NTT DATA

Security Edge Protection Proxy

Index

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 (signaling) 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.

Market Clients clearly demand to have additional features located at SEPP level to the ones from the standard, for domain security, certificates, manipulation and filtering on messages, and roaming traffic documentation for billing purposes.
Those features come from GSMA recommended scenarios, the NTT DATA SEPP Implementation is ready to support.

Enablement of Roaming Services

A couple of 5G-enabled Operators establish a Roaming relationship, aiming to provide 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 (SEPP chain topology) as per GSMA recommendations. Operators and Carrier are all equipped with SEPP components, to create a sort of star topology where the Carrier is the middle.

Aim of NTT DATA solution for 5G stand Alone Roaming is to provide Operators and Carriers with SEPP functionalities as a cloud-native application, delivered as containerized Network Function (CNF) trough automated and zero-touch Edge deployment, with autoscaling, redundancy and disaster recovery features whenever requested.

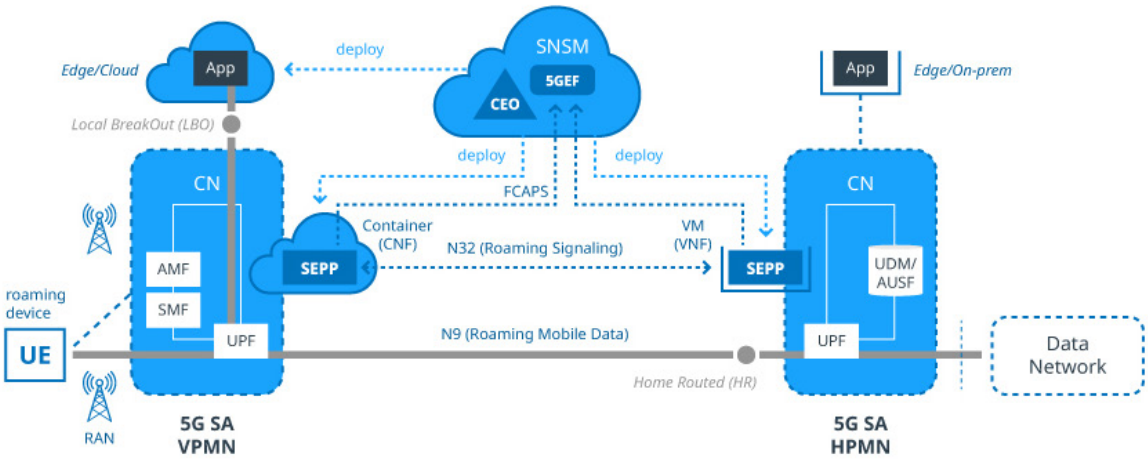
SEPP Delivery

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 Network Functions are deployed as cloud applications, as network services. The containerized environment is prepared based on the resources available for such delivery SEPP Network Functions are created and managed through the SEPP Network & Service Manager (SNSM), which is a module of NTT DATA 5G Enabling Fabric (5GEF®) product suite. The dialogue between SNSM and SEPP instances is based on 3GPP standard APIs and resource model.

SEPP deployment is provided over Kubernetes® containers (CNF components), both on-prem (K8S) and Edge or cloud (CaaS), preferably over Amazon Web Services technology (AWS EKS®, ECS® and serverless over AWS Fargate®). Hybrid deployment over VM-based environments, as OpenStack®, Linus KVM® and VMware vSphere® is also supported. Google GCP® and MS Azure® are also supported, providing a high level of flexibility and scalability. Target is to reduce vendor lock-in. NTT DATA CreEdgeOn deployment manager can do it automatically (CI/CD pipeline), by exposing standard APIs to SNSM manager.

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



5G SA	5G Stand Alone (full standard)	RAN, CN	Radio Access Network, Core Network
N32	3GPP Roaming Relationships interface	AMF	Access Management Function
TDR	Transactions Detailed Record	SMF	Session Management Function
IPX	Internet Packet eXchange (Data Carrier)	UDM	User Data Management
HPMN	Home Public Mobile Network	AUSF	Authentication User Service Function
SEPP	Security Edge Protection Proxy	UPF	User Plan Function
SNSM	SEPP Network & Service Manager	VPMN	Visited Public Mobile Network
CNF	Containerized Network Function	5GEF	5G Enabling Fabric
VNF	Virtualized Network Function	CEO	CreEdgeOn

SEPP Interoperability

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 to negotiate (N32 Controlinterface, N32-c) the security-related topics on (HTTP/2 encrypted) message forwarding (N32 Forwarding interface, N32-f) and for exchanging 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 theex changed 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 themanipulation of “clear” attributes as stated by the N32-c handshake proceduredirectly executed between MNOs. Apart of the manipulation of clear type attributes, PRINS doesn’t include any service logic on signaling procedures between the Operators.

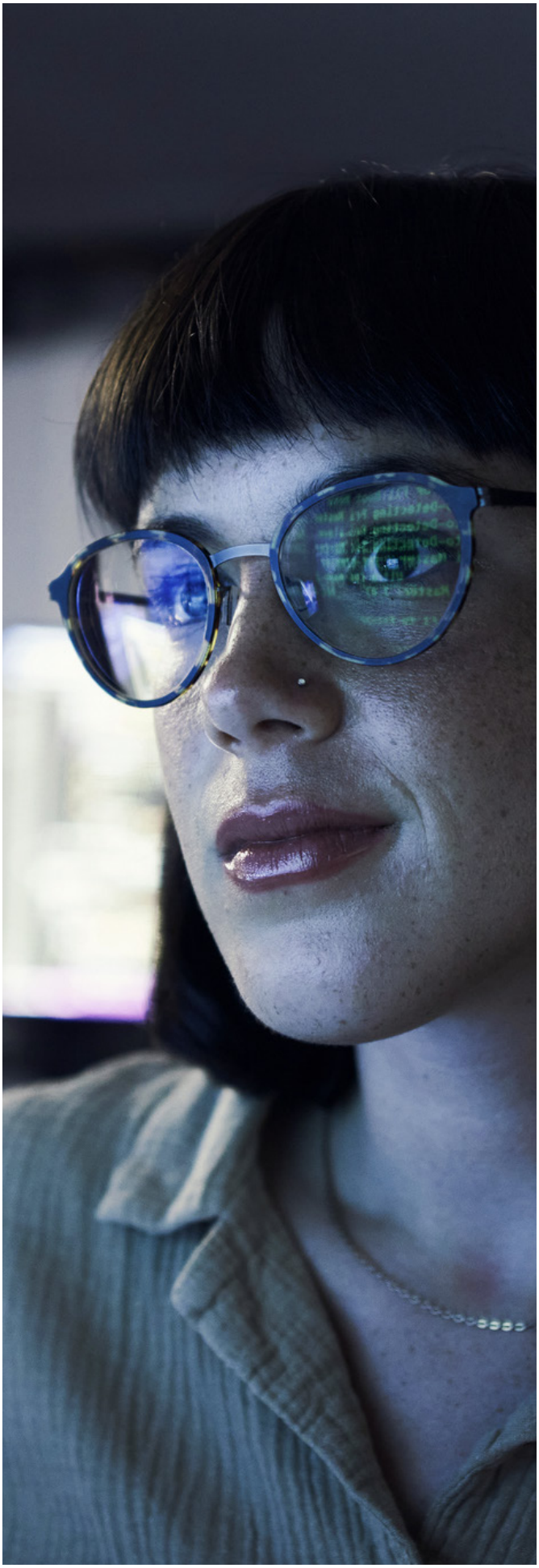
In case another entity is present between two Operators, acting as Roaming Hub, a “man-in-the-middle” (SEPP chain) schema must be provided, with additional servicelogics (Value Added Services) involved in the flow. Such scenario is therefore interesting for Operators and Carriers in a Roaming Hub solution. Value Added Services (VAS) may enhance the elaboration (manipulation, filtering, Steering of Roaming) and the content of messages (HTTP/2 primitives). TLS mode is managedby 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 optionally an individual context identifier for each MNO aiming to secure the dialogue. Consequently, Hub solution introduces a more extended and flexible way to address the destination for message forwarding, with the optimization of roaming topology under the Carrier’s control.

SEPP Network & Service Manager (SNSM)

5GEF® module SNSM is capable to provide FCAPS management for SEPP nodes. SNSM exposed northbound interfaces towards cross-domain OSS systems, by using 3GPP standard APIs and resource model. All the relationships between operators and N32 routes are configured by SNSM. A supportive GUI can also help the administrator to manage all the SEPP nodes in scope. The SNSM component is intended for Service Providers' adoption, since they offer the Roaming Services to different operators, or otherwise Carriers provided with thei rown Hub. Alternatively, Operators can use SNSM to manage Roaming nodes within their own network infrastructure.

Routing Tables

The Roaming Service administrator can have access to SEPP Network Functions in order to describe the routing rules for inbound and outbound traffic routes, with up to four IP addresses for each individual destination. NTT DATA SEPP supports load balancing (round robin) policy for resources optimization and redundancy. Alternatively, primary/secondary routing policy is supported for disaster recovery requirements (secondary choice is selected in case the primary option is no more reachable, revertive mode applies when the primary choice is restored). N32 handshake is established between local and remote SEPP nodes any time a fault condition is recovered.



Service Communication Proxy

NTT DATA SEPP support sembedded Service Communication Proxy (SCP) function, aligned with 3GPP standard, which is useful to facilitate the enablement of 5G Core Networks with 5G Stand Alone Roaming services, including SEPP Network Functions. Both SEPP and SCP functions are registered to Network Resource Function (NRF) for mapping the 5G Core related AMF, SMF, AUSF, UDM and PCF Network Functions.

Manipulation and Filtering

NTT DATA SEPP can manage message manipulation and filtering rules. SPP instances can ingest textual files with metadata information for managing the requested changes. The rules are enabled run-time as soon as the textual files are ingested. Manipulation and filtering are monitored, counted, and periodically collected as performance indicators.

SEPP Portal

Each individual SEPP instance is deployed with its own configuration GUI. Local administrators can provision SEPP instances for local routing tables (testing purposes), for manipulation and filtering rules, for retention of Transaction Documentation Record (TDR) forevery active N32 route, and also for integrating the configuration of embedded SCP services and NRF information. The SNSM managed and the SEPP Portal are aligned one each other, by means of a flooding mechanism that synchronize the SEPP Network & Service Manager with all the local SEPP Instances any time an attribute change session is committed.

Hosted SEPP

A Roaming Service Provider, or a Carrier, can deploy SEPP Network Function and assign them to Operators in hosting mode. Such “Hosted SEPP” service implementation by NTT DATA is aligned with GSMA standardized use cases and compliant to 3GPP standards for N32 security and operation.

Transaction Documentation Records

Transactions (HTTP/2 primitive invocation and related acknowledge) are counted and periodically collected as accounting information. Retention period is by default set to 24 hours. Counter are exposed through SFTP files as well as exported through exposed APIs for billing purposes by external systems.

Certificates

SEPP instances manage TLS related certificates for N32 handshake and message forwarding message flows.NTT DATA SEPP implementation is capable to manage mutual authentication, required by producer (server) to consumer (client). Whitelist restrictions can be defined atproducer SEPP side, to restrict the roaming conditions for improving security.

> NTT DATA SEPP product and SNSM manager, as module of 5GEF® product suite, propose a cloud-native solutioneasily delivered to Operators and Carriers by Service Providers with zero-touch and automated deployment pipeline. It is an effective way to accelerate 5G diffusion, IoT enablement, and monetize the benefits coming from 5G technology and the innovation path towards IOWN.

NTTDATA

NTT DATA – a part of NTT Group – is a trusted global innovator of IT and business services headquartered in Tokyo. We help clients transform through consulting, industry solutions, business process services, IT modernization and managed services. NTT DATA enables clients, as well as society, to move confidently into the digital future. We are committed to our clients' long-term success and combine global reach with local client attention to serve them in over 50 countries.

Visit us at nttdata.com.

The NTT DATA Innovation Centre comprises a Strategy Headquarters, the headquarters that defines the technology strategy, and local centres in six countries (Japan, the United States, Italy, Germany, China and India), each one dedicated to specific technology areas with around 100 experts, mainly researchers, consultants and engineers. Thanks to joint R&D initiatives with leading companies, technology partners and collaboration with universities and start-ups, these centres will be among the first to gather information on advanced technologies to set future strategies. success and combine global reach with local client attention to serve them in over 50 countries.

Via Calindri, 4
20143 Milano
+39 02 831251


NTT DATA