. **PLMN is using more than one PLMN ID.**
   This PLMN's SEPP may use the same N32-connection for all of the PLMN's PLMN IDs as sketched in Figure 10 for a VPLMN owning PLMN ID's a, b and c.

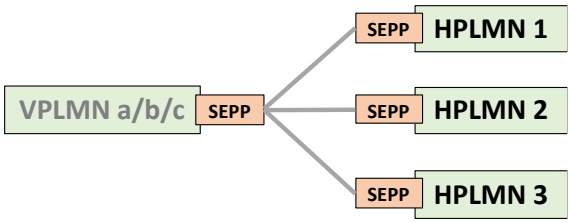
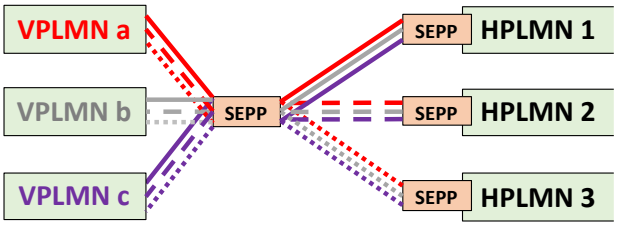


Figure 10 – SEPP using same N32-connection for all VPLMN's PLMN IDs

2. **Different PLMNs represented by the PLMN IDs**
   If different PLMNs represented by the PLMN IDs are supported by a SEPP, the SEPP shall use separate N32-connections for each pair of PLMNs as sketched in Figure 11 for VPLMNs owning PLMN ID's a, b and c.



Each line represents a separate N32-connection

Figure 11 – SEPP using separate N32-connections for the connected VPLMNs

5.7 Usage of TLS and PRINS between SEPPs

As per update of TS 33.501 0 section 13.1 “Protection at the network or transport layer” about the use of TLS and PRINS as in the Change Request S3-212367 0, the usage of TLS and PRINS between SEPP is clarified as depicted in Figure 12:

1. TLS shall be used for N32-c connections between the SEPPs.
2. If there are no IPX providers between the SEPPs, TLS shall be used for N32-f connections between the SEPPs.
3. If there are IPX providers which only offer IP routing service between SEPPs, either TLS or PRINS shall be used for protection of N32-f connections between the SEPPs.
4. If there are IPX providers which, in addition to IP routing offering services like billing, PRINS shall be used for protection of N32-f connections between the SEPPs

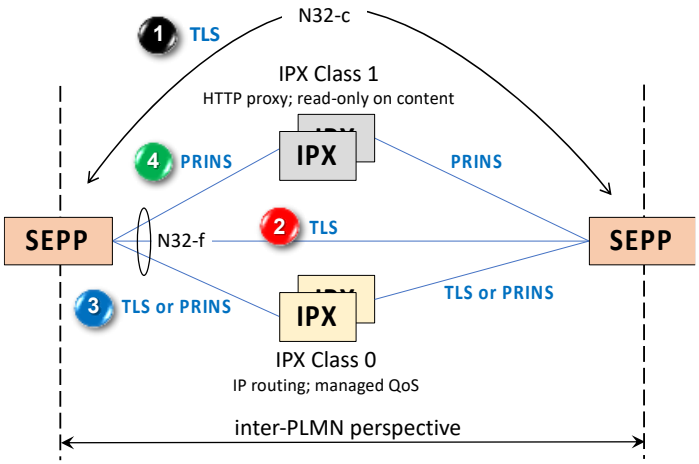


Figure 12 – SEPP using separate N32-connection for connected PLMNs

Based on the 5GMRR solution principle “Simplest Model per Use Case”, based on the business/operational requirements outlined in section 3.1, TLS is concluded as connection model for 5GMRR Phase 1 support of bilateral inter-PLMN roaming deployment scenarios

making use of direct connections or utilizing an IPX for http proxy services (read only content for IP routing and managed QoS).

The usage of PRINS and the automated migration to additional IPX service is being further analyzed.

5.8 Originating network identification

5.8.1 Issues

Originating network identification is especially important for trouble shooting based on passive probing systems or for roaming value-added services.

A limited number of N32-f messages contains Originating network in the application layer (like registration), and other N32-f messages do not contain the Originating Network (like deregistration) as the Originating Network ID is determined by other identities and is used and stored by NF Consumer and NF Producers.

Originating network of N32-f message could be identified by SEPP of the Receiving network using a stateful procedure by correlating this N32-f message with the associated N32-c negotiated parameter containing the authorized PLMN. However, this method does not address the following use cases:

- The originating network could be composed of multiple PLMN-IDs, negotiated on N32-c with the plmnIdList parameter, while unique identification of PLMN-ID is required per signaling (different PLMNs per service, e.g. IoT, etc.)
- In the hubbing case, where it is not specified by 3GPP how N32-c negotiation is done, i.e. how PLMN-IDs are managed over N32-c is not clear.

5.8.2 3GPP Rel-17 defined HTTP custom header 3gpp-Sbi-Originating-Network-Id

3GPP Release 17 TS 29.500 0 defines a new HTTP custom header (3gpp-Sbi-Originating-Network-Id) which allows to provide originating network identification on all N32-f messages whenever possible:

- 3gpp-Sbi-Originating-Network-Id HTTP custom header is sent by NF, SCP, or SEPP (depending on operator configuration) in the originating network supporting 3gpp-Sbi-Originating-Network-Id as specified in 3GPP Release 17 TS 29.500 0 whenever possible
- 3gpp-Sbi-Originating-Network-Id HTTP custom header (if available) can be used (depending on operator configuration) by SEPP in the receiving network supporting 3gpp-Sbi-Originating-Network-Id as specified in 3GPP Release 17 TS 29.500 0 to check or identify the originating network

Note: Detailed specifications related to 3gpp-Sbi-Originating-Network-Id header can be found in Table 5.2.3.2.1-1 of clause 5.2.3.2.1 and section 5.2.3.2.15 of 3GPP Release 17 TS 29.500 0.

5.8.3 Bilateral case

This section describes the different rules at sender/receiver side for the bilateral case.

Rules for the Originating Network

- Supporting entities of the Originating network shall, whenever possible, insert 3gpp-Sbi-Originating-Network-Id header, in accordance with 3GPP Release 17 TS 29.500 0.

Rules for the Receiving Network

- Supporting SEPP of the Receiving network shall check the 3gpp-Sbi-Originating-Network-Id header (if available) in the received N32-f message against the plmnIdList negotiated in N32-c (which could contain several PLMNID). If the PLMN-ID does not belong to the originating network, the receiving network shall discard the message.

5.8.4 Hubbing case

This section describes the different rules at sender/receiver side for the hubbing case.

Rules for the Originating Network

- Supporting entities of the Originating network shall, whenever possible, insert 3gpp-Sbi-Originating-Network-Id header, in accordance with 3GPP Release 17 TS 29.500 0.
- In case of Hubbing based on PRINS, originating network using SEPP shall not encrypt 3gpp-Sbi-Originating-Network-Id

Rules for the Roaming Hub

- The Roaming Hub (RH) shall forward the 3gpp-Sbi-Originating-Network-Id header if available without any modification
- Receiving RH shall identify the originating Network based on 3gpp-Sbi-Originating-Network-Id header if available

Rules for the Receiving Network

- Supporting SEPP of the Receiving Network shall identify the originating Network based on 3gpp-Sbi-Originating-Network-Id header, if available.
- Receiving NF shall rely on contents of HTTP body, i.e. JSON payloads, to identify the Originating Network.
- In case of Hubbing based on PRINS or TLS, supporting SEPP of the receiving network shall check the 3gpp-Sbi-Originating-Network-Id header (N32-f) (if available) with the N32-c parameter (plmnIdList) that is received from the Originating Network. If the PLMN-ID does not belong to the originating network, the receiving network shall discard the message.

6 Use cases

Note: Postponed till 5GMRR Phase 2.

7 Roaming VAS

Note: Postponed till 5GMRR Phase 2 when the full solution for 5G VAS is defined.

8 Naming, Addressing and Routing for 5G SA Roaming

8.1 SEPP Discovery

Based on the research about the automation of the related key management solution in the DESS working group, the following four discovery options were being considered as depicted in Figure 13.

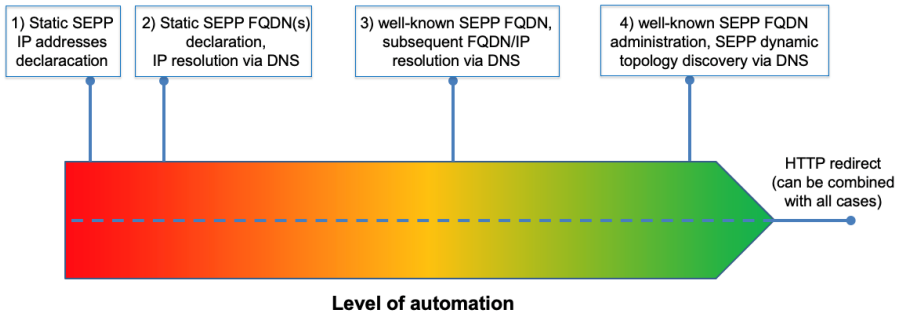


Figure 13 – Options for SEPP discovery based on the level of automation

As a result of the initial evaluation of these options, the following conclusions were drawn:

1. Elimination of option 1 due to the incompatibility with FQDNs, not suited for end-to-end, and any form of automation and routing.
   Note: only considerable for final local hop-by-hop section.
2. Use a best of breed strategy that supports manual configuration or full automation:

- SEPP FQDNs can be ‘static’ or ‘dynamic’.
- Static implies that DNS requests A or AAAA records.
- Dynamic implies that DNS requests NAPTR/SRV and subsequent A or AAAA records.

3. Option 3 is then no longer required.

To take optimal advantage of the best practices for discovery and routing practices in the internet, it was agreed to proceed further with the 4th option “Well-known SEPP FQDN administration, SEPP dynamic topology discovery with DNS and HTTP Redirect” as chosen solution for 5G SA Roaming. The other options were not considered further given the above considerations and the lack of interest and absence of written submissions otherwise.

The following Figure 14 sketches the logical diagram of the functions and interactions involved with this 4th option “Well-known SEPP FQDN administration, SEPP dynamic topology discovery with DNS and HTTP Redirect”.

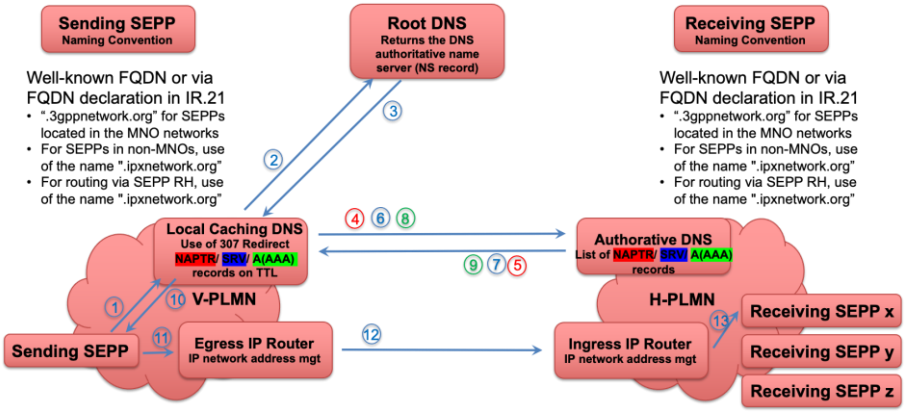


Figure 14 – SEPP dynamic topology discovery with DNS and HTTP Redirect

The solution makes use of both NAPTR records and SRV records as depicted in Figure 15:

- NAPTR records are used for the more static part of the SEPP discovery solution and is based on well-known SEPP FQDN(s).
- SRV records are used for the dynamic part of the SEPP discovery solution to differentiate between aspects like service classes, weight and priority that are renewed per TTL policies.

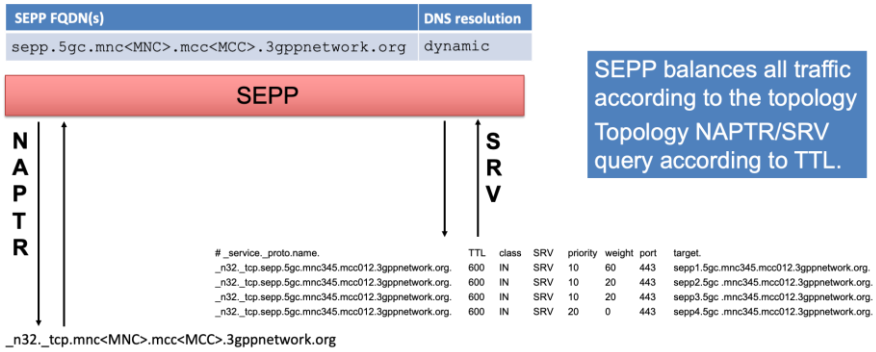


Figure 15 – The use of NAPTR records and SRV records as part of SEPP discovery

The DNS aspects of the SEPP Discovery procedures have been included in IR.67 0. The details of the SEPP HTTP Redirections, SEPP Load Distribution and SEPP administration, naming conventions and routing have been included in GSMA PRD NG.113 0. The aspects for SEPP Outsourcing to multiple IPX providers have also been included in the GSMA PRD NG.113 0.

8.2 Naming scheme for non-MNO entities on the IPX Network

8.2.1 Introduction

With the introduction of 5G roaming there is an increased need (see below) for identifiers of other players than MNOs on the IPX network.

Non-MNOs may offer/need:

1. Hosted and Operator group SEPPs
2. Roaming hub SEPPs
3. RVAS entities
4. Identifiers for hop-by-hop security through the IPX network
5. DESS Phase 1 AVP signing
6. …

8.2.2 Domain names and identifiers for MNOs

For MNOs the domain `3gppnetwork.org` is used and the identifier is a combination of 2 levels of subdomains for MNC and MCC: `mnc<MNC>.mcc<MCC>.3gppnetwork.org` Different MNC or even MCC can identify the same MNO.

The subdomains are implicitly owned by the MNO as ITU T and their local national numbering authority has granted the usage of such MCC/MNC. The procedure is formalized by registering the entire subdomain in GSMA root DNS pointing to the authoritative DNS of the MNO.

8.2.3 Domain names and identifiers for non-MNOs

For non-MNOs the domain `ipxnetwork.org` is ready to be used (already configured in GSMA root DNS) As non-MNO entities do not possess MCC/MNCs an alphanumeric name, obtained on a first come, first serve bases shall be used as identifier: `<UNIQUE-IPX-PROVIDER-ID>.ipxnetwork.org`

8.2.4 Registration procedure

For non-MNOs the registration procedure is very similar to the procedure for MNOs registering the MCC/MNC domain to the GSMA root DNS. In the registration procedure the approving entity shall keep a registry of existing non-MNO entities and shall register the proposed alphanumeric subdomain in the root DNS.

The alphanumeric name should be unique and have linkage to the entities name. As per IR.67 0 there should be only one alphanumeric name per non-MNO entity.

The details of this naming scheme for non-MNO entities on the IPX Network and the forms for registration are included in IR.67 0.

9 Mapping of Service Requirements and Defined Roles for the 5G SA Roaming Services outsourced to intermediaries

9.1 Introduction

This section provides the outcome of an analysis in the 5GMRR task force for the support by providers of intermediary services for 5G SA Roaming with 5GMRR Phase 2.

The focus is on providers of intermediary Roaming Hub services.

Note: The outcome of the analysis of additional services outsourced to different categories of intermediaries will be added to this section in the document at a later date.

An inventory is made of the service requirements to be supported by the Roaming Hub services. Subsequently, these service requirements are mapped to the distinct provider roles that may be assumed by a specialised and independent provider, as well as the identified combinations that may assumed by a multi-service provider in the IPX domain.

9.2 Background of outsourced 5G SA Roaming Services

For the specific IPX and Roaming Hub aspects please be referred in this document to both section 2.1.2 for the definition of IP Exchange (IPX) provider (with the cross references to GSMA PRDs AA.51 0 and IR.34 0) and section 2.1.4 for the definition of the Roaming Hub (RH) service (with the cross references to GSMA PRDs BA.60 0, BA.62 0 and BA.63 0) in the context of the 5G roaming architecture.

The overview in Figure 16 outlines the operation of the RH model, in which the VPMN has outsourced all or part of its roaming relationships via the 'left' RH provider and the HPMN has outsourced all or part of its roaming relationships via the 'right' RH provider. The RH model allows a maximum of two RH providers in the roaming path between a VPMN and HPMN.

The provisioning model for the RH service in IR.85 0 implies that the ‘left’ Client operator has an agreement with its adjacent ‘left’ RH provider about the set of roaming partners being served. In the case of 2 RHs in cascade, by default the Client operator has no insight which remote ‘right’ RH provider is used by its adjacent RH provider for which roaming partners. However, per contract the Client operator may agree with its RH provider about the use of a specific remote RH provider for specific roaming partners.

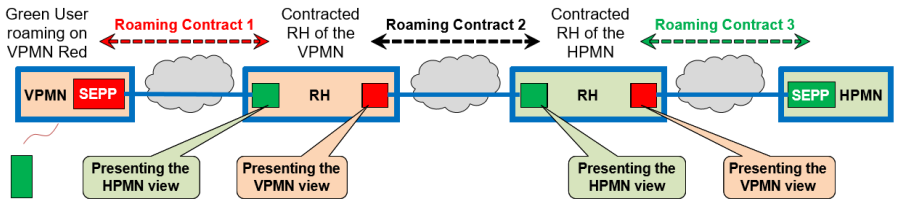


Figure 16 – Roaming Hubbing model and Roaming Contractual relations

The following diagram in Figure 17 outlines the position of the RH service as an extension of the 5G SA bilateral deployment variants as defined in 5GMRR Phase 1, assuming that both the VPMN and the HPMN are served by different RH providers and noting the following aspects (not exhaustive):

- 5GMRR Phase 1 operator group scenarios are not shown in the diagram.
- The functional diagram is technology agnostic, thus not restricted to either the TLS Hop-by-Hop model or the PRINS ALS end-to-end model.

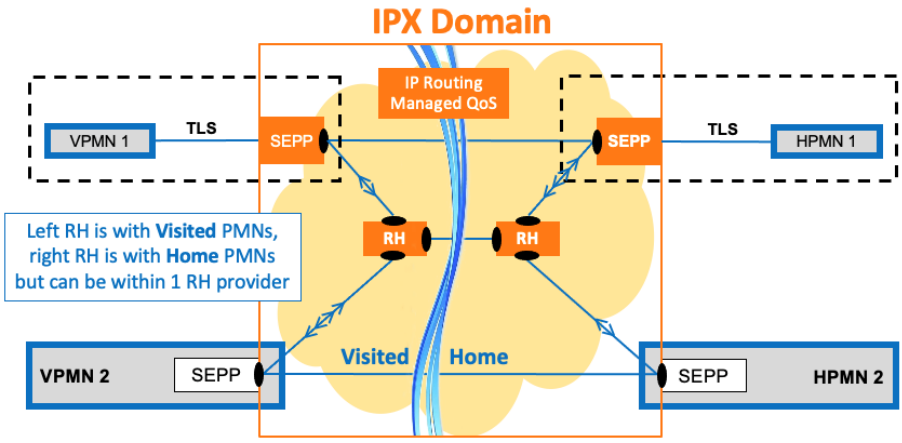


Figure 17 – Perspective of RH added to 5GMRR Phase 1 bilateral model

Note 1:The <> on the blue lines point to the message exchange between the top VPMN and the bottom HPMN. Idem the <<>> refer to the message exchange between the bottom VPMN and the top HPMN. This is to clarify that the interconnections via the RH providers are not working as backup routes for the bilateral interconnections.

Note 2: The orange-coloured SEPPs are Outsourced SEPPs as defined as part of 5GMRR Phase 1. In addition, the dotted lines indicate the relationships with the VPMN and the HPMN, respectively.

9.3 Mapping of Service Requirements for Roaming Hubbing to 5G SA Roaming Services

Operators can choose per roaming relation whether to have a bilateral connection or to use a roaming hub service. In the latter case the operators can choose which roaming hub's service to use for a roaming relation.

The Roaming Hubbing service is based on the following Trust Model alternatives:

- In Option 2 in clause 6.2 of AA.73 0 “Provider takes Financial Liability: where the VPMN has a business relationship only with RH and similarly HPMN has a business relationship only with the RH.”, i.e., both VPMN and HPMN have fully outsourced all or part of their roaming associations to their respective RH provider(s) and for these

roaming associations there is no direct contact between VPMN and HPMN. The trust model assumes that an RH assumes full liability for the Roaming Hubbing services and all exchanged traffic (control and user plane) utilized in the execution of the Roaming Hubbing service. The RH is required to effectively apply all necessary security controls, as stated in requirement 12 below. The RH and the client PLMN operator are also required to respect applicable privacy regulation. This regulation may require them to only grant access to information the RH needs to be able to fulfil its tasks, but not to the entire traffic. This regulation may also mandate which jurisdictions the traffic may be directed to, or pass through.

Note: This trust model is dependent on the liability clause being updated to reflect that liability is not limited only to proven negligence outside of billing, invoicing and payment of International Roaming charges.

- In Option 3 of the same clause 6.2 of AA.73 0, the RH provider assumes no such liability.

The list below reflects the set of service requirements for the Roaming Hubbing service in the 5G SA roaming eco-system. The roaming hub shall be able to:

1. Provide services outside a PLMN's domain, without the need for PLMNs to establish direct network connections with each other, and without impacting how the roaming partners of the Client Operators operate.

   Note: Provide technical services to establish roaming on behalf of a PLMN (Client Operator), outside a PLMN's domain.
   A PLMN can support both bi-lateral direct relationships and RH services toward different roaming partners (exclusive relationships)

2. Provide Roaming Hubbing agreements management including financial, privacy and security liabilities.

   Note: Provide visibility to and management (or control) of CP and UP traffic between PLMNs as the primary contracting and liable party.
   Related but different requirements are in 5 and 13.

   Note: A Roaming Hub provider acts as the primary contracting and liable party on behalf of a PLMN (including financial, privacy and security liabilities) by providing Roaming Hubbing agreements management, which has impact on how a roaming hub requires to manage CP and UP traffic, see requirements 5 and 13 below.

3. Perform passive tracing for signalling messages & content, i.e. determine that a message or user plane data has passed through the RH.

   Note: This requirement is independent from lawful interception capabilities.

4. Provide CDR generation and storage for wholesale billing mediation, charging and dispute handling.
5. Establish control plane connectivity with the Roaming Partners on behalf of the Client Operators.

6. Reject the N32 interface connectivity and any control plane traffic exchanged over the N32 interface with Roaming partners on behalf of the Client Operators.
7. Centralise roaming inter-operability tests for RH-mediated relations.
8. Peer with another RH provider, each serving different Client Operators. A maximum of two RH providers shall be supported in a roaming path.
9. Identify visited and home PLMN in every message exchanged over the N32 interface

   Note: It is preferred that the RH service is able to identify the home PLMN ID in every message. However, that depends on the feedback from 3GPP WGs and whether that is possible.

10. Implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g. FQDNs or PLMN IDs).
11. To be perceived as a roaming partner for its Client Operators in a similar manner as RH providers are defined and working in the mobile roaming eco-system for 2G/3G and LTE.

    Note1: A Roaming Hub is an intermediary that provides the technical and commercial means to facilitate the deployment and operation of International Roaming Services between the Client Operator and a set of selected Connected Operators. The Roaming Hubs specific requirements, according to their role and responsibilities assumes financial and technical liability to apply all necessary controls and access to all CP and UP communications.

    Note 2: Provide the ability for RH to support any Client PLMN applicable privacy and security regulations, which may limit access to specific information not required for RH to fulfil its obligations or may mandate jurisdiction where services can be provided.

12. Adhere to the same technical security guidelines as those applicable to mobile operators. In this regard, please be referred to FS.21 0 chapter 14 “Holistic Security approach for Mobile Roaming services” that need to be added as binding condition in the Roaming Hubbing Agreement Templates.

    Note:This implies that all actors (PLMN, outsourced SEPP, RHUB, RVAS) must, among other things, comply with:

    - Process and store identifiers and end-user information in a secure manner.
    - Only be able to modify, add or delete information that is relevant to their role, respecting what is contractually agreed in service level agreements (SLAs) and service level objectives (SLOs) and enforced technically.
    - Isolation of the individual operator signalling flows should be taken into account as well as the associated means for isolation breaches detection and mitigation.

13. Control the roaming subscriber user plane because the RH is financially liable. This control shall include the ability to prevent high data consumption as well as throttling or stopping ongoing data sessions on an individual user basis.
14. To limit roaming to a set of test users during the test phase, as only test users are allowed to perform roaming registration via the roaming hub.

To avoid impacts on business, the roaming hub shall be able to reject commercial user registration with an appropriate release cause in order for the UE to be able to reselect another roaming partner or technology.

15. To automate or streamline the management of multiple connections and certificates by the RH for its operator customers, for reasons of service viability and operational efficiency.
16. To serve hundreds of roaming relations between its customer operators in an efficient manner. In a setting with n RH customers, up to n * (n – 1)/2 roaming relations need to be supported, each involving N32 connections for inbound and outbound roamers separately. It is anticipated that, without respective considerations in solution development, scalability issues are likely to occur and operational handling to be difficult. The solution should therefore scale accordingly.

9.4 Requirements for Roaming Hubbing in relation to the Operators connected

The following list provides the set of requirements for the Roaming Hub service abilities to be offered to the served PMNs in terms of sending operator and receiving operator as well as in terms of visited network and home network.

The operators need quick and cost-effective access to the roaming footprint, so they need to be able to get easy access to Roaming Hub services and migrate to and from bilateral roaming without additional overhead.

1. The Client Operator which outsourced its roaming relationships to the Roaming Hub shall be able to receive roaming services with other Client Operators which outsourced its roaming relationships to the same Roaming Hub or other Roaming Hubs. It shall not be required to have individual roaming agreement among those Client Operators.
2. The Home network shall have the ability to know which Visited network its subscriber is roaming to.
3. The Visited network shall have the ability to know which Home network the subscriber is roaming from.

10 Documentation

Within the scope of 5GMRR Phase 1 the following documentation delivery is followed:

- 5GS Roaming Guidelines in CR proposal to NG.113 0 with detailed outline of the 5GMRR Phase 1 support of bilateral inter-PLMN deployment scenarios including SEPP Outsourcing and Mobile Operator Group Roaming Hub.
- Documentation of the surrounding security and operational aspects to be covered with the 5GMRR Phase 1 technical solution in CR proposal to FS.21 0.
- CR proposals to IR.21 0 and IR.85 0 for the support of roaming contracts of 5GS bilateral inter-PLMN connection support for 5GMRR Phase 1. With 5GMRR Phase 2 further enhancements are foreseen to cover the additional 5GS roaming use cases.
- Adding options for the internal RHUB solution within operator groups with intuitive descriptions in a CR proposal to IR.80 0.
- CR to FS.34 v1.0 0 with enhancements of the manual key management procedure for 5GS roaming support for SEPP Outsourcing as part of the work in FASG DESS.

There is currently no need for a CR to FS.36 v2.0 “5G Interconnect Security” 0 for 5GMRR Phase 1. However, at a later time refinements are foreseen following decisions on how TLS and PRINS will be used.

Following feedback at NG#13 there is no need for CR proposals to align on IPX, RVAS and RH definitions in IR.34 0, BA.60 0, etc. with the added cross-references to the definitions in sections 2.1 and 2.3.4.

Annex A Guidelines for Inter-PLMN Connection

The detailed solution is described in NG.113 Annex B 0.

For the initial support of 5GS Roaming as with 5GMRR Phase 1, NG.113 Annex B provides the guidelines for the bilateral inter-PLMN connection deployment scenarios including SEPP Outsourcing and Mobile Operator Group Roaming Hub.

Additional guidelines for 5GS Roaming are planned in a future version of NG.113 0 for the more comprehensive 5GS Roaming use cases such as IPX services, Roaming Value Added Services (RVAS) and Roaming Hub (RH).

Annex B Considerations for SEPP Outsourcing

The contents of this Annex reflect the state of affairs as of mid-2022. It should be considered that given the evolving nature of this area, these regulations are still under constant review and their completeness varies by country and region as they are drafted. It is intended that the content of this Annex will be re-evaluated in early 2024.

B.1 Overview

This section considers the applicability of these considerations to possible responses from national governments for sourcing and hosting arrangements for the SEPP.

5G standards development in 3GPP 0 has adopted a stronger security approach, leading to:

- **Use of Mutual Authentication:** Confirming sender and receiver have an established trust and the end-to-end relationship is secured.
- **A presumed "open" network:** Removing any assumption of safety from overlaid product(s) or process(es), for example secure perimeters.
- **An acknowledgment that all links could be compromised:** Mandating encryption of inter/intra-network traffic, ensuring the encrypted information is worthless when intercepted.
- **Provide control to the end-points of communication between PLMNs:** Allow for controlled access to information elements by encryption and modification policies

With the advent of 5G, one of the other areas of security focus is to make a step-change in signalling and roaming security through the deployment of the SEPP.

Previously, in 4G networks, the use of the Diameter Edge Agent (DEA) was an attempt to improve the security of Diameter signalling. Mobile operators have typically maintained a range of direct inter- PLMN connections and have supplemented this through use of IPX providers to overcome the '1 to n' connectivity problem. Also, signalling hubs have been used within to aggregate connections between network operators, including within operators acting as corporate groups. Finally, commercial intermediaries exist on interworking interfaces providing a plethora of different functions, so called RVAS. The functionality of DEA, IPX and RVAS capabilities has long been achieved through a range of delivery options. Outsourcing of IPX and signalling security functions has often formed part of this solution.

Considerations are provided hereafter for the SEPP to be used in a similar fashion.

The home SEPP (hSEPP) and visited SEPP (vSEPP) are shown in the diagram in Figure 18 as part of the wider 5G network.

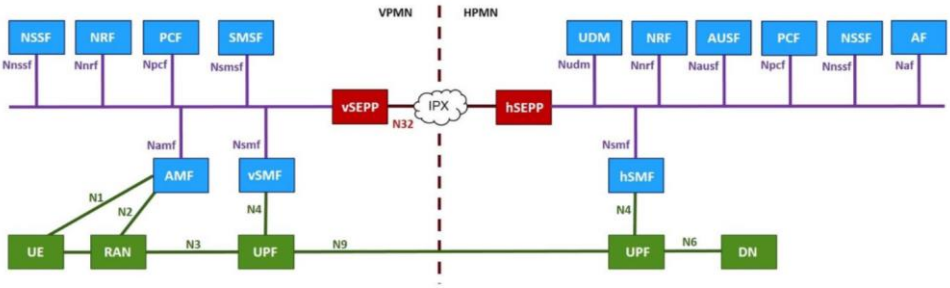


Figure 18 – An Example Overview of 5G SEPP Interconnect

An IPX provider is an interconnect partner enabling transport of inter-PLMN traffic between operators on the IPX network. SLAs that cover network quality of service, specific SLOs, bandwidth guarantees, and latency guarantees may also be provided.

The 5G roaming architecture and procedures support outsourcing of the edge elements, such as SEPP to the third parties, too. This outsourcing may include operation of the SEPP within the Operator premises, the SEPP provider, or a third party.

B.2 Outsourcing in 2G/3G/4G

Previous network generations support outsourcing edge network elements (e.g., DEA) and services (e.g., Roaming Hubbing) to a third party.

B.3 Examples of Legal and Regulatory Requirements & Guidance

A short survey was undertaken to identify possible approaches to security of SEPP related functions. These are listed:

- EU EECC 0
- ENISA 5G Supplement 0
- EU Toolbox 0
- UK Telecoms Security & associated ‘TSRs’ 0
- EC Revised Directive, Network and Information Systems 2 (NIS2) 0
- Cyprus 0
- General Data Protection Regulations 0

Note – In addition, also specific national approaches are applicable in Sweden[2], Germany[3], India[4], US[5] and Australia[6].

The survey assessed the regulation set to identify considerations that affect the sourcing arrangements for outsourcing of the SEPP function.

B.4 SEPP Selection Considerations

The survey noted four areas where specific aspects should be considered:

- National Regulation
- Regulatory Application
- Supply Chain
- Implementation

B.4.1 National Regulation

The underpinning components of national communication infrastructure and services have often been identified as 'critical functions' / 'essential functions'. Increasingly, mobile networks are also being defined as Critical National Infrastructure (CNI). Security for CNI is a national competence, even where they exist, regional regulations / guidelines may not necessarily apply and regional directives would still require national transposition. Given that signalling and IPX functions are cited directly or indirectly as critical functions it is likely that any solution would be of interest to national governments. Thus, the SEPP may be defined as a critical function for end-to-end 5G services.

Many governments are adopting a range of approaches to effect leverage into the mobile operator supply base. Existing legislative powers are being used in new ways, for example, adding new conditions into existing operating licences for supplier selection of 'trustworthy source' suppliers. Some governments are establishing entirely new laws and powers.

For example, the UK has enacted a Telecoms (Security) Act 0 to allow it to issue Codes of Practice (CoP) and to explicitly limit vendor selection / usage in relation to trustworthy vendors. The intent is to introduce new CoPs that will be explicit about the level and approach for security. Although the UK approach is a single example, international co-operation and knowledge sharing may mean a wider applicability of this approach or a variant.

The UK Act was informed by a security analysis by the UK National Cyber Security Centre 0 that identified a number of core and IPX functions where compromise was deemed 'critically sensitive'. These included:

[2] Sweden Post and Telecom Authority: https://pts.se/en/

[3] Germany Bundesnetzagentur: https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/ServicerProviderObligation/PublicSafety/Catalogue/Catalogue_node.html

[4] India Department of Telecommunications: https://dot.gov.in/

[5] US Department of Commerce: https://www.commerce.gov/tags/entity-list

6 Australian Telecoms Sector Security Reforms: https://www.legislation.gov.au/Details/C2017A00111

- Virtualisation infrastructure, orchestrators and controllers
- Internet gateways and monitoring functions
- Core network equipment, including database functions and access control functions
- IP core (routing and switching of traffic)

Identifying virtualisation infrastructure and routing (signalling) traffic as crucially sensitive. The resultant conclusions for areas of most interest were:

- exploitation via the operators' management plane
- exploitation via the international signalling plane
- exploitation of virtualised networks
- exploitation via the supply chain
- loss of the national capability to operate and secure networks

Given that SEPP functions are likely to be enabled by virtualised infrastructure and will deliver international signalling, for the UK it is likely that future CoPs will directly identify the SEPP function and virtualisation infrastructure as 'critically sensitive'.

More broadly, data protection legislation is also a required consideration for international operations and many countries are updating their existing laws or implementing new ones for the first time. In the EU for example, the General Data Protection Regulation (GDPR) 0 places obligations on businesses that impacts the processing and storage of EU citizens' data. In addition, there are many restrictions across the flow of personal data across countries.

Many mobile operators also operate under a licence that contains specific conditions relating to customer data or overall data sovereignty. In recently proposed legislation, some countries wish to have full control and ownership over any data that is generated within their country, regardless of where the organisation is based. Additionally, new proposals are being considered such as those in the U.S. whereby intermediate and terminating voice service providers will be prohibited from accepting traffic from 'foreign' Voice Service Providers if those entities are not registered in the FCC's Robocall Mitigation Database (certifying that they have implemented STIR/SHAKEN Call Authentication Standard and the Robocall Mitigation Plan).

From a technical interface perspective, there is no relation between SEPP and STIR/SHAKEN. The SEPP is working on the N32 interface exchanging roaming control signalling whereas STIR/SHAKEN acts on the SIP signalling in the IMS domain. However, there is potential synergy on the matter of key management to perhaps use the same key management solution for 5G/LTE roaming and for STIR/SHAKEN passports.

B.4.2 Regulatory Application

For each nation, there is a role for the national regulator to consider appropriate practical security responses to sufficiency, legacy and risk management decisions. These decisions will take into consideration governmental regulations, CoPs and guidance on risk appetite. These sufficiency aspects may relate to requirements to be able to effect 'fast' local (national, per operator) management of software functions like SEPP and may extend further into cloud infrastructure and certificate management. Such requirements for fast (e.g. a few hours) management control may, in practice, mean it is difficult to meet the response time

without having significant in-house staffing, skills and permissions. If this is the case, it adds additional cost and may undermine a business case to outsource.

The application of new regulations may be focused on just 5G capabilities (such as Network Slice management or SEPP), rather than existing 2G/3G/4G signalling capabilities, i.e. they may not be retrospective. This may mean that existing outsourcing arrangements can be maintained and focus applied purely to 5G SEPP rather than a bigger solution encompassing all signalling.

There are some regulations emerging, for example in the UK, to 'increase the network's resilience to disruptive attacks from external signalling networks' 0. To address this, it may be necessary to implement signalling security analysis such as inspection and filtering. This will require visibility of unencrypted signalling messages so compliance arrangements would need to be considered such that access is maintained before any encryption is applied or such that visibility is maintained in some other manner.

B.4.3 Supply Chain

Supply chain requirements are emerging to influence national operator use designated, trustworthy source suppliers. A recurring feature is to have an active management of an operator's supply chain. Consideration will be necessary as to the required 'depth' of management and 'deep understanding' of supply chains. For example, it may be required to manage direct outsource arrangements but also through further sub-contract and use of other 3rd parties by the outsourced entity.

A possible requirement is to be able to maintain operational network service without international connectivity. This may require in-house capabilities to be able to maintain service and consideration should be given to the potential duration of any such service period. In a longer-term, support access for bug fixes, security enhancements and upgrades may make maintaining service problematic.

The opportunity for indirect attacks through supplier or third-party tooling cannot be underestimated, as was shown when SolarWinds was compromised and delivered infected binaries to many of its customers 0 leading to multiple services that used the platform and tools becoming vulnerable to exploit through a supply chain attack. This emphasizes not only the need for vigilance in which 3rd party tools to use and the security stance of the 3rd party, but also good control and separation of assets.

Another specific case of government intervention into the supply chain is the US Entity Listing. In May 2020, the U.S. Department of Commerce (DoC) amended the foreign-produced direct product rule. In August 2020, the US DoC further restricted access to items produced domestically and abroad from U.S. technology and software. Hence, for SEPP outsourcing, the vendor selection and vendor solution's use of tools and technology should be assessed for compliance with the entity listing.

Finally, in several countries, for example, India, UK and US, there is a push not only for a more diverse supply chain but for that to include more use of national suppliers. There may be government incentives to use certain domestic suppliers that may be financially beneficial. Of course, these vendors must also be able to meet the wider security provisions

already mentioned and comply with relevant procurement and industry competition regulations.

B.4.4 Implementation

The precise implementation details of any SEPP outsourcing arrangement will matter from a government and regulatory interest viewpoint. For example, it should not be assumed that all outsourcing will be outside of national boundaries, so outsourcing to another domestic supplier may well be totally adequate from a regulatory viewpoint. Also, should the SEPP be outsourced within the national boundary but the IPX outsourced abroad, then this might be more acceptable from a regulatory viewpoint. Similarly, should the SEPP function be installed in the same security domain as the IPX provider or even outsourced but managed within the Operator's security domain, these may be deemed an acceptable arrangement by a national regulator.

Where regulations apply, the precise details of any given installation may need to be approved on a case-by-case basis through an approved government installation inspection. So a specific use and configuration of equipment may be acceptable subject to specific approvals, even where a wider reading of regulations may suggest otherwise. The scale of operation may also be important here where smaller or medium operations may attract a different regulator risk appetite than larger ('Tier 1') operations.

One further consideration is that the IPX provider may be providing a much wider connectivity function for routing user-traffic as well as signalling for SEPP. This may act in differing ways. One interpretation is that the regulations may be interpreted to allow this arrangement as it builds SEPP security alongside user traffic security. A contrary view could be that combining both traffic types present a bigger risk. A specific risk analysis and response can help make the case for any specific approach.

Depending on the solution architecture a range of operational remote access arrangements may be required. For example, multiple software vendors may be providing applications / micro-services, virtualisation and operating system support may be required through to managed cloud service accesses. Certificate management for software and for traffic encryption may also require remote access to update key material. Such handling may also attract specific security considerations.

B.5 SEPP Outsourcing Conclusions

There are differing views/appetites between jurisdictions. While some countries have clear and advanced position, others rely on existing mechanisms applied in new ways, whilst others appear to be still developing a response. Hence, any position will vary significantly depending on each individual country of operation and of potential outsource arrangement.

It is not GSMA's role to mandate compliance to national regulations but it also important that GSMA specifications do not prohibit adherence to national regulations.

Given that the SEPP function may be defined as CNI, solutions are likely to be in-scope for specific national security regulation.

The survey did not identify any countries where a specific SEPP outsourcing ban has been specified, but did identify four areas of consideration for SEPP outsourcing:

- National Regulation
- Regulatory Application
- Supply Chain
- Implementation.

Annex C Considerations on PRINS for Roaming Hubs

C.1 Introduction

There may be one or two roaming hubs involved in the communication between two PMNs. The roaming hubs require the ability to allow roaming relations between these PMNs via these roaming hubs. Furthermore, roaming hubs with financial liability require the ability to shape roaming traffic between the PMNs.

PRINS can allow and disallow establishment of TLS (which is used to carry) N32-c through standard HTTP proxy functionality. PRINS can also be used to dynamically introduce a traffic shaper under control of the RH into the data plane.

Commented [KS(1]: This is not correct as discussed in ANNEX F. This is only possible for the first HUB in the chain and only if HTTP CONNECT method is used and. Additionally control is not on N32-c level but only on TLS or connection (IP) level. This also means that control is not possible on PLMN Id level as this is only visible within N32-c

Commented [dcm02R1]: Annex C shows what is possible using proxies. For that, the connect method is proposed. I clarified that the control is on TLS level.

C.2 Solution details

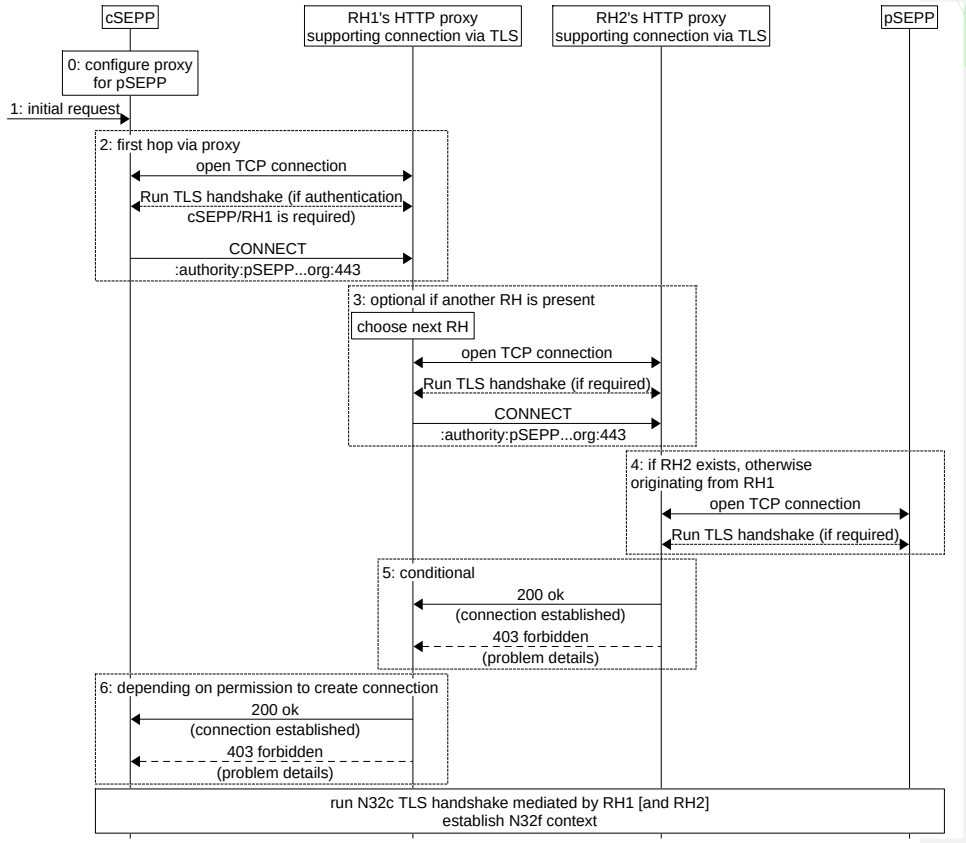


Figure 19 – Establishment of N32-c via roaming hubs

0. The cSEPP is configured to make use of RH1. cSEPP and pSEPP are configured with default protection policies:

a) encryption policy is to encrypt the IEs defined as mandatory to encrypt in 3GPP TS 33.501 0. Thus, the Subscription Permanent Identifier (SUPI) is not encrypted as this is not mandatory.
b) Modification policy is to allow modification of any IE that is not encrypted.

1. After receiving an initial request, the cSEPP sets up a TLS connection with RH1's proxy. The cSEPP then sends a CONNECT command to RH1's proxy indicating the destination to be pSEPP.
2. RH1's proxy shall verify that cSEPP is allowed to set up a roaming relation with pSEPP. If not, the flow continues with the error message of step 6. Otherwise, it continues with step 3.
3. If pSEPP requires another roaming hub to be reached, RH1's proxy sets up a TLS connection with RH2's proxy. RH1's proxy then sends a CONNECT command to RH2's proxy indicating the destination to be pSEPP. RH2's proxy shall verify that RH1 is allowed to set up a roaming relation with pSEPP. If not, the flow continues with the error message of step 5. Otherwise, it continues with step 4.
4. If RH2 is present, RH2's proxy, otherwise RH1's proxy shall set up a TCP connection to pSEPP. This connection may be protected by TLS.
5. If successful, if RH2 is present, RH2 shall return success with code 200.
6. If successful, RH1 shall return success with code 200.

If successful, pSEPP and cSEPP shall establish a TLS connection via the proxy/proxies for N32-c and establish an N32-f context, selecting PRINS as the protection mechanism.

Commented [KS(3]: Open question : Is this standard functionality and described anywhere or is this a proprietary functionality to be developed by the Hubs? Only thing I could find about proxy chaining is where the client is in control by using sequential connect method to sequential proxies.

Commented [dcm04R3]: Chaining of proxies exists in popular public proxy implementations

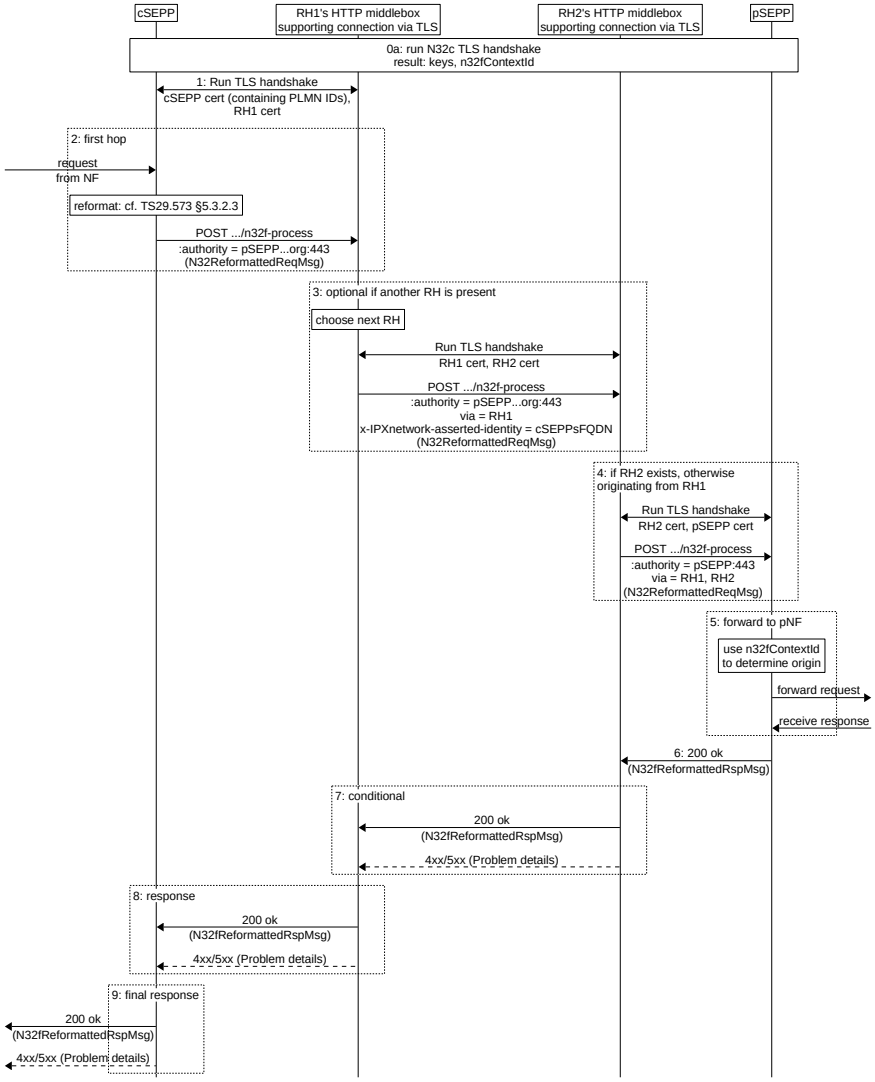


Figure 20 – N32-f via roaming hubs

1. cSEPP may either intiate a new TLS connection to RH1's middlebox, or reuse the TLS connection from setting up N32-c. In any case, communication between cSEPP and RH1's middlebox shall be TLS protected.
   Note: the name "middlebox" is chosen to avoid confusion with a pure HTTP proxy without any PRINS application logic.
2. After receiving a request from an NF, the cSEPP shall encapsulate the request as defined in TS 29.573 0 subclause 5.3.2.3 and send the reformatted message to RH1's

middlebox. The URL to send the request to shall be located on RH1's middlebox, thus RH1's middlebox is able to read the request.

3. If RH1 intends to reject the request, it shall generate the appropriate error, going straight to step 8, i.e. sending this error to pSEPP. If another RH is present, RH1's middlebox shall forward the message to RH2's middlebox, including a via header and an asserted identity header asserting the identity of the cSEPPs PMN. If RH2 is not present, then this request shall be sent directly to pSEPP.
4. If another RH is present, If RH2 intends to reject the request, it shall generate the appropriate error, going straight to step 7, i.e. sending this error to RH1. Otherwise, RH2's middlebox shall forward the request to pSEPP, including a via header giving both RH proxies. An asserted identity header is not necessary as pSEPP can identify the source PMN from the N32-f context.
5. pSEPP shall check that no encrypted IE is to be modified, apply the patches, decapsulate the request, and forward the decapsulated, patched request to the pNF. The pSEPP later (asynchronously) receives the response from the pNF.
6. pSEPP shall reformat the response and forward to RH2 (if present) or to RH1 (if RH2 is not present).
7. If RH2 is present, then RH2's middlebox shall forward the response to RH1's middlebox.
8. RH1's middlebox shall forward the response to cSEPP.
9. In case cSEPP receives a response code of 200 ok, cSEPP shall check that no encrypted IE is to be modified, apply the patches, decapsulate the response, forward it to the cNF. In case the cSEPP receives an error code, the cSEPP shall forward this error to the cNF, as specified in 29.500 0 clause 6.10.8.3.

All communication shall be TLS protected on the hops between cSEPP and RH1's middlebox, RH1's middlebox and RH2's middlebox, RH2's middlebox and pSEPP.

RH1's middlebox and RH2's middlebox both may include modifications, or return errors, e.g. in case of roaming policy violations.

The following two messages sequence charts give examples:

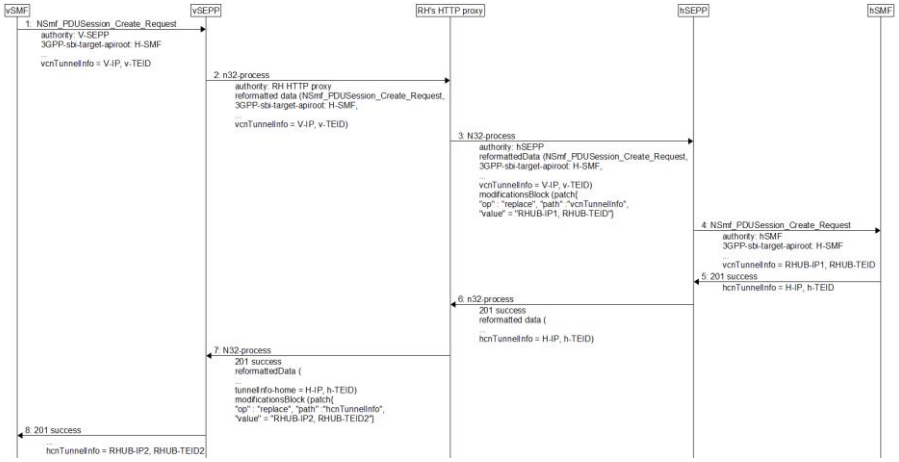


Figure 21 – Roaming hub inserting a traffic shaper

In case the RH would like to manage the bandwidth on a connection, it can insert a traffic shaper. To insert a traffic shaper (sometimes also called traffic controlling or traffic policing entity) into the roaming user data plane, the RH may include a modifications block that rewrites the N9 endpoints IP address and Tunnel Endpoint ID (TEID) for the visited network's UPF in step 3, and another modifications block that rewrites the N9 endpoints IP address and TEID for the home network's UPF in step 7. As these modifications blocks are signed, the modifications are attributable.

The traffic shaper can rate limit the traffic by delaying or dropping packets on a per GTP-U bearer basis. In order to terminate a session, the traffic shaper can make use of the networks' northbound interfaces.

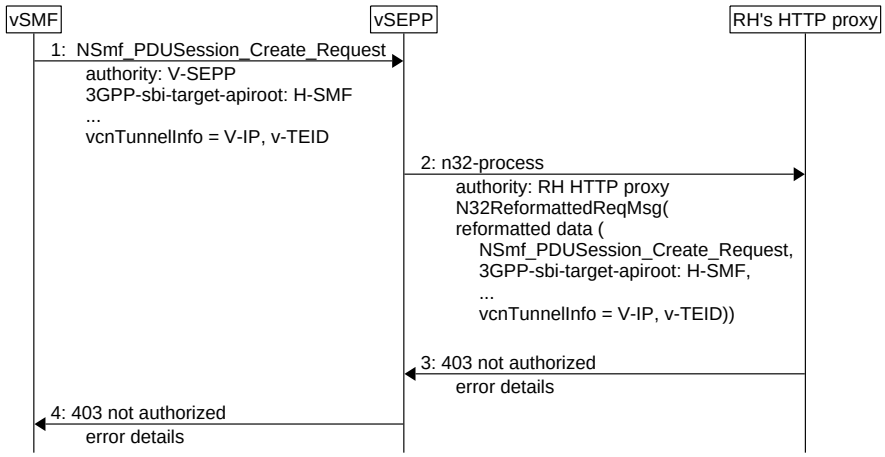


Figure 22 – Roaming rejecting a session creation request

A roaming hub may also reject service requests of particular subscribers according to the roaming hub's policy. An example of this would be a PDU session setup request by returning an error in step 3. This error is forwarded to the vSMF in step 4. This may be triggered by some information in the request visible to the RH. As different SUPIs require different handling, then of course, SUPI shall not be encrypted in the request.

C.3 Service Transparency

Using the PRINS model, service transparency issues, i.e. information available to a roaming hub, have been identified with the support of Roaming Hubbing services in 5G SA as currently supported in 2G, 3G, and 4G/LTE as Roaming Hubbing services.

This is based on the situation that with the PRINS model the N32-c for negotiating TLS or PRINS is established end-to-end routed via the Roaming Hub acting as HTTP middlebox (not SEPP), and the potential PRINS encryption policy, by which not all information elements at N32-f may be visible to the Roaming Hub service provider.

Although the impact may vary per Roaming Hub provider given that not all Roaming Hubbing services are covered in GSMA specification, the following generic issues were identified:

Roaming Data Control

- User plane control is essential for an intermediary RH entity given its financial liability. If NEF based user plane control is considered insufficient to instruct termination of sessions, additional work by 3GPP may be required.

Privacy and confidentiality

- Using the PRINS protocol allows to protect sensitive data.

Non-repudiation

- Using the PRINS protocol enables fraud investigations

Irrespective of the additional end-to-end data protection provided with the PRINS model, the Roaming Hub provider shall follow the security guidelines for the “Holistic Security approach for Mobile Roaming services” in GSMA PRD FS.21 0.

C.4 Evaluation

The solution allows a RH to open and close roaming relations. In addition, it allows traffic shaping of the user plane roaming traffic between two PMNs making use of the roaming hubs.

The solution exposes user plane traffic to roaming hub's traffic shapers (when present). However, at both PMNs, the presence of the traffic shapers is visible in the modifications blocks. Furthermore, modifications performed by the roaming hubs are attributable.

Note: attributable here means being able to identify the originating security domain (i.e. operator or RH) of messages and their modifications.

The proposed solution addresses the perceived operational complexities of PRINS pointed out in section 4.2 as follows:

- Protection Policies may vary per partner MNO – There is only one default protection policy for roaming hubs.
- Roaming agreement may vary per partner MNO – all roaming agreements via roaming hubs are treated identically.
- JSON Patch control for both visited and home network roaming hubs – automatically handled by the protocol implementation.
- Operators will need to be aware of which intermediary is allowed to modify messages, as well as of public keys of these intermediaries – The Parameter Exchange Procedure for Security Information list Exchange on N32-c as specified in TS 29.573 0 clause 5.2.3.4 exchanges the public keys or certificates of the intermediaries. The certificate of its own intermediary can be obtained directly from the RH that MNO has a contract with, or from the RAEX tool.

Certificates necessary for N32-c establishment can be retrieved from RAEX tool.

It is technically non-problematic to establish N32-c between two PLMNs via RH, even though there is no contract between HPLMN and VPLMN. This doesn't interfere with the RH ability to ensure that N32-c is only established between its client operators according to contractual agreements.

The RH will be able to monitor its client operators' TLS connectivity and certificates, thus being able to troubleshoot any problems as they occur.

From a service transparency perspective, using the PRINS model will require changes on how to the support Roaming Hubbing services in 5G SA compared to how they are currently supported in 2G, 3G and 4G/LTE.

Updates will be required to 3GPP PRINS 3GPP specification in the version current in March 2023, in order to allow N32-f errors to become visible to the PRINS middleboxes.

Annex D Hop-by-hop TLS Architecture

D.1 Introduction

In the roaming eco-system, various services may be outsourced by MNOs to third parties, such as an IPX carrier or VAS provider. These services include hosted SEPP, potentially combined with hosted NF and hosted UPF, as well as services in the context of a Roaming Hub contract, including financial liability.

In the interest of business continuity, an architecture is required that recognizes service provider relations, that serve a collection of (international) roaming relations. This architecture is described in the following chapters, where D.2 covers the case where only one operator has outsourced services, D.3 covers the case where both operators have outsourced services, and D.4 covers the common part for both options.

D.2 Hop-by-hop TLS: Architecture Description for hosted SEPP

Consider two Mobile Network Operators (MNOs) O1 and O2 having a roaming relation. O1 outsourced services to a hosted SEPP provider, while keeping a SEPP function in-house to manage a limited set of (domestic) relations as well as the relation with the hosted SEPP service provider. The hosted SEPP service provider may offer additional services such as active network steering, fraud detection and prevention, sponsored roaming or data roaming control, involving the deployment of hosted NF and UPF in the most general case.

O2 has no relation with the hosted SEPP service provider and treats the relation with O1 as a normal bilateral roaming relation using direct TLS.

The following pictures illustrates the SEPP discovery process, with in sequence NAPTR, SRV and A/AAAA queries.

Figure 23 shows the basic process, in case of a bilateral relation between O1 and O2 based on Direct TLS.

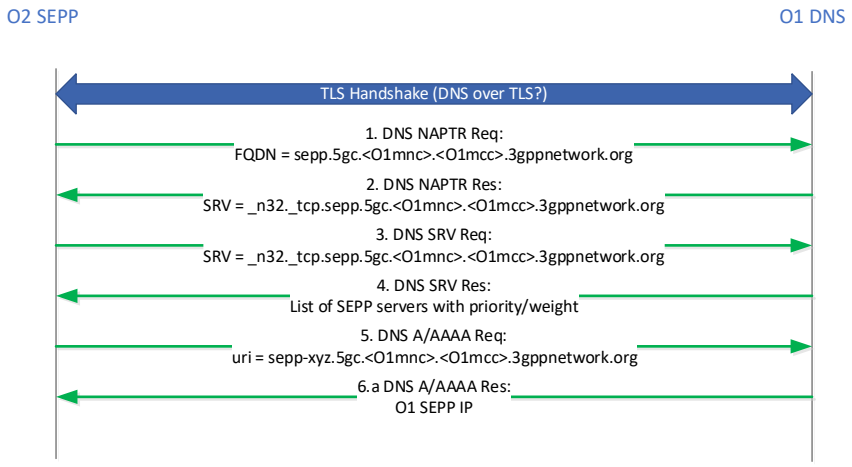


Figure 23 – Bilateral relation between O1 and O2 based on Direct TLS

O1 DNS IP is published in its IR.21; at this time it is still unclear how the DNS query in itself is going to be protected – DNS over TLS is just one option.

On receiving the NAPTR query from O2 SEPP, O1 DNS returns a service record for the SEPP service. O2 SEPP then launches a SRV request, and receives a list of SEPP servers to choose from. Finally, O2 SEPP launches a A/AAAA request to obtain the IP of the selected O1 SEPP.

This flow is the same in case of outsourced SEPP, as the SEPP service and SEPP IP are considered to belong to O1' security domain.

Figure 24 shows the SEPP discovery flow for hosted SEPP. In this case, the SEPP service is provided by a host and "hosted" in the security domain of the host.

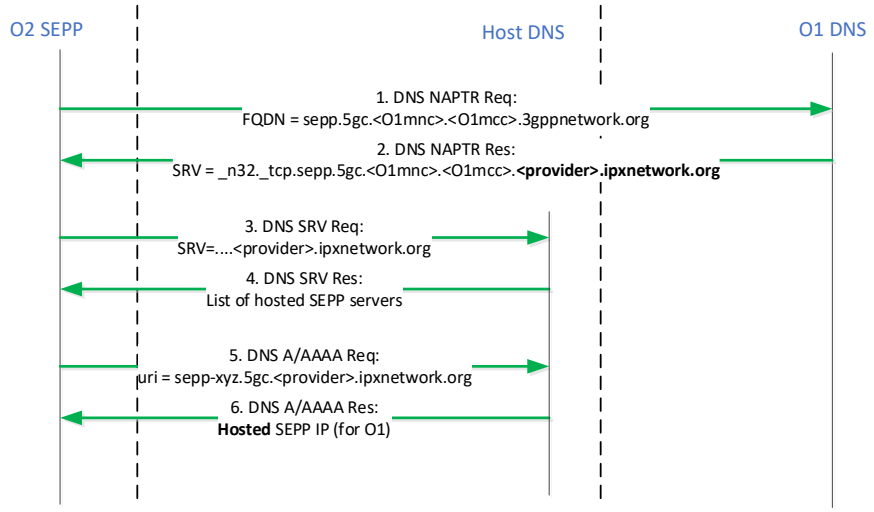


Figure 24 – SEPP discovery flow for hosted SEPP

The NAPTR query is still sent to O1 DNS, as authoritative DNS for the domain. However, the response contains a service record pointing to the domain of the host. The SRV and A/AAAA are subsequently handled by the host DNS, as authoritative for the host domain. By using <O1mnc>.<O1mcc> as subdomain, different SEPP server instances and corresponding IP can be provided per hosted customer.

As shown in Figure 25, O1 SEPP in turn only needs to discover the hosted SEPP, as it is managing all (or most) of the roaming relations. For any remaining (e.g. domestic) relations, the roaming partners can agree to use a domestic DNS, configure static domestic SEPP IP, or configure a source IP based DNS result (not shown in the picture).

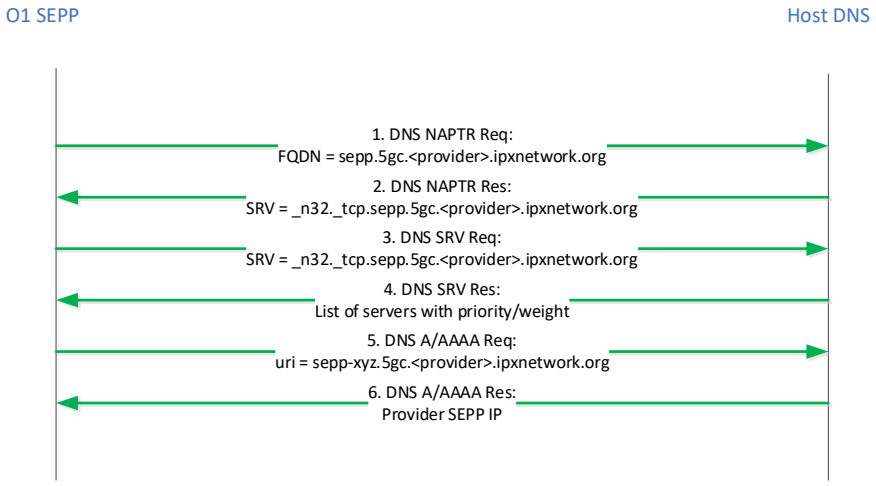


Figure 25 – Complementary SEPP discovery flow for hosted SEPP

Figure 26 shows TLS handshake and N32-c exchanges between both O1 and O2. SEPP+ indicates a SEPP with additional functionalities to handle the customer-provider relationship (n32"p"). The difference with "classic" SEPP is in the validation of a provider certificate instead of a PLMN certificate, and verifying that the relation with the roaming partner (O2), as identified in the N32-f traffic, is indeed managed via the provider.

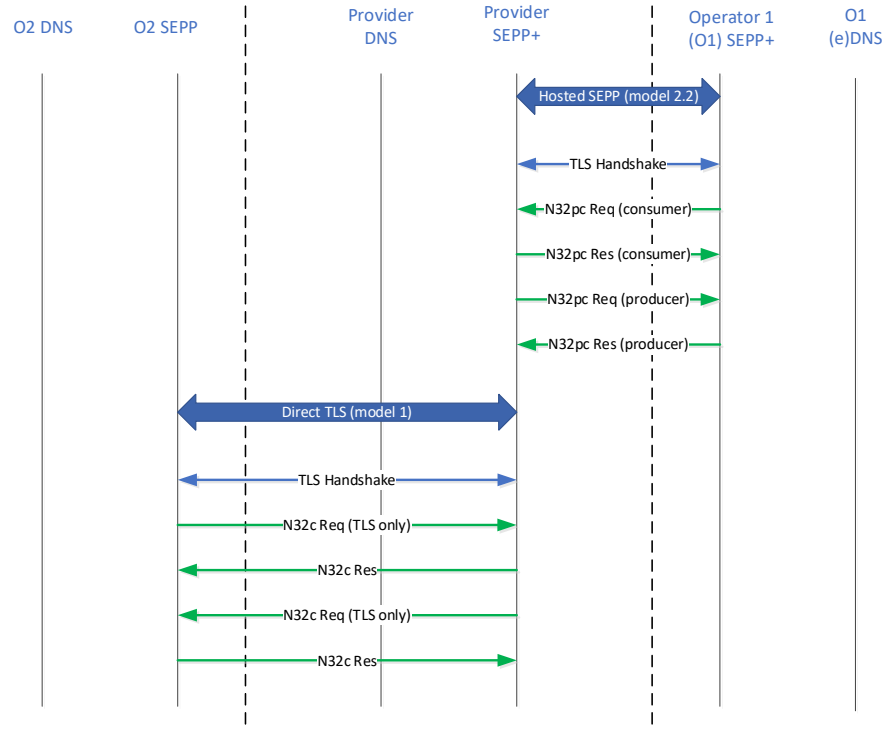


Figure 26 – TLS handshake and N32-c exchanges between both O1 and O2

Note that:

- O1 SEPP IP are not exposed to the general IPX community, only to the limited set of in-house managed relations (not depicted here) and to the hosted SEPP provider. O1 SEPP will not accept TLS handshakes or N32-c requests from the general IPX community, outside of the hosted SEPP provider.
- As for the N32-c exchange, it provides the option to negotiate custom headers e.g. 3ggp-Sbi-Originating-Network-Id, as per service contract. Optionally, PRINS can be engaged to provide integrity protection and authentication for non-repudiation purposes when required.

As for O2, there is no notable difference compared to the direct TLS model, other than receiving a provider's server list and SEPP IP as result of the SEPP discovery process. It's required for O2 to open their IP firewall for provider IP – this should be covered in the bilateral roaming agreement between O1 and O2. From a technical perspective, it is much more convenient to use provider IP rather than "loan" IP from each individual customer.

Once N32-c is setup between all parties, N32-f traffic can flow in both directions as illustrated in Figure 27.

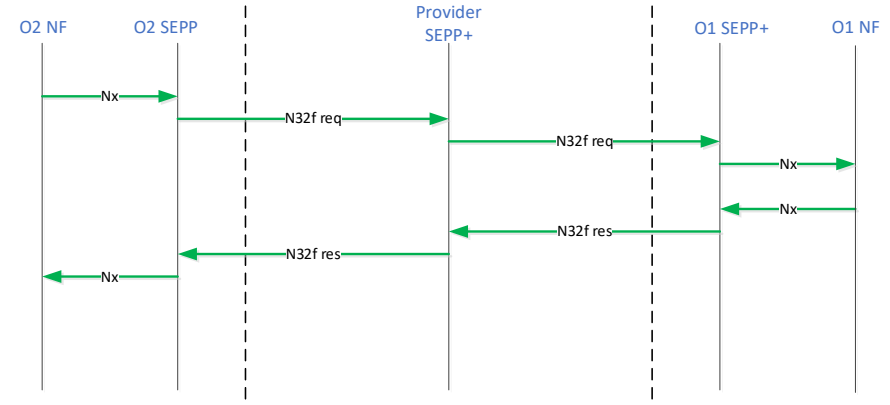


Figure 27 – N32-f traffic flow in both directions

The provider SEPP forwards N32-f based on the 3gpp-Sbi-Target-ApiRoot header, which indicates the target NF at the roaming partner's. O1 SEPP simply forwards the N32-f traffic to the hosted provider managing the roaming relation.

Optionally, the host may provide additional value added services that require more than just a simple forwarding of messages or a simple mediation of message content. A SEPP+ may then no longer be sufficient. Figure 28 illustrates the NF discovery process in case a provider NF must be included in the control flow. Situation: O1 UE roaming in O2's network, so O1 has the HPLMN role and O2 has the VPLMN role.

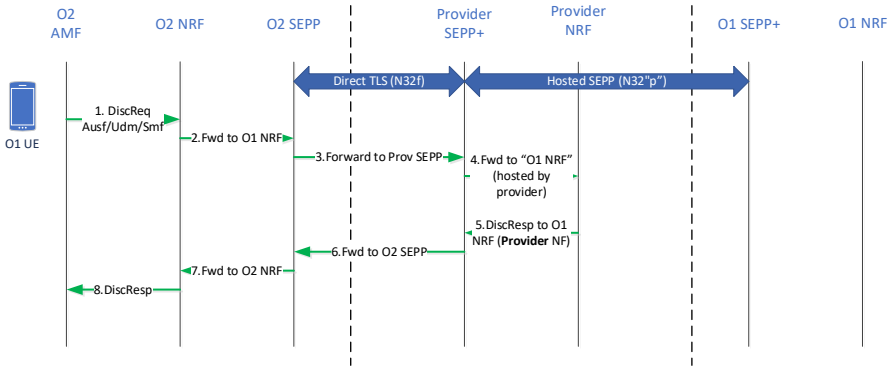


Figure 28 – NF discovery process if a provider NF must be included in the control flow

O2 follows the normal 3GPP procedures, so the discovery request arrives at the provider SEPP (steps 1, 2 and 3).

Step 4: provider SEPP checks the validity of the request, i.c. target O1 is a valid customer and roaming relation with O2 is open. If the request is valid, provider SEPP forwards the request to provider NRF, as per service contract.

Step 5: provider NRF answers the discovery request, with a provider NF as result. NF naming needs to be agreed with O1 and be consistent with O1's naming conventions and domain name. Finally, this answer is forwarded to O2 AMF via O2 SEPP.

Further N32-f and N9 flows are discussed in chapter D.4, as they are similar for both the hosted SEPP and hub SEPP architectures. Discovery of O1 NF by provider NF is also handled there.

D.3 Hop-by-hop TLS: Architecture Description for hub SEPP

In this situation, both operators O1 and O2 have outsourced services to a 3rd party provider that involves the use of a 3rd party SEPP.

In case of a hub scenario, O2 SEPP does not contact O1 DNS as there is no direct agreement or contract between them anymore. Instead, the agreement is brokered by the hub provider. O2 SEPP therefore needs to discover the hub SEPP. This is shown in Figure 30.

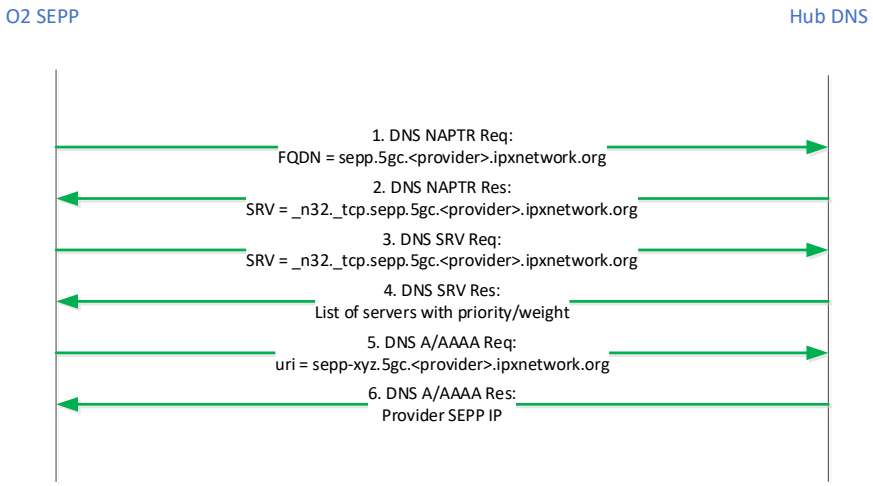


Figure 29

Figure 30 – O2 SEPP therefore needs to discover the hub SEPP

Note that from O1's perspective, not much has changed compared to the hosted SEPP model described in chapter D.2. In other words, if O1 uses a service provider for all its relations, bilateral and hub agreements can technically be handled in the same way.

Notable differences with the hosted SEPP model:

- O2 no longer uses the well-known FQDN of O1 to discover O1's SEPP, but instead the FQDN of the provider managing the relation with O1. Provider DNS is queried instead of O1 DNS (NAPTR, SRV and A/AAAA).
- The number of TLS handshakes and N32 connections between parties is much reduced, as bilateral connections are replaced by a hub-and-spoke architecture. Iow connections per roaming relation are replaced by a relation with the service provider, managing all those relations. This heavily reduces the number of persistent connections to manage and allows for a quicker upscaling of roaming relations.

Once N32-c is setup between all parties, N32-f traffic can flow in both directions.

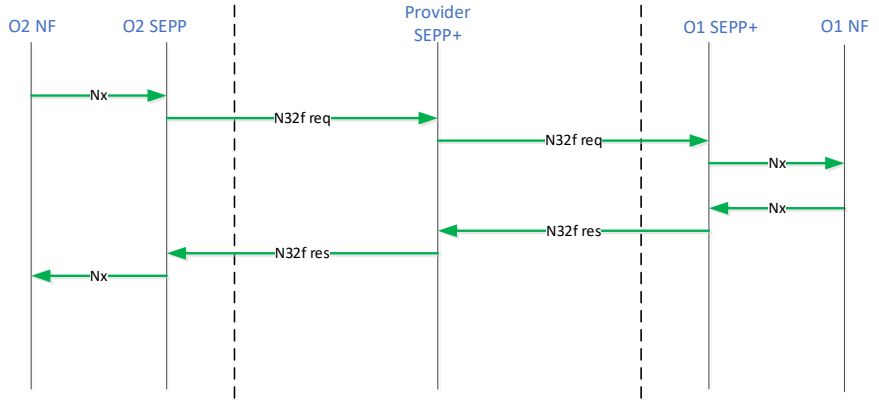


Figure 31 – N32-f traffic flow in both directions via Provider SEPP

The provider SEPP forwards N32-f based on the 3gpp-Sbi-Target-ApiRoot header, which indicates the target NF at the roaming partner's. O1 and O2 SEPP simply forward the N32-f traffic to the hub provider managing the roaming relation.

Optionally, the hub may provide additional value added services that require more than just a simple forwarding of messages or a simple mediation of message content. A SEPP+ may then no longer be sufficient. Figure 32 illustrates the NF discovery process in case a provider NF must be included in the control flow. Situation: O1 UE roaming in O2's network, so O1 has the HPLMN role and O2 has the VPLMN role.

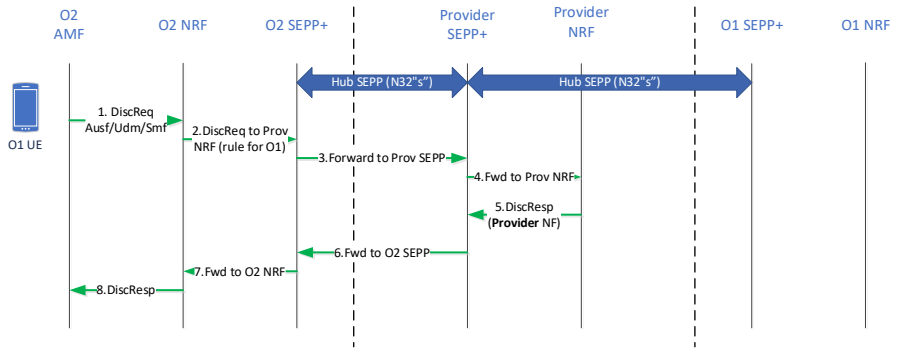


Figure 32 – NF discovery process if a provider NF must be included in the control flow

note: N32"p" used for hosted SEPP may be identical to N32"s" used for hub SEPP

Notable differences with the hosted SEPP model:

- Provider NF/NRF naming can be done independently of O1 or O2 naming conventions, using the provider's own domain.
- O2 knowingly communicates with provider NRF/NF from the provider's domain instead of O1's domain.

SEPP verification is quite similar to what's described for the hosted SEPP model:

- Verification of customer/provider TLS certificates
- Verification whether roaming relation is open and the correct provider is chosen for the relation
- Rejection of traffic if either of these verification steps fail

Further N32-f and N9 flows are discussed in chapter D.4, as they are similar for both the hosted SEPP and hub SEPP architectures. Discovery of O1 NF by provider NF is also handled there.

D.4 Hop-by-hop TLS: N32-f and N9 flows

Figure 33 illustrate the call flows for control and user plane, under the assumption that provider NF and UPF are to be involved as part of the service contract. The same roaming situation is taken as before, namely O1 UE roams in O2's network.

The first picture shows a generic control plane flow, where the hosted NF either directly provides a result (a) or reissues the initial request (b), potentially with changes to the content, to the target network. The provider NF takes on different roles in the latter case.

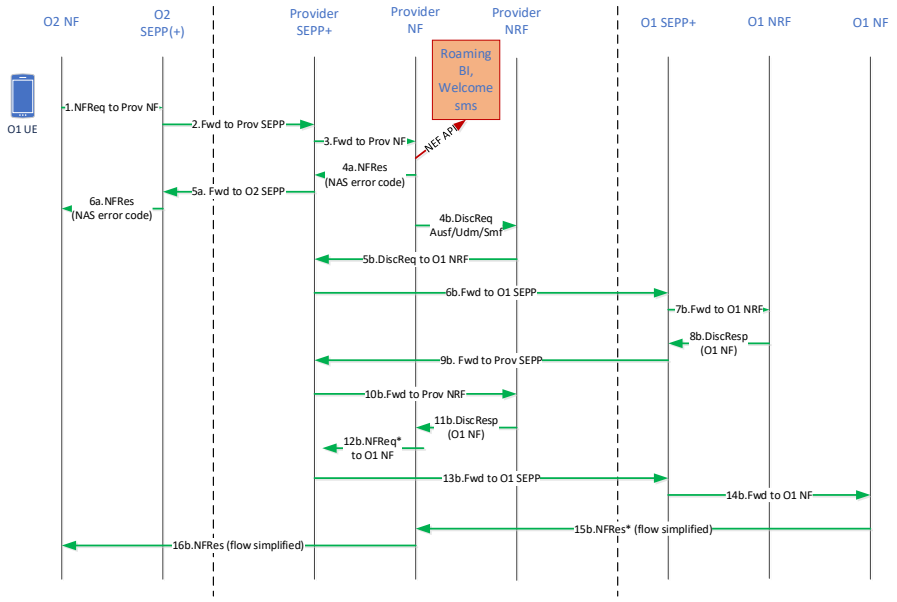


Figure 33 – call flows for control and user plane if provider NF and UPF are involved

Step 1: O2 NF targets the provider NF for the request, as per result of the NF discovery process shown in D.2 and D.3.

Steps 2, 3: request verification and forwarding by O2 and provider SEPP.

Step 4: the provider may trigger additional services, exposed via NEF API, to other systems or application functions, e.g. roaming business intelligence or welcome sms applications.

Step 4a: as part of the service contract with O1, NF requests can be rejected by the provider NF using a proper NAS error code. Examples: O1 UE tries to register on a forbidden network, or the request is deemed to be fraudulent. This flow is then concluded in steps 5a and 6a.

Step 4b: when O2's NF request is allowed, the provider NF acts as the visited network AMF and issues a discovery request for O1's target NF. The NF type is determined from the request type received from O2. The discovery request is targeted at O1's NRF. Roaming partner transparency can be kept by means of 3ggp-Sbi-Originating-Network-Id header or appropriate NF naming (implementation decision). The originating network id header can be populated by O2 or inserted by the provider.

Steps 5b, 6b, 7b: request verification and forwarding by provider and O1 SEPP.

Step 8b: O1 NRF responds with NF uri, which finally arrives at provider NF (steps 9b, 10b 11b)

Step 12b: the provider NF (acting as visited AMF) reissues the initial NF request from O2, possibly with altered content (NFReq*), to O1 NF.

Steps 15b, 16b: O1 NF returns a result to provider NF, which is then reissued by provider NF (acting as AUSF, UDM or home SMF such as the case may be) to O2 NF. In these steps, the path via the respective SEPPs is no longer shown for simplicity.

It may be enough for the provider SEPP to be in the loop wrt to the control plane, e.g. when the service provider just provides passive services, or a basic hub function without financial liability.

However in most cases the provider is expected to step in and initiate certain processes on NF level, such as rejecting requests, changing request/response parameters or modifying/deleting ongoing data sessions. The latter is illustrated in the call flow in Figure 34.

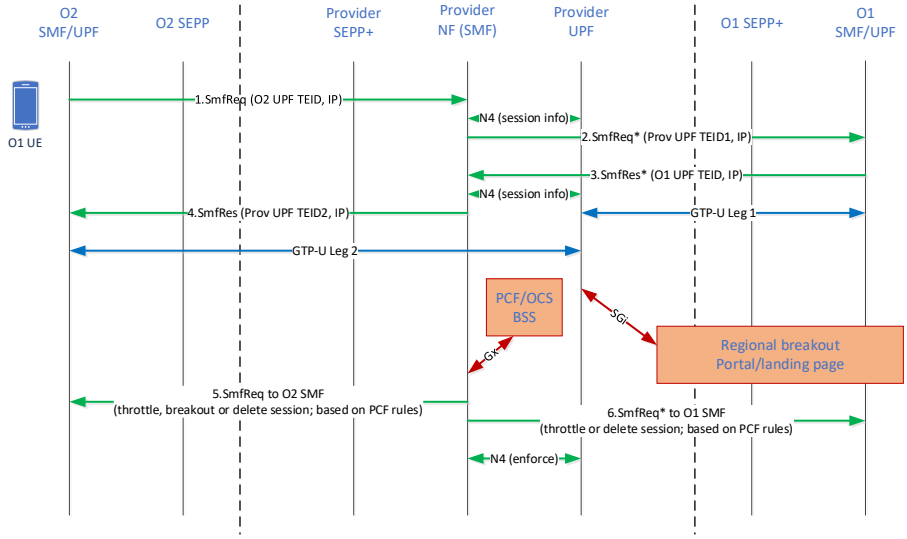


Figure 34 – provider steps in and initiate certain processes on NF level

Verification and forwarding by O1, O2 and provider SEPP is no longer shown explicitly.

Step 1: O2 SMF targets the provider NF, as per result of the NF discovery process shown in D.2 and D.3.

Step 2: the provider NF, in the role of vSMF, in turn issues a data session request to O1 SMF, with agreed upon parameters as per service contract. In addition, it manages provider UPF resources over N4, generates PDRs for wholesale settlement etc.

Step 3: O1 SMF accepts the data session request and returns GTP-U and other parameters to provider SMF. This concludes the setup of GTP-U tunnel 1 between O1 and the provider UPF.

Step 4: the provider NF, in the role of hSMF, accepts the data session request from O2 SMF and returns GTP-U and other parameters to O2 SMF. This concludes the setup of GTP-U tunnel 2 between provider and O2 UPF.

Under conditions specified by the service contract, a provider may omit steps 2 and 3 and break out the session regionally (SGi) – e.g. when the provider offers direct access to nearby edge computing centers, that may host applications used by the UE, to reduce latency.

Steps 5 and 6: when the provider's budget control system detects a situation of insufficient customer (O1) funds, it may issue instructions to (heavily) reduce data consumption, interrupt data sessions with a forced breakout to a landing page, or simply to delete data sessions. Note that traffic shaping is intended to level out traffic peaks, but is not suitable to handle sizeable lasting bandwidth reductions, which inevitably cause buffer overflow. Control of GTP-U parameters on NF level is essential.

Figure 35 illustrates the authentication flow for sponsored roaming, whereby the service provider is backed by a sponsor MNO to provide international roaming services to operators who don't have roaming agreements of their own. In such a situation, the visited network operator (O2) is only aware of sponsored identities (provider SUPI) and is unaware of any operators making use of the service (O1).

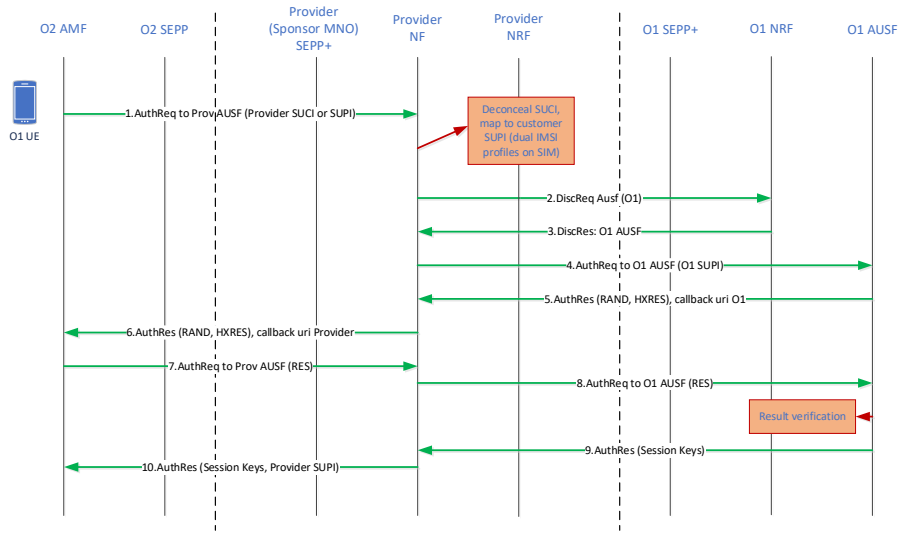


Figure 35 – Authentication flow for sponsored roaming

For simplicity's sake, it is assumed that the visited network operator (O2) has a bilateral roaming agreement with the provider (acting as sponsor MNO), based on direct TLS.

Step 1: O1 UE contains a SIM card with a dual SUPI (IMSI) profile. There is a single secret key (Ki) used for the 5G authentication process, managed exclusively by O1. However, there are 2 SUPIs, one from O1 and one from the provider.

Each has their own set of public/private network key pairs used for SUPI concealment. The provider manages the SUPI mapping and public/private network key pair for provider SUPI concealment.

When O1 has no roaming relation with O2, the UE will use the provider SUPI to get roaming service. Therefore, the authentication request is sent to the provider NF, acting as AUSF/SDM. If it is an initial request, it contains a provider SUCI which must be deconcealed first. Once the provider SUPI is known, it can be mapped to the correct client SUPI (O1).

Steps 2, 3: provider NF, acting as visited AMF, discovers O1 AUSF.

Step 4: provider NF reissues the authentication request to O1 AUSF, using O1 SUPI.

Step 5: O1 AUSF answers with a challenge (RAND) and a hash of the expected result (HXRES).

Step 6: provider NF, acting as AUSF, reissues the answer to O2 AMF.

Step 7: once the actual result (RES) is obtained from the UE, O2 AMF computes hash HRES and verifies if it matches the received HXRES. If successful, it issues another request containing RES to provider NF using the callback uri.

Step 8: provider NF reissues this request to O1 AUSF.

Step 9: O1 AUSF verifies RES and finally returns the required cryptographic materials (session keys) to provider NF.

Step 10: provider NF reissues the answer to O2 AMF, completing the authentication/registration process.

Annex E Local PRINS (L-PRINS) for Roaming and Service Hubs

E.1 Introduction

In 3GPP specifications, ALS (PRINS) is used to establish end-to-end security over the roaming N32 interface. There may be one or two roaming hubs involved in the communication between two PMNs. The roaming hubs are tasked with facilitating the establishment of roaming relations between these PMNs via these roaming hubs. Furthermore, roaming hubs with financial liability require the ability to shape user plane traffic between the PMNs.

Local PRINS (L-PRINS) can be used to provide N32-f content availability to the Roaming Hub by terminating the N32-c at the Roaming Hub while at the same time provide local attribution and non-repudiation between any pair of consecutive hops. Local PRINS does not require a modification policy. Due to non-repudiation, the RH can provide convincing evidence on the message originator identity, in terms of previous or next hop, of any message stored in its logs.

Due to terminating N32 at the intermediary, e.g., Roaming Hub or Service Hub, Local PRINS provides the flexibility that is needed for the Roaming Hub and the Service hub to perform all the services possible in a mechanism that is identical to hop-by-hop TLS from service perspective while being more secure.

E.2 End-to-end Attribution

3GPP specification (TS 33.501 0 and TS 29.573 0) define an Application Layer Security (ALS) protocol (PRINS) which provides end-to-end security over the roaming interface (N32). When using PRINS, end-to-end attribution is provided for every message dynamically as the receiving SEPP (e.g., pSEPP) is able to validate the origin of the N32-f message and any modification (if any) that is done by any of the intermediaries, e.g., IPX. When PRINS protocol is used, the HPLMN SEPP, for example, is not required to keep any logs nor need any other entity collaboration to validate the end-to-end attribution of any message exchanged over N32-f.

In the case of L-PRINS, the receiving entity is always able to dynamically attribute the received message to the immediate previous hop which sent the message. This means L-PRINS provides a dynamic and immediate hop-by-hop attribution. However, if every intermediary maintains the logs of the received messages in addition to the message it sent, an end-to-end attribution is possible assuming the collaboration of all intermediaries. In other words, L-PRINS provides a cryptographical means that can be used to convince a third party of the origin and attributability of any N32-f messages exchanges over the roaming interface for a possible conclusion of an end-to-end attribution.

Note: As an example, in the case there is a single Roaming Hub in the path between VPLMN and HPLMN, end-to-end attribution is possible by mandating the RH to keep logs of all messages its receives and all messages it sends for a specific period of time. During that period of time, for messages in the path from VPLMN to the HPLMN, logs of message received by the RH include the digital signature of cSEPP and thus the content of the message can be attributed to cSEPP. Message sent by the RH includes the RH-SEPP digital signature and the content can be attributed to the RH. Therefore, end-to-end

attribution is possible by offline processing of the RH logs made available to VPLMN or HPLMN.

E.3 Solution details

E.3.1 N32-c establishment using L-PRINS

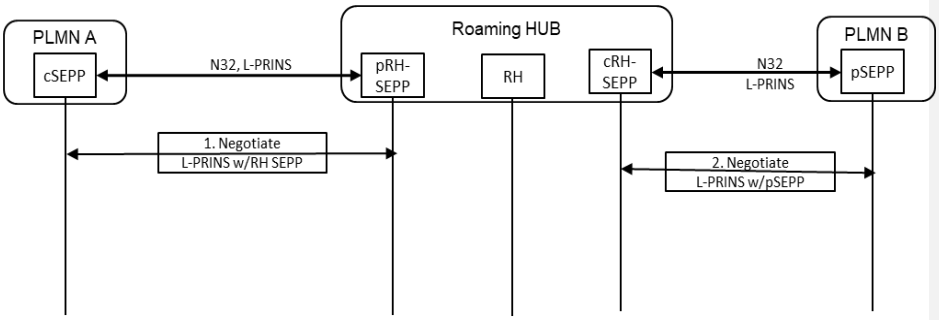


Figure 36 – Establishment of N32-c using Local PRINS

1. The cSEPP negotiates Local PRINS (L-PRINS) with its local next hop pRH -SEPP (RH-SEPP). Local PRINS allows both cSEPP and RH-SEPP to use PRINS while the N32-c and N32-f terminates at the cSEPP and the RH-SEPP. Both cSEPP and the RH-SEPP will exchange their certificates as part of the Local N32-c negotiation.

   Note: The RH-SEPP is captured in this call flow as pRH-SEPP and cRH-SEPP but that is to simplify the call flow as this is a logical distinction and it can be the same RH-SEPP. When pRH-SEPP and cRH-SEPP are deployed as one physical instance, in this case RH-SEPP will be having two N32 interfaces.

2. The cRH-SEPP negotiates Local PRINS (L-PRINS) with its local next hop pSEPP using Local PRINS. Similar to step No. 1, L-PRINS allows both cRH-SEPP and pSEPP to use PRINS while the N32-c terminates at the cRH-SEPP and the pSEPP. Both cRH-SEPP and the pSEPP will exchange their certificates as part of the Local N32-c negotiation.

   Note: The RH can possibly use GSMA RAEX tool to securely publish the PLMNs it represents. Each PMN client would then be able to map the RH-SEPP (i.e., cRH-SEPP or pRH-SEPP) certificate to the list of supported PLMN-IDs.

   Note: The certificate exchanged between cSEPP with pRH-SEPP, includes the cSEPP public key pair which can be used by the pRH-SEPP to validate the cSEPP signature that is generated by cSEPP using its private key pair. The same is true for the exchanged pRH-SEPP and the pSEPP certificates.

E.3.2 Call Flow over N32-f using L-PRINS

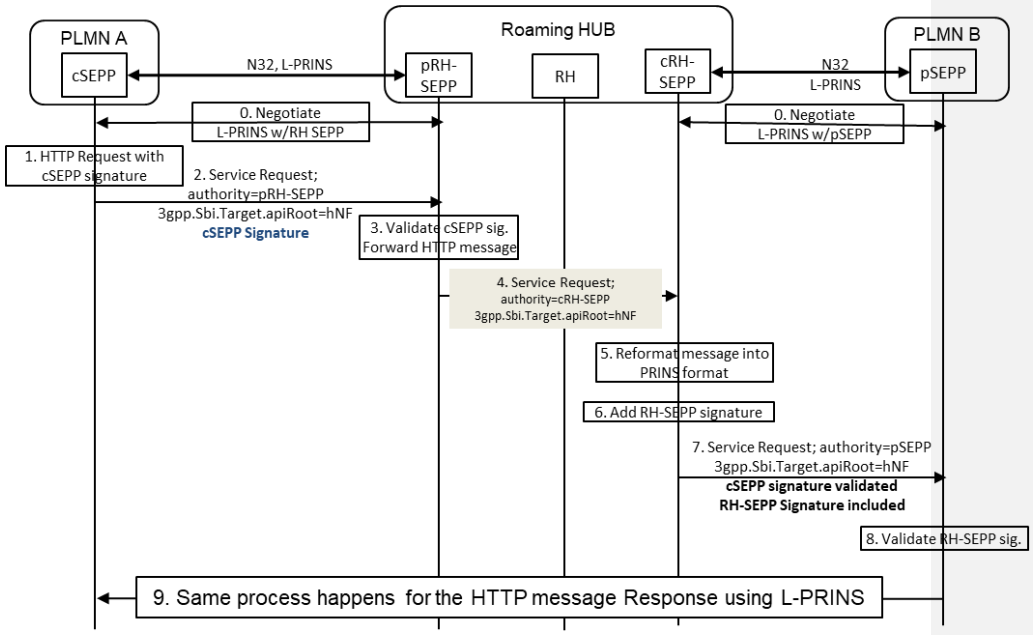


Figure 37 – Call flow over N32-f using Local PRINS

0. The cSEPP establishes N32-c and N32-f with RH-SEPP and RH-SEPP establishes N32-c and N32-f with the pSEPP.

1. cSEPP reformats the HTTP message to PRINS format and adds cSEPP signature using its private key.

    a) The cSEPP signature is generated using the cSEPP asymmetric private key and it protects the whole message. ”none” algorithm cannot be used when generating the signature.

2. cSEPP sends the reformatted message (for example Service Request message over N32-f) with cSEPP signature included to the RH-SEPP.

    Note: The RH-SEPP is captured in this call flow as pRH-SEPP and cRH-SEPP but that is to simplify the call flow as this is a logical distinction and it can be the same RH-SEPP. When pRH-SEPP and cRH-SEPP are deployed as one physical instance, in this case RH-SEPP will be having two N32 interfaces.

3. RH-SEPP receives the PRINS message and shall do the following:

    a) aThe RH-SEPP validates the cSEPP signature using the cSEPP public key that was exchanged in the cSEPP certificate during N32-c setup.

b) bThe RH-SEPP reformats the PRINS message back into HTTP message.

4. The pRH-SEPP forwards the Service Request internally within the RH for processing and finally to the cRH-SEPP.
5. cRH-SEPP reformats the HTTP message to PRINS message.

   Note: Since it is mandatory for the cRH-SEPP to validate the cSEPP signature of the message, there is no need to add an indication that RH-SEPP has validated the cSEPP signature.

6. The cRH-SEPP adds its signature using its private key which maps to the public key of the certificate that was exchanged over N32-c with the pSEPP.
7. cRH-SEPP sends the reformatted message with its signature to the pSEPP.
8. pSEPP validates the RH-SEPP signature and reformats the message to HTTP message and sends it to the hNF.

   Note: communication between pSEPP and hNF is identical to all solutions and use cases and thus not captured in here.

9. The same L-PRINS hop-by-hop protection is used in the response direction from pSEPP to cSEPP.

E.4 Local PRINS Advantages

Local PRINS (L-PRINS) enables GSMA to provide a single solution with combined approach for all use cases where an intermediary is providing a service other than IP routing, e.g., Roaming Hub, IPX, RVAS, while providing the following flexibility to enable all these use cases.

1. It provides a security solution that provide the RH and Service Hub full access to the HTTP message over N32-f while providing Attribution and non-repudiation for all messages exchanged between any pair of consecutive hops, e.g., between cSEPP and RH, or between RH1 and RH2, or RH and pSEPP.
2. With the mandate for the cSEPP, pSEPP, and intermediary (RH or Service hub) to maintain the logs, end-to-end attribution and non-repudiation using cryptographical means is also possible when the RH logs and the cSEPP, RH-SEPP, and pSEPP certificate containing the respective public key are made available to the roaming partners for offline processing. The digital evidence produced is suitable to convince third parties.

There are 3GPP changes required for L-PRINS, however, all mechanisms in the end-to-end PRINS is believed applicable with the end-to-end being the immediate two hops, e.g., PLMN-A and RH or PLMN-B and Service Hub. Whether reusing an existing mechanism for enabling all entities, e.g., cSEPP, RH-SEPP, and pSEPP, to digitally sign the message or defining a new one is to be evaluated by 3GPP.

E.5 Evaluation

L-PRINS is a hop-by-hop approach, which does not provide end-to-end security between PMNs. However, it provides additional security than hop-by-hop TLS and is considered as a possible milestone towards a solution with end-to-end security between VPMN and HPMN.

L-PRINS is a GSMA 5GMRR working solution assumption for enabling GSMA roaming use cases which require an intermediary to provide a roaming service other than IP routing, i.e., Roaming Hub, IPX, and RVAS. L-PRINS is a working solution assumption where GSMA roaming services offered by an intermediary, e.g., Roaming Hub, IPX, RVAS, can be enabled while maintaining a reasonable security with a possible path forward to end-to-end security using PRINS in the future.
The L-PRINS provides a single solution for all the use cases where an intermediary is providing a service other than IP routing, e.g., Roaming Hub, IPX, RVAS, while increasing the traceability, attribution, and non-repudiation over N32 interface while at the same time enabling both the RH and Service Hub full access to the Http messages exchanged over N32-f and N32-c.

More importantly, this solution can possibly provide a natural evolution to an end-to-end security solution in case it is mandated by regulatory.

Finally, an update to 3GPP specification is required to enable GSMA to provide a complete 5G SA roaming solution.

Annex F Security Profiles for PRINS

This annex provides the view of some companies.

To facilitate and simplify the deployment and operation of PRINS, security profiles could be introduced. For this, the N32-c negotiation for PRINS can be enhanced to allow selecting the existing scheme (for backward compatibility and high security requirements voiced in discussions) or selecting one or several security profiles such as:

- "full PRINS“ profile, for negotiation of a cipher suite and exchange of modification and encryption policies is needed (as specified by 3GPP current schema).
- a pre-defined profile, e.g. "profile A" or "profile B", negotiated between SEPPs based on GSMA guidelines, by which IPX can be instructed equally.
- "integrity-only PRINS" profile, as one option, which in current understanding means, that JSON objects are created without encryption policies but integrity protected.

  Note: integrity-only PRINS may however not be preferable, since AVs and authorization tokens need protection

With this information, during N32-c handshake, if the PRINS enhanced profile, e.g., “B”, is chosen, then both SEPPs (VPLMN and HPLMN) know how to handle the communication on the N32-f interface and the intermediary IPX providers as well. I.e., a profile indicator during N32-c negotiation phase can be propagated as an indication of the selected PRINS profile to the IPX; since only PRINS can be chosen, N32-f will always be based on application layer.

Enumaration value	Description
TLS	TLS security
PRINS Profile full Profile integrity-only Profile A Profile B … Operator defined profile	Protocol for N32 Interconnect security with subcategories to indicate full usage of PRINS, with integrity protection onl or specific profiles

Table 3 – Example of N32 security profile

If PRINS with "full PRINS" is chosen, configuration parameters can still be negotiated/exchanged, which keeps market open to those, really wanting this high security option

a) Modification policy. A modification policy indicates which IEs can be modified by an IPX provider of the sending SEPP.
b) Data-type encryption policy. A data-type encryption policy indicates which types of data will be encrypted by the sending SEPP.
c) Cipher suites for confidentiality and integrity protection, when application layer security is used to protect HTTP messages between them.
d) N32-f context ID. The N32-f context ID identifies the set of security related configuration parameters applicable to a protected message received from a SEPP in a different PLMN.

If PRINS with any other profile is chosen, the following configuration parameters need to be negotiated/exchanged and profiles need to be defined.

a) A PRINS profile indicating a predefined set of one or more of the above policies.

Note: Data type encryption policy for integrity-only PRINS profile: this policy will not specify any data type to be confidentiality protected; Modification policy for integrity-only PRINS profile: this policy will not specify any IE subject to be modifiable. Still, integrity protection is provided.

Annex G Document Management

G.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	01 Oct 2021	First Document Version	ISAG	Pieter Veenstra, NetNumber
2.0	05 July 2022	Including CR1002, CR1003 and CR1004	ISAG	Pieter Veenstra, NetNumber
3.0	27 October 2022	Including CR1005 and CR1006	ISAG	Pieter Veenstra, Titan.ium Platform
4.0	… May 2023	Including: CR1007 – NRG 016_004 CR1008 – NRG 016_005 CR1009 – 5GMRR Doc 41_26_Rev1 CR1010 – 5GMRR Doc 41_15-r1 CR1011 – 5GMRR Doc 41_17-r1 CR1012 – 5GMRR Doc 41_16 CR1013 – 5GMRR Doc 41_05r3 CR1014 – 5GMRR Doc 41_06r1 CR1015 – 5GMRR Doc 41_11r2 CR1016 – 5GMRR Doc 41_23r2 CR1017 – 5GMRR Doc 42_05r1	ISAG	Pieter Veenstra, Titan.ium Platform

G.2 Other Information

Type	Description
Document Owner	Networks Group
Editor / Company	Pieter Veenstra, Titan.ium Platform

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.