MAVENIR

DATA SHEET

SECURITY EDGE PROTECTION PROXY (SEPP)

The Security Edge Protection Proxy (SEPP) is an essential 5G Core Network Function that provides protection for signaling exchange between roaming Mobile Network Operators (MNOs) at the 5G interconnect control plane level.

SEPP provides secure communication between the local PLMN and the remote PLMN for the signaling communication over all roaming interfaces. SEPP supports the local breakout roaming case in addition to the home routed roaming case transparently, while securing communications over all roaming interfaces, i.e., N8, N10, N12, N16, N21, N24, N27, and N31.

KEY FEATURES

- 3GPP Release 17 interfaces
- Cloud Native network functions
- Service Based Architecture
- Interconnect filtering, policing, and fraud detection
- Orchestration and Automation

The fundamental functionality of SEPP is to provide message filtering and policing on inter-PLMN control plane, in addition to topology hiding and protection against all fraud use cases that have been identified by GSMA in FS.36 and FS.21. Additionally, the local SEPP ensures that only an authenticated and authorized local 5G Core (5GC) Network Function (NF) can communicate with its peer 5GC NF in the remote PLMN over the N32 interface.

The remote SEPP ensures that the operator permitted roaming messages are received over a secure N32 interface from an authenticated remote SEPP according to the operator roaming policy agreed with the remote PLMN.

Supported services and interfaces

Figure 1 illustrates the services and reference points supported by SEPP. N27 is used as an example for communication over N32.

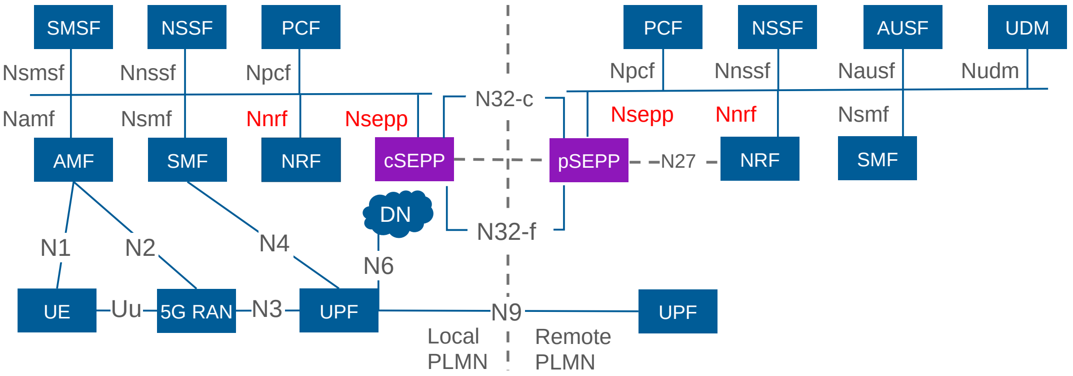

Figure 1: Service-based Representation

SEPP consumes the **Nnrf_NFManagement** service to register, update or deregister its profile in the NRF.

The **Nsepp_Telescopic_FQDN_Mapping** service is provided by SEPP to other local PLMN 5GC NFs. It allows the consumer NFs (e.g., NRF, NSSF) to request the SEPP to construct a telescopic FQDN for a destination in the remote PLMN (roaming partner), so that the local 5GC NF can establish a TLS connection to the local SEP (e.g., AMF) or an SCP in the case of indirect communication.

Cloud Native Principles

- Stateless functional software elements with state-efficient processing to achieve greater resource efficiency and webscale capacity
- Microservices based software disaggregation with connectionless messaging protocol (REST APIs)
- Fully automated Life Cycle Management (LCM) and scalability based on Kubernetes integration
- Service Based Architecture (SBA) using web-based APIs (e.g., HTTP/2)
- Continuous Integration and Continuous Delivery
- (CI/CD) software pipeline
- Deployment flexibility — all Mavenir products and solutions including SEPP can be deployed on ANY cloud
- Dynamic mediation and scalability:
  - SEPP performs dynamic mediation for inter-PLMN connections where interoperability issues are more likely to occur
  - SEPP is built on microservices that have small image sizes, which facilitate quick and dynamic scaling compared to hardware specific solutions or VMs with specific hypervisors

Mavenir SEPP Features

- Message filtering and policing on inter-PLMN control plane interfaces
- Local PLMN topology hiding
- Telescopic FQDN for direct and indirect mTLS connection with local 5GC NFs
- Support direct end-to-end TLS connection with the remote SEPP
- Support Protocol for N32 Interconnect Security (PRINS) for securing communication over N32-f where IPX(s) present between local & remote SEPPs
- Integration with Fraud Management System for multi-technologies networks Unified Fraud detection
- Support DoS and DDoS protection on per remote PLMN, Reference point, Peer SEPP, Remote-NF, etc.
- Support Unified flexible rule engine via LUA scripting
- Support stateless application while supporting integration with stateful firewall
- Support indirect communication with local PLMN 5GC NFs via SCP
- Support throttling and overload control
- Supports dynamic scaling of microservices, stateless availability and performance in a fully cloud-native environment

Standards References

- 3GPP TS 23.501 v17.4.0: System Architecture for the 5G System
- 3GPP TS 33.501 v17.5.0: Security architecture and procedures for 5G System.
- 3GPP TS 29.573 v17.4.0: 5G System; Public Land Mobile Network (PLMN) interconnection
- GSMA FS.36 5G Interconnect Security
- GSMA FS.21 Interconnect Signalling Security Recommendations

Maximizing Investments

To help optimize technology investments, Mavenir and its partners offer complete solutions that include professional services, technical support, and education.

For more information, contact a Mavenir sales partner or visit mavenir.com.

About Mavenir

Mavenir is building the future of networks and pioneering advanced technology, focusing on the vision of a single, software-based automated network that runs on any cloud. As the industry's only end-to-end, cloud-native network software provider, Mavenir is transforming the way the world connects, accelerating software network transformation for 250+ Communications Service Providers in over 120 countries, which serve more than 50% of the world's subscribers.

For more on Mavenir solutions please visit our website at www.mavenir.com

Ver. 20221021