NTT DATA
Trusted Global Innovator

5G / SOLUTION

Security Edge Protection Proxy

"Security in 5G roaming service delivery"

SEPP (Security Edge Protection Proxy) is a key function for 5G roaming scenarios, as clearly required by 3GPP technical specifications.

The 3GPP standardization body explicitly mentions SEPP as a mandatory functional component between pairs of roaming parties, where each Operator participates in such relationship with its own identity and edge infrastructure. SEPP is required to manage the connectivity in trusted mode and to ensure that the exchange of information (signalling) among Operators may take place in a confidential, secure and robust way, aiming to protect against malicious attempts or attacks on data confidentiality, identity spoofing or information tampering.

A couple of 5G-enabled Operators establish a Roaming relationship, aiming to provide (differentiated connectivity) services to mobile users connected out of the scope of their own Home Network PLMN (HPMN). The Visited Network PLMN (VPMN) where the roaming user attaches its own device has a signalling relationship with the corresponding HPMN, based on authentication and service permissions for being connected. Both VPMN and HPMN are provided with SEPP.

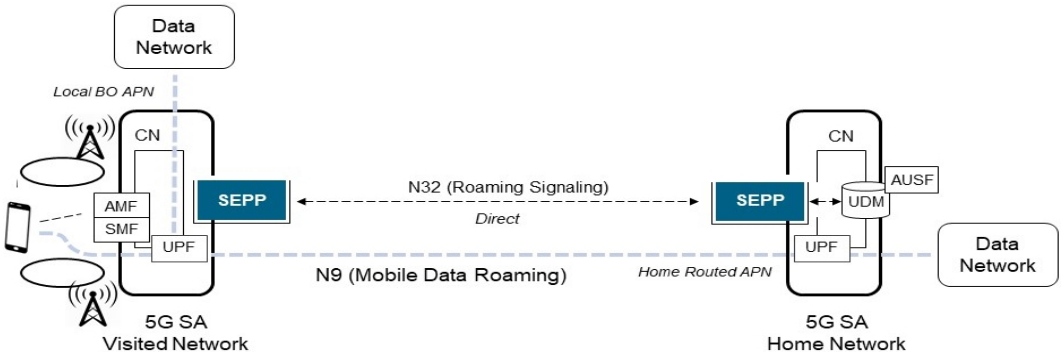
SEPP components plays the role of Edge signalling proxy, capable to establish a trusted connection among Operators for the secure roaming signalling dialogue. User identity, Service Profile, User Credentials are exchanged between VPMN and HPMN for the individual users. SEPP assures the integrity and confidentiality of such dialogue. The flow between a couple of SEPP nodes is referred by standards as N32 interface.

A couple of Operators can be directly in touch for roaming procedure or interconnected through a third party entity, namely a Roaming Carrier, as a “man-in-the-middle” schema. Operators and Carrier are all equipped with SEPP components, in order to create a sort of star topology where the Carrier is the center.

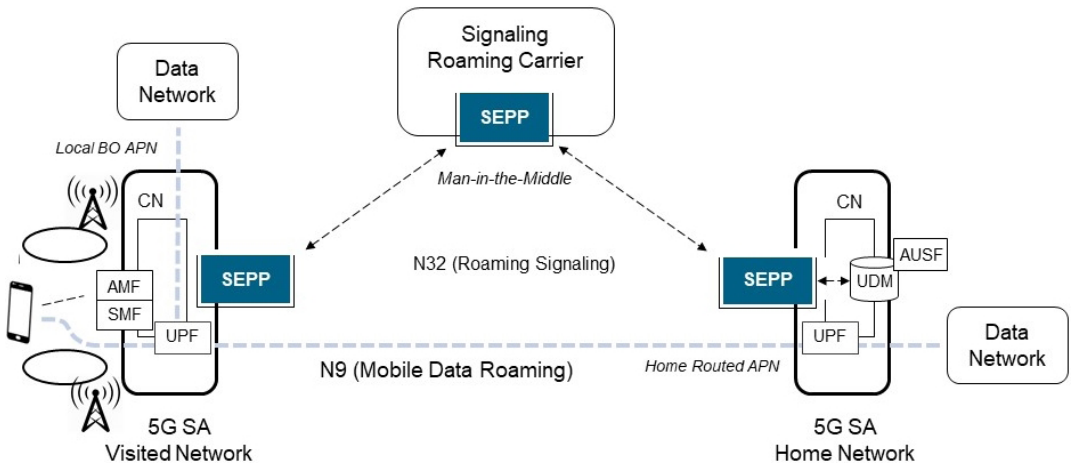
SEPP Scenario

“Direct Scenario and Carrier involvement”

In specific, what is under SEPP scope is the actual implementation of N32 reference point. The current indications coming from 3GPP/ETSI standardization body focus on an overarching guideline, based on the following points:



In case of MNO-to-MNO roaming relationship (“direct” scenario), SEPP components from both the Operators authenticate one each other in order to negotiate (N32 Control interface, N32-c) the security-related topics on (HTTP/2 encrypted) message forwarding (N32 Forwarding interface, N32-f) and for exchange API primitives. Control and message Forwarding procedures leverage on Transport Layer Security (TLS) encryption.
In case of transport network domains (IPX subjects) between MNO couples, SEPP include the opportunity to manage an additional standard layer of security (Application Level Security, ALS) for protection. ALS is capable to encrypt parts of the exchanged messages but keeping some information elements open to changes (clear type) by IPX subjects. That scenario requires a standardized mechanisms (named Protocol for N32 INterconnect Security, PRINS) to safely allow the manipulation of “clear” attributes as stated by the N32-c handshake procedure directly executed between MNOs. Apart of the manipulation of clear type attributes, PRINS doesn’t include any service logic on signaling procedures between the Operators.



In case another entity is present between two Operators, acting as Roaming Hub, a “man-in-the-middle” schema must be provided, with additional service logics (Value Added Services) involved in the flow. The “man-in-the-middle” (MiM) scenario is therefore interesting for Operators and Carriers in a Roaming Hub solution. Value Added Services (VAS) may enhance the elaboration and the content of messages (HTTP/2 primitives). TLS mode is managed by Roaming Hub with appropriate transparency mode, where a Roaming Hub can act “on-behalf-of” served MNOs. Handshakes are executed between MNOs and Hub, with an individual context identifier for each MNO aiming to secure the dialogue. Consequently, the requested schema, without any lack of conformity of technical specifications, shall introduce of a more extended and flexible way to address the destination for message forwarding with crossing through Roaming Hub. Indeed, MiM schema with Roaming Hub involvement is the preferred scenario for the optimization of roaming topology and for the engagement of centralized service nodes by Carrier.

SEPP Function is provided by NTT DATA as a product based on NTT Data 5G Enabling Fabric (5GEF®) platform, available for the virtualized deployment as VNF/CNF components over NFVI platforms.

Reference Standards

"SEPP enables Service Based Architecture"

The following standard references are included in the document, just to mention the most relevant references – not intended to be an exhaustive list– for the functionalities involved in SEPP Emulation. Hereafter the list, with the motivation for the reference.

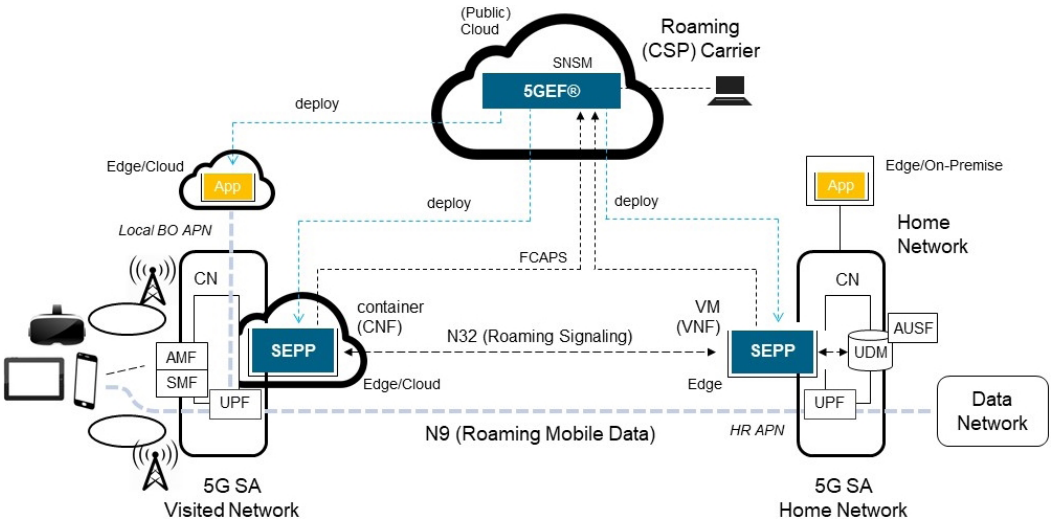
- TS 29.500 – Description of Service Based Architecture, as primitives and NFs.
- TS 29.573 – Description of N32 interfaces between SEPPs.
- TS 33.501 – Description of Security guidelines for 5G architecture, including SEPPs.
- TS 29.571 – Description of Data Model adopted for Provisioning on SEPPs.
- TS 23.501 – Description of NFs and related API primitives, including 5G Roaming.

•TS 23.501 – Description of NFs and related API primitives, including 5G Roaming.

NTT DATA SEPP Product Concept

"SEPP definition is following the ongoing standardization process"

NTT Data SEPP product pave the way for the simplification of the implementation of 5G Roaming. The paradigm of SBA and the idea of service invocation for the dialogue among network and application functions is extended to the deployment model. In Cloud environment, SaaS applications are deployed and reachable through their associated URI. SEPP are deployed as a Cloud SaaS application.



The virtualized environment is prepared based on the resources available for such delivery. The same may apply for 5G network functions, as definitely for the Security Edge Protection Proxy, as well. SEPP components are deployed automatically as a virtualized network function. 5G Enabling Fabric (5GEF®) can deploy the SEPP as 5G use case on a remote (edge server) platform. In the standard scenario, both the two options will be implemented for 5G roaming SA network, “man in the middle” and “direct” connection, based on the presence of centralized services at Roaming Hub level.

SEPP can be deployed as virtualized machine (VNFs, OpenStack default) or container-based platform (CNFs) based on Docker/Kubernetes platform, either on-premise or public Cloud/Edge solutions (AWS EKS).

In addition, SEPP product is also inclusive of protection, autoscaling and redundancy logic, since fault, assurance and overload characteristics are a relevant part of the solution.

Physical Layer

“Physical and Virtualized deployment”

SEPP is designed as a set of VNF/CNF components, deployable on a generic NFVI layer. The SEPP can be also delivered with a certified hardware platform, integrated with NTT Data software components, with flexible and stackable MNO solutions coming from edge boxes up to data center 19” bricks, with in addition fully scalable high-capacity nodes addressing Roaming Hub solutions.

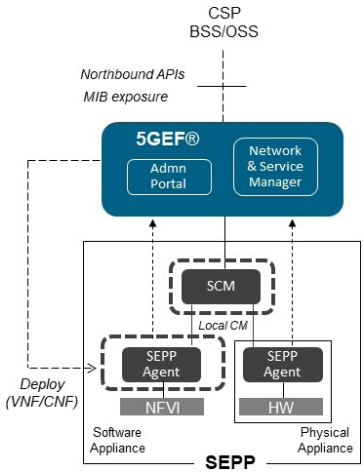
SEPP Configuration Manager (SCM)

"SEPP function is created as a dynamic 5G Service"

SEPP Configuration Manager is an Application Function deployed as a 5G Service and capable to configure and provision SEPP components. A single SCM instance per network domain (or Data Center tenancy) is requested.
5GEF is capable to deploy SCMs and SEPPs as 5G Services included in MNOs or third party domains, as 5G applications for Operators. The Roaming Carrier could potentially act as a Cloud Service Provider (CSP) for such scenario. SBA paradigm is followed

The deployment of the solution includes the following features:

- Creation of Edge Computing server or Data Center (EDC)
- Creation of VM or container-based platforms
- Deployment and Activation of SCM, SEPP application instances



5G Enabling Fabric (5GEF®)

"Enabling 5G Solutions as use cases for Operators"

5GEF® is a cloud based platform specifically designed for configuring and delivering business services to enterprise customers or Telco Operator environments. NTT Data's solution provides Telcos and MNOs with a modular platform for deploying business applications provided by any relevant vendor, to virtually any location worldwide. In case of 5G Roaming, SEPP components are deployed as SBA components, fully virtualized, and activated by remote in few-clicks.

A slice-oriented architecture supports delivery of secure, dedicated services on a global shared platform, while an abstraction layer enables customer self-selection for automated launch of configurable use cases.

Additional key features:

- Standard Network Slicing model (GSMA)
- Now Ready for 4G or 5G NSA early deploy
- Focused on 5G SA solutions
- Deliverable for Cloud Service Providers
- Supported Pay-per-use and SaaS applications
- 3GPP NSMF, CN NSSMF.

The innovation introduced by 5GEF® offers the opportunity for Telco Operators to play as Cloud Service Providers in terms of flexibility, fast service delivery and resources optimization in a completely orchestrated and simplified way for the Customers.