Report 5G Mobile Roaming Revisited (5GMRR) Phase 1

Version 2.0

06 July 2022

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

Security Classification: Non-confidential

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

Copyright Notice

Disclaimer

Compliance Notice

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

[Note to editor: Include one of the following statements only; delete the other]:

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 in GSMA AA.35 - Procedures for Industry Specifications.

OR

This Permanent Reference Document has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.34 - Policy and Procedures for Official Documents.

Table of Contents

1 Introduction

1.1 Overview

This report provides the conclusions phase 1 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 [1], TS 23.501 [7] and TS 29.573 [25] is provided, followed by key issues and alternative 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:

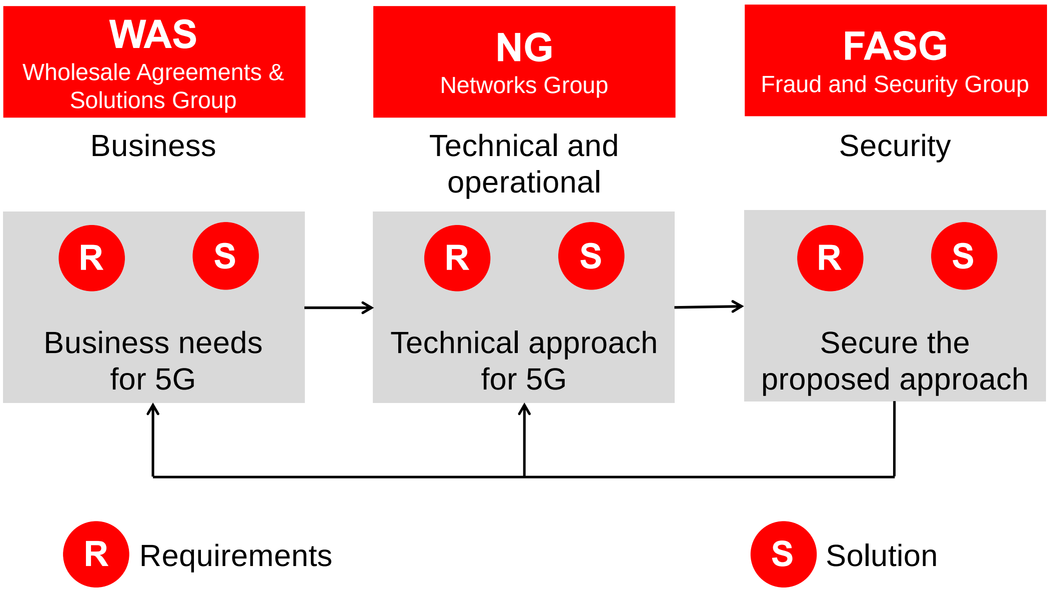


Figure 1 – Requirements & Solution Design

1.3 Scope

This document proposes a set of recommendations for the establishment of 5G roaming agreements between two MNOs (potentially via intermediates like IPX, Roaming VAS and Roaming HUB with further details outlined in section 2) both using a 5GS Core that meet 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. The detailed solution is described in NG.113 Annex B [6] and is based on the following deployment principles and implementation restrictions:

- 5GS Roaming Architecture for bilateral inter-PLMN connections via either direct TLS connections between SEPPs or with TLS connections 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 hosted SEPP with TLS as secure interface between PLMN and hosted SEPP.
- The implementation details of the internal Roaming Value Added Services (RVAS) solution are not described.

The timeline for 5GMRR Phase 1 is shown in Figure 2.

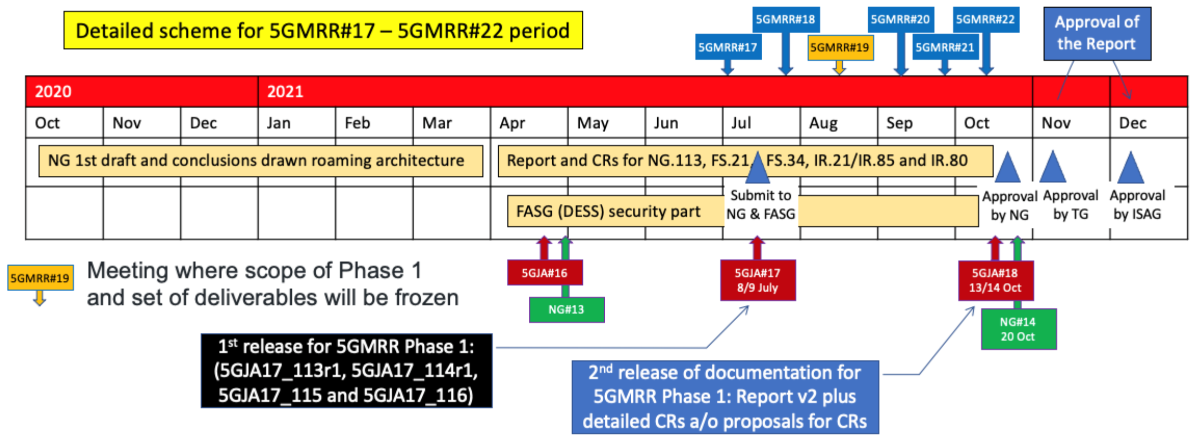


Figure 2 – Timeline for the activities of the 5GMRR task force

GSMA originally requested 3GPP to provide a secure roaming solution for 5G. During the process of revisiting the current roaming solutions to consider all business need, 3GPP will be actively engaged. Depending on the set of recommendations, this timeline may need adaptation in case work is needed in 3GPP.

In Phase 2 more 5GS roaming use cases will be addressed that allow more comprehensive services like by IPX, Roaming VAS and Roaming HUB to be incorporated. The scope and timeline for 5GMRR Phase 2 is not yet defined.

This report is to reflect the findings of 5GMRR Phase 1 with the aim to outline the deliverables that will provide the updated guidelines for 5G Roaming foreseen as CRs to GSMA PRDs like NG.113 [6], FS.21 [8] and FS.36 [9], and the potential refinements of the 3GPP standards. See section 10 for more details about the documentation impact.

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
CP-SOR	Control Plane Steering Of Roaming
DRC	Data Roaming Control
E2E	End-To-End
EECC	European Electronic Communications Code
ENISA	European Union Agency for Cybersecurity
EPC	Evolved Packet Core
HPLMN	Home Public Land Mobile Network
IMSI	International Mobile Subscriber Identity
IPUPS	Inter-PLMN User Plane Security
IPX	IP Exchange
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
NF	Network Function
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
TLS	Transport Layer Security
TSR	Telecoms Security Requirements
UPF	User Plane Function

Term	Description
VAS	Value Added Services
VPLMN	Visited Public Land Mobile Network

1.6 References

Ref	Doc Number	Title
[1]	3GPP TS 33.501	Security architecture and procedures for 5G
[2]	IETF RFC 7540	Hypertext Transfer Protocol Version 2 (HTTP/2)
[3]	IETF RFC 793	Transmission Control Protocol (TCP)
[4]	IETF RFC 7159	The JavaScript Object Notation (JSON) Data Interchange Format
[5]	GSMA PRD IR.73	Steering of Roaming Implementation Guidelines
[6]	GSMA PRD NG.113	5GS Roaming Guidelines
[7]	3GPP TS 23.501	System architecture for the 5G System (5GS)
[8]	GSMA PRD FS.21	Interconnect Signalling Security Recommendations
[9]	GSMA PRD FS.36	5G Interconnect Security
[10]	3GPP TR 29.829	Technical Specification Group Core Network and Terminals; Service-based support for SMS in 5GC (Release 17)
[11]	3GPP TS 23.122	Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode
[12]	3GPP TS 29.550	Technical Specification Group Core Network and Terminals; 5G System; Steering of roaming application function services; Stage 3
[13]	ENISA	Guideline on Security Measures under the EECC https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc
[14]	ENISA	5G Supplement - to the Guideline on Security Measures under the EECC https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc
[15]	EU Toolbox	The EU toolbox for 5G security https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security
[16]	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
[17]	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
[18]	GSMA PRD AA.51	IPX Definition
[19]	GSMA PRD IR.34	Guidelines for IPX Provider networks
[20]	GSMA PRD BA.60	Roaming Hubbing Handbook
[21]	GSMA PRD BA.62	Roaming Hubbing Business Requirements Commercial Model

Ref	Doc Number	Title
[22]	GSMA PRD BA.63	Roaming Hubbing Hub to Hub Operational Procedures
[23]	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"
[24]	S3-212367	Change Request 33.501 CR 1105 rev 1 v15.12.0 "Clarify the usage of TLS and PRINS between SEPPs"
[25]	3GPP TS 29.573	Technical Specification Group Core Network and Terminals; 5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3
[26]	GSMA PRD FS.34	Key Management for 4G and 5G inter-PLMN Security
[27]	UK TSR	United Kingdom Telecom Security Requirements, not yet published.
[28]	GSMA Whitepaper	Mobile Network Operator Business-Need Security and National Security
[29]	GSMA PRD IR.21	GSM Association Roaming Database, Structure and Updating Procedures
[30]	GSMA PRD IR.67	DNS Guidelines for Service Providers and GRX and IPX Providers
[31]	GSMA PRD IR.80	Technical Architecture Alternatives for Open Connectivity Roaming Hubbing Model
[32]	GSMA PRD IR.85	Hubbing Provider Data, Structure and Updating Procedures
[33]	GSMA PRD AA.73	Roaming Hubbing Client to Provider Agreement

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” [18] 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” [19] 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” [20] that provides an overview about Roaming Hubbing.
- GSMA PRD BA.62 “Roaming Hubbing Business Requirements Commercial Model” [21] 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” [22] 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 [1], TS 23.501 [7] and TS 29.573 [25].

There are different regulatory frameworks, such as the EU Toolbox [15] 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 the reference to the GSMA whitepaper in Annex B for details of regulations that would apply for SEPP Outsourcing 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 [8].

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 [7]. Figure 3 shows this split between the N32-based Control Plane and the N9-based User Plane as part of the Roaming 5G System Architecture.

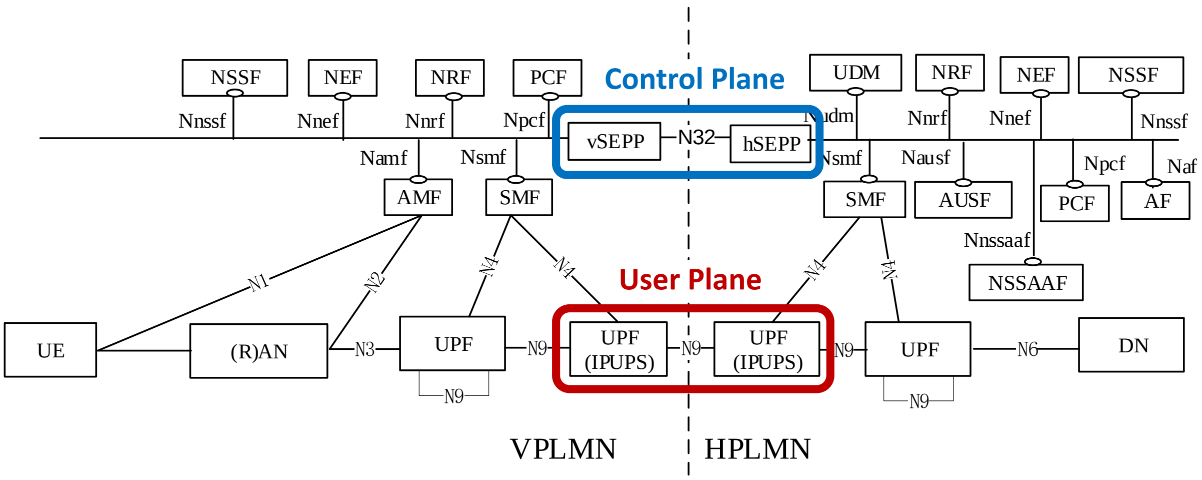


Figure 3 – Roaming 5G System Architecture

2.3.2 Roaming 5G Reference Points

Based on the list of reference points in 3GPP TS 23.501 [7], Figure 4 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 4 – 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 [6] and FS.21 [8] 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 [8] 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 [6].

3.3 Security and Privacy Requirements

As defined by 3GPP in TS 33.501 [1], 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 section 14.4 in FS.21 [8].

3.4 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.

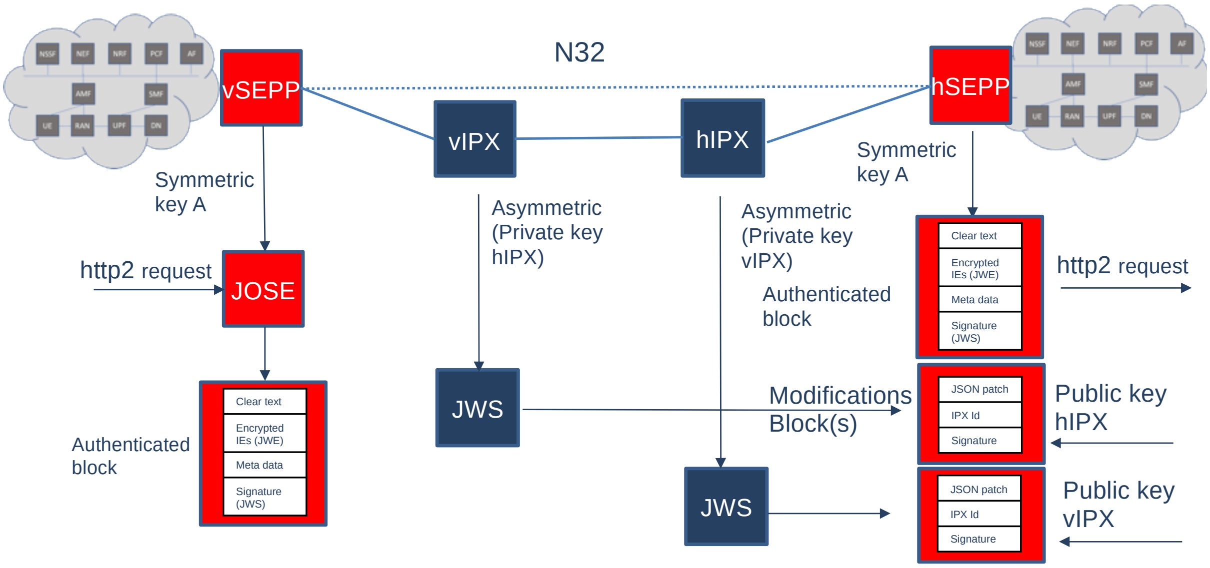
5G addresses the problem in the 3GPP specifications by enabling confidence in signalling integrity and confidentiality and gives the ability to establish authenticity through either:

- 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.

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 5. The use of PRINS is negotiated via N32-c (not depicted).



Key: cMNO / vMNO: consumer's MNO / visited MNO | pMNO / hMNO: producer's MNO / home MNO | (same terminology applies for IPX references)
JOSE: Javascript Object Signing and Encryption | JWS: Java Web Signature

Figure 5 – 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].
- 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.

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

4.3 Direct TLS

The Direct TLS model for the support of 5G roaming is shown in Figure 6. The use of direct TLS is negotiated via N32-c (not depicted).

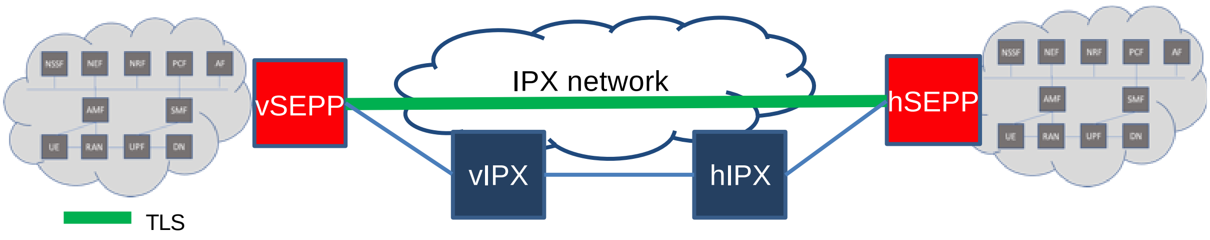


Figure 6 – Direct TLS model for 5G roaming

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 [1] prescribes that for N32-f either Direct TLS is to be used end-to-end for a roaming relation if no intermediaries are on the path, or alternatively, PRINS. 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 a discrete choice to be settled between both 5GS roaming partners.

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 7.

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.

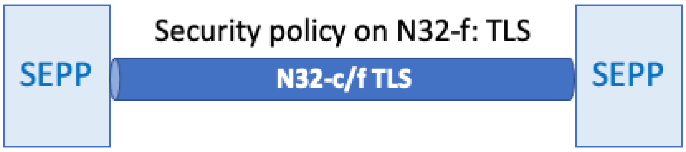


Figure 7 – Direct TLS Architecture

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 8.

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.

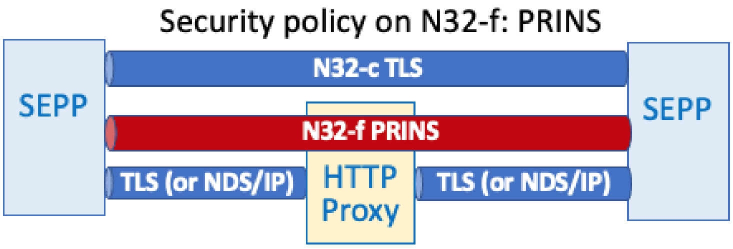


Figure 8 – PRINS Architecture

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).

With the model in Figure 9, 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.

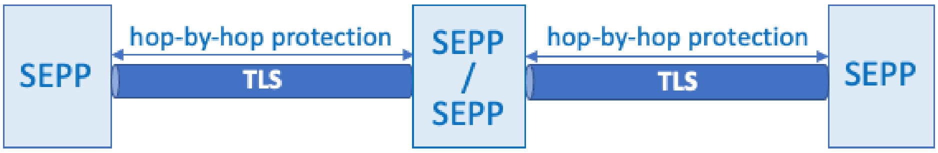


Figure 9 – Direct TLS used with intermediate hops

With the model as in Figure 10, PRINS provides end-to-end protection for sensitive IEs at signaling hops for the confidentiality protected IEs via the PRINS ALS layer.

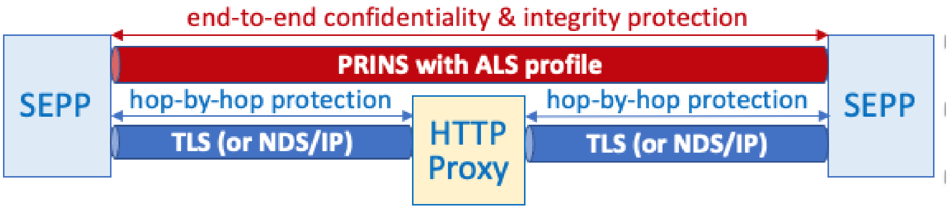


Figure 10 – PRINS used with intermediate hops

PRINS provides more granular and flexible security handling of data transferred between SEPPs. From a security point of view, who attaches or modifyies a particular Information Element in the chain, when IPX is involved, may be con 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 [8] 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 [26] 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 [1] section 5.9.3.2 "Requirements for Security Edge Protection Proxy (SEPP)" for Rel.17 as in the Change Request S3-212287 [23], 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 11 for a VPLMN owning PLMN ID's a, b and c.

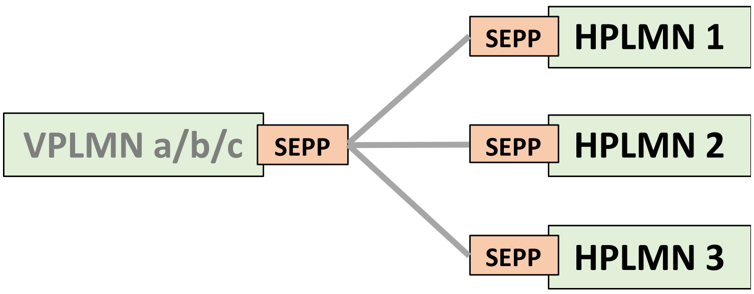
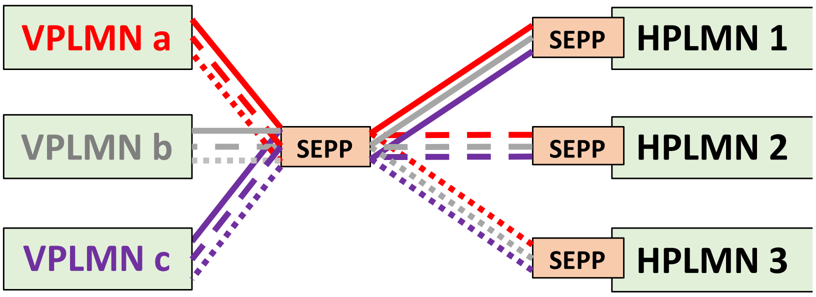


Figure 11 – SEPP using same N32-connection for all VPLMN's PLMN IDs

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 12 for VPLMNs owning PLMN ID's a, b and c.



Each line represents a separate N32-connection

Figure 12 – 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 [1] section 13.1 "Protection at the network or transport layer" about the use of TLS and PRINS as in the Change Request S3-212367 [24], the usage of TLS and PRINS between SEPP is clarified as depicted in Figure 13:

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

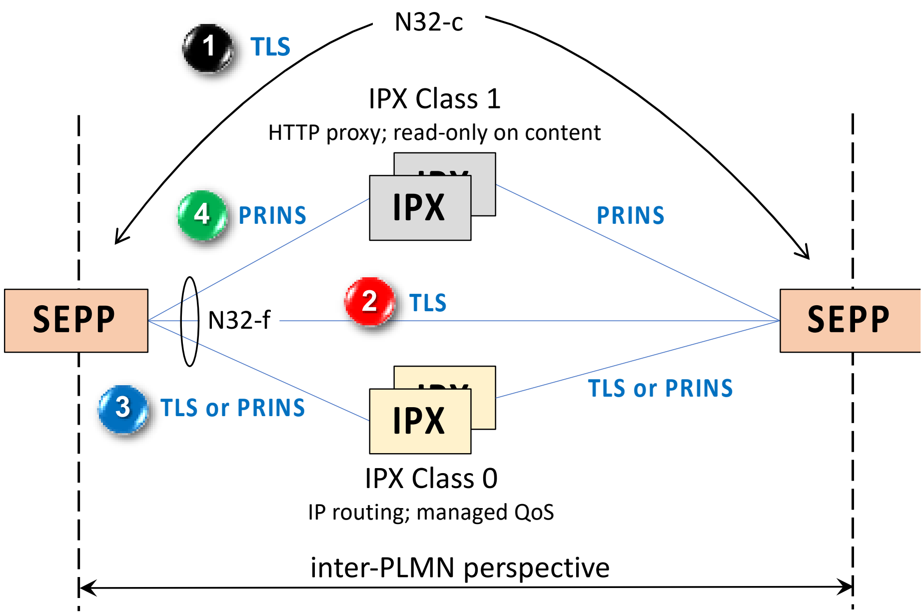


Figure 13 – SEPP using separate N32-connection for connected PLMNs

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.

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 14.

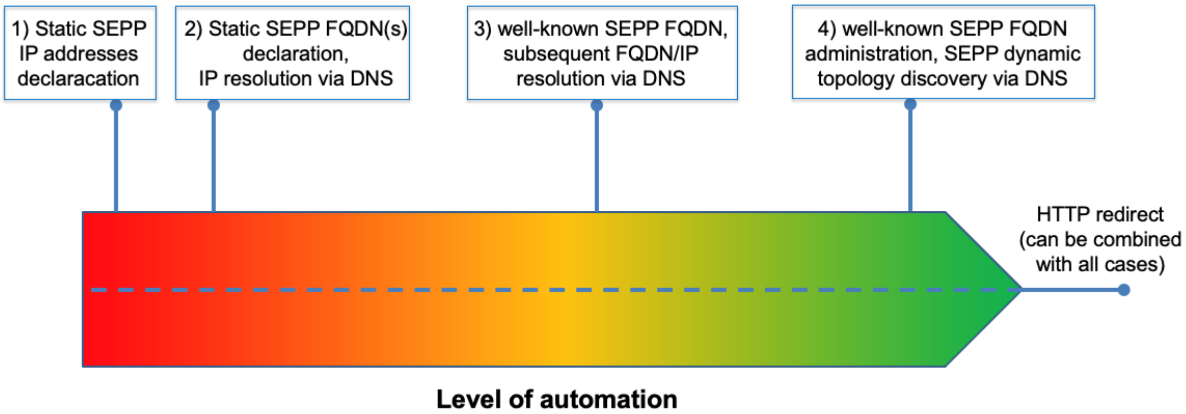


Figure 14 – Options for SEPP discovery based on the level of automation

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 15 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”.

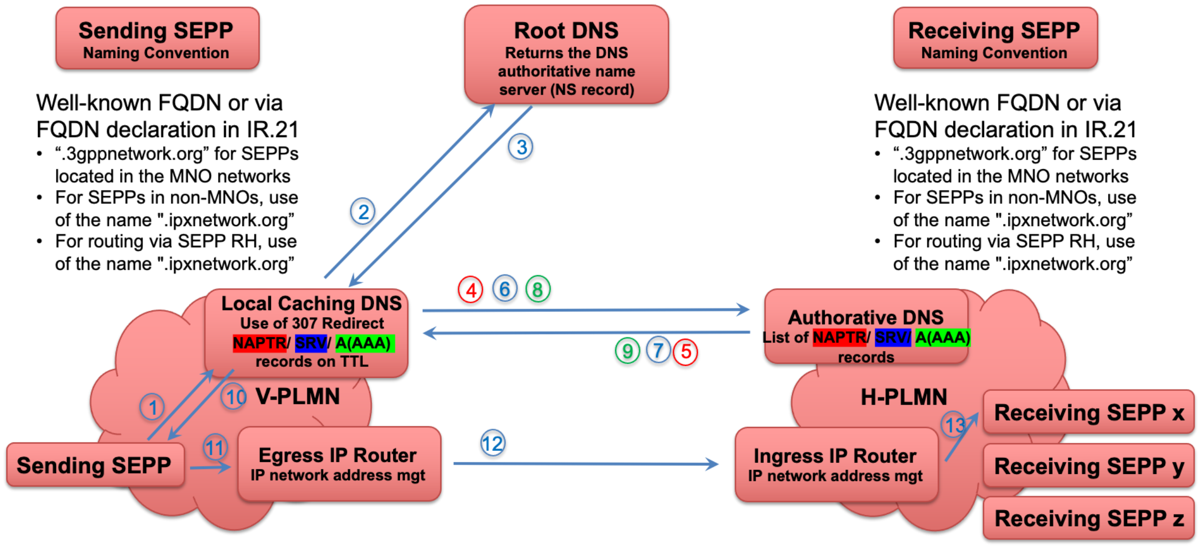


Figure 15 – SEPP dynamic topology discovery with DNS and HTTP Redirect

The solution makes use of both NAPTR records and SRV records as depicted in Figure 16:

- 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.

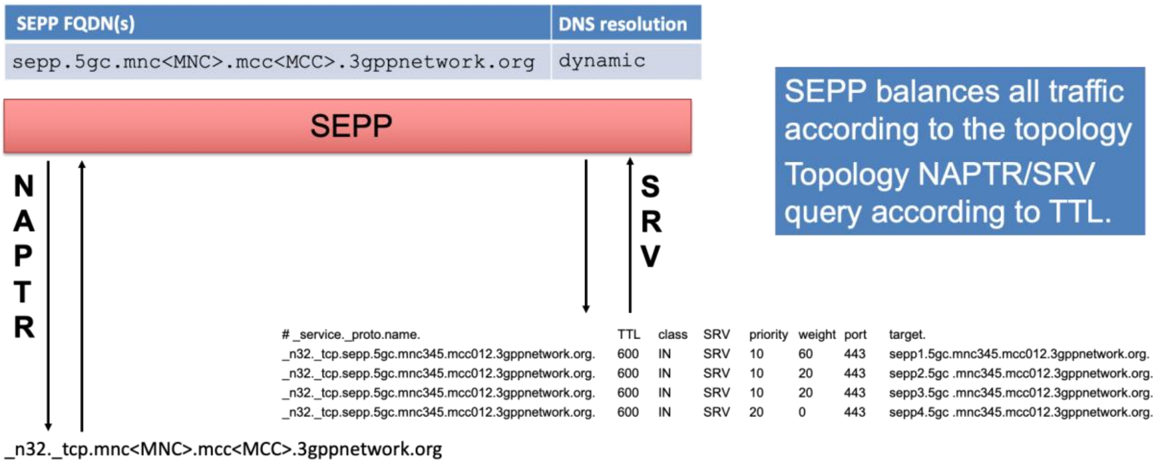


Figure 16 – The use of NAPTR records and SRV records as part of SEPP discovery

The DNS aspects of the SEPP Discovery procedures have been included in IR.67 [30]. 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 [6]. The aspects for SEPP Outsourcing to multiple IPX providers have also been included in the GSMA PRD NG.113 [6].

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

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 [30] 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 [30].

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 [18] and IR.34 [19]) and section 2.1.4 for the definition of the Roaming Hub (RH) service (with the cross references to GSMA PRDs BA.60 [20], BA.62 [21] and BA.63 [22]) in the context of the 5G roaming architecture.

The overview in Figure 17 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 [32] 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.

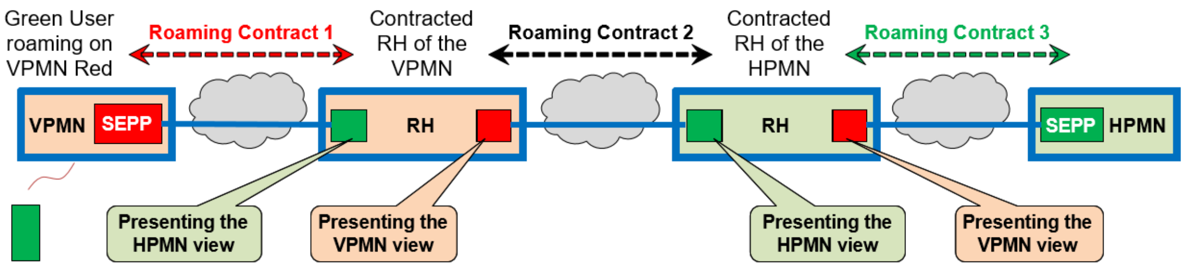


Figure 17 – Roaming Hubbing model and Roaming Contractual relations

The following diagram in Figure 18 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.

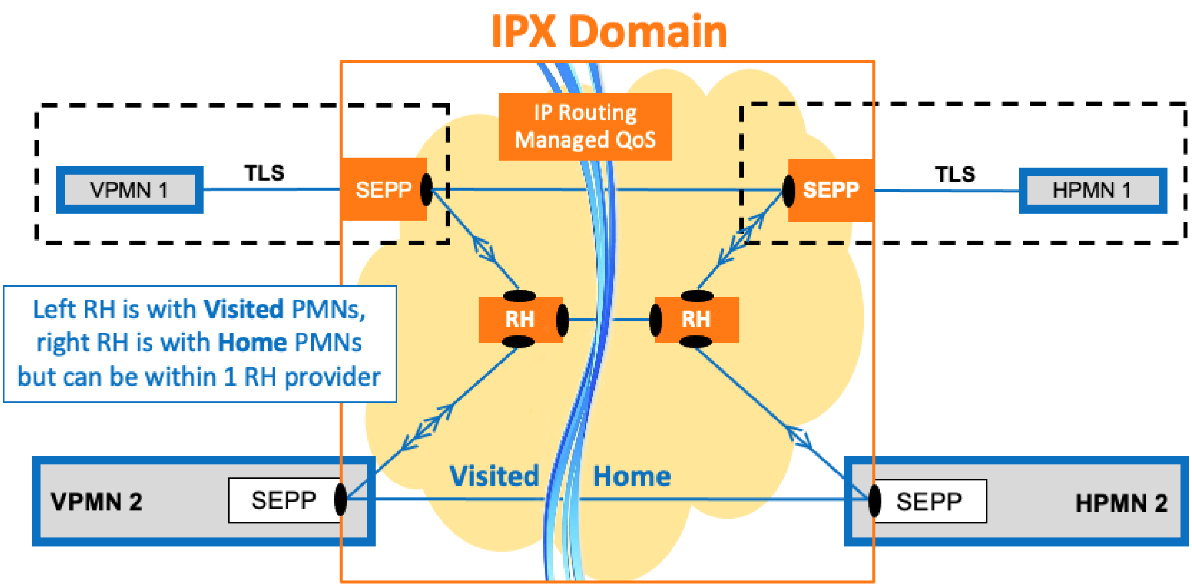


Figure 18 – Perspective of RH added to 5GMRR Phase 1 bilateral model

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

The following is the list of service requirements identified for the Roaming Hubbing service in the 5G SA roaming eco-system (non-exhaustive). The roaming hub shall be able to:

1. Provide services transparently 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.
2. Provide Roaming Hubbing agreements management including financial, privacy and security liabilities.
3. Ability to perform passive tracing for signalling messages & content, i.e. determine that a message or user plane data has passed through the RH. Note: this doesn't mean interception capabilities.
4. Provide CDR generation and storage for wholesale billing mediation, charging and dispute handling.
5. Ability to establish control plane connectivity with the Roaming Partners on behalf of the Client Operators.
6. Ability to 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.
8. Ability to peer with another RH provider, each serving different Client Operators. A maximum of two RH providers shall be supported in a roaming path.
9. Ability to 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. Ability to implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g. FQDNs or PLMN IDs).
11. Business Model – A RH is 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.
12. Trust Model – In Option 2 in clause 6.2 of AA.73 [33] “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 13 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 IR charges.

In Option 3 of the same clause 6.2 of AA.73 [33], the RH provider assumes no such liability.

13. Security Measures – RH providers shall adhere to the same technical security guidelines as those applicable to mobile operators. In this regard, please be referred to FS.21 [8] chapter 14 “Holistic Security approach for Mobile Roaming services” that need to be added as binding condition in the Roaming Hubbing Agreement Templates.

The following is the list of additional considerations for the Roaming Hubbing service in the 5G SA roaming eco-system (non-exhaustive):

1. For service viability, operational efficiency by providing a method to automate or allow streamlined ability to manage multiple connections and certificates by the RH for its operator customers is required.

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 [6] 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 [8].
- CR proposals to IR.21 [29] and IR.85 [32] 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 [31].
- CR to FS.34 v1.0 [26] 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” [9] 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 [19], BA.60 [20], 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 [6].

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 [6] 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

Security and national regulation issues related to SEPP Outsourcing are provided in the GSMA whitepaper "Mobile Network Operator Business-Need Security and National Security" [28].

Annex C Document Management

C.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

C.2 Other Information

Type	Description
Document Owner	Networks Group
Editor / Company	Pieter Veenstra, NetNumber

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.