MAVENIR

SECURING 5G SIGNALLING FOR ROAMING (SEPP)

WHITE PAPER

October 2022

INTRODUCTION

5G brings a paradigm shift in network security

Fifth-generation (5G) wireless technology is built on a services-based architecture that uses HTTP/2 based signalling. Being the communication language of the internet, attackers and fraudsters are more familiar and knowledgeable about HTTP/2, and the security mechanisms used for 4G and earlier Gs are no longer adequate or secure enough.

Interconnection and roaming are critical for mobile operators and they are highly interested in ensuring the security of all inter-PLMN (Public Land Mobile Networks) signalling and traffic.

Hence, 3GPP built in security into the 5G architecture and standards—to make it '**secure by design'**— by defining N32 as the interconnection interface. And their System Security Group (3GPP SA3) has defined a mechanism for securing the 5G signaling over the interconnect by introducing the **Secure Edge Protection Proxy (SEPP),** which protects the edge of the mobile operator 5G Core network.

KEY TOPICS IN THIS WHITE PAPER

- 5G brings a shift in network security
- SEPP significance in 5G
- SEPP – Securing the 5G Interconnect
- SEPP – The Mavenir advantage
- 5G SEPP features and capabilities
- 5G SEPP use-cases

In comparison to 4G and earlier generations, SEPP is a new network element and its main function is to protect the local mobile network edge, acting as the security edge proxy on the interconnection between the local network and remote networks.

SEPP SIGNIFICANCE IN 5G

SEPP is a proxy that sits at the perimeter of the PLMN and oversees the transit of all roaming signaling traffic across the operator network. It ensures end-to-end confidentiality protection, integrity, and replay protection between the source and destination PLMNs for all inter-PLMN SBI signaling traffic.

For the purposes of roaming, mobile operator networks may be connected to other operator networks directly or via intermediaries—such as IPX providers or roaming hubs—which provide interconnectivity and services to mobile operators and their roaming partners.

SEPP – Securing the 5G Interconnect

When the visiting (local PLMN) and home (remote PLMN) networks are directly connected and end-to-end Transport Layer Security (TLS) is used, the 5G signaling passing over the interconnect between the two PLMNs is encrypted end-to-end. In this case, intermediaries such as IPX providers may offer only IP routing service.

However, to allow other roaming services, 3GPP defined the Protocol for N32 Interconnect Security (PRINS). PRINS decouples the integrity and confidentiality guarantees from the end-to-end encryption provided by TLS, without compromising either, using application-level security. Intermediaries such as IPX service providers may securely inspect and/or modify the signaling during transit, if allowed by the protection and/or modification policies defined by the interconnected operator networks or GSMA. The receiving PLMN network can validate and verify that any modifications were performed in accordance with the effective policies by the intended intermediaries.

The value of SEPP is augmented by:

- **Traffic Filtering and policing** – The authentication between SEPPs provides proof of origin which enables effective filtering of traffic coming over the interconnect. SEPP provides firewalling and policing of the N32 interface and NF-specific roaming interfaces, and against malformed signaling messages.
- **A new application-level security (PRINS) protocol** on the N32-f interface between the SEPPs – designed to provide end-to-end protection of sensitive data attributes, attribution, and replay protection while still allowing mediation services over the interconnect.
- **Topology hiding** – This functionality hides the internal topology information of a PLMN from the external parties.

MAVENIR

5G SEPP – THE MAVENIR ADVANTAGE

Mavenir's Secure Edge Protection Proxy (SEPP) is a state-of-the-art security proxy that supports both local breakout roaming and home routed roaming transparently, while securing communications over all the roaming interfaces. It provides the following advantages:

- **Cloud Native** – Mavenir's SEPP is purpose-built for the cloud-model, offering easy scaling, hardware de-coupling, agility, portability, reduced capex, high availability, and resilience across multiple cloud environments. It supports containerized deployment on any cloud.
- **Microservices-based** – Mavenir's SEPP is built using microservices that allow de-coupling from the platform and network infrastructure. Its service-based APIs provide flexibility and extensibility for service agility. The Network Function (NF) is based on microservices, containerized, reliable, agile, and stateless. This architecture lends control and simplicity to the environment.
- **Any Cloud** deployment – SEPP along with Mavenir 5G Core (5GC) NFs can be deployed on ANY cloud: private (Kubernetes, OpenStack, VMware, etc.), hybrid or public (AWS, Google Cloud, Microsoft Azure, etc.).
- **Advanced Inter-PLM Security** – Mavenir SEPP is 3GPP Rel. 17 compliant and supports PRINS
- **Resolves inter-PLMN interoperability issues** – Mavenir SEPP provides a dynamic, real-time mediation capability.
- Enables **operator special use-cases,** such as Data Network Name (DNN) replacement, Steering of Roaming (SoR), Policy based special routing, Mobile Virtual Network Operator (MVNO), etc.
- Continuous Integration and Continuous Delivery **(CI/CD)** software pipeline.

SEPP Features and capabilities

Mavenir's SEPP provides the following features:

- 3GPP application-level protection, message filtering and policing on inter-PLMN control plane interfaces.
- Support for all filtering criteria as defined in GSMA FS.36.
- Support for network slicing and source network PLMN-ID validation.
- Support for NRF services per 3GPP TS 29.510 and other related specifications.
- SEPP intra-PLMN and inter-PLMN security procedures.
- Home PLMN topology hiding.

- Telescopic FQDN for direct and indirect mTLS connection with home 5GC NFs.
- Support for PRINS for N32 Interconnect Security for securing communication over N32-f where IPX(s) present between home & visited SEPPs.
- DoS and DDoS protection on per visited PLMN, Reference point, Peer SEPP, Visited-NF, and more.
- Unified flexible rule engine via LUA scripting
- Integration with Fraud Management System for unified fraud detection in multi-technologies networks (2G, 3G, 4G and 5G).
- Support for stateless application while supporting integration with stateful firewall.
- Support for indirect communication with home PLMN 5GC NFs via Service Communication Proxy (SCP).
- Throttling and overload control
- Dynamic scaling of microservices, stateless availability and performance in a fully cloud-native environment

3GPP SEPP ROAMING USE CASES

1. **Use Case 1: End-End TLS (IPX offers IP routing only)**

   The signaling information between the visited PLMN and the home PLMN, or between IPX providers, is secured end-end. In this case, the IPX providers can only provide IP routing, since the signaling message cannot be read or modified. In this scenario there is no possibility of any roaming services on transit.

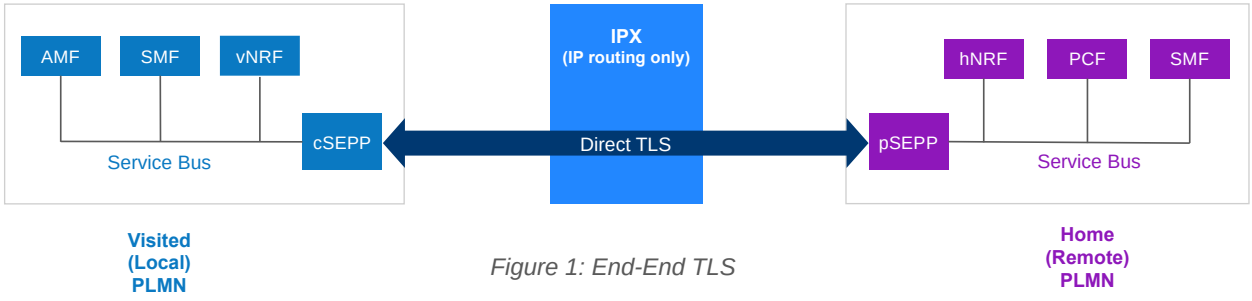

Figure 1: End-End TLS

2. **Use Case 2: Application Layer Security (PRINS)**

   In this scenario, the message is end-to-end secured at the application layer. The PRINS model allows secure modifications while providing confidentiality of sensitive

information, integrity and replay protection during 5GC signaling transport between different PLMNs.

It delivers traceability and attribution of changes to signaling information between PLMNs. The intermediaries can be IPX providers or roaming hubs.

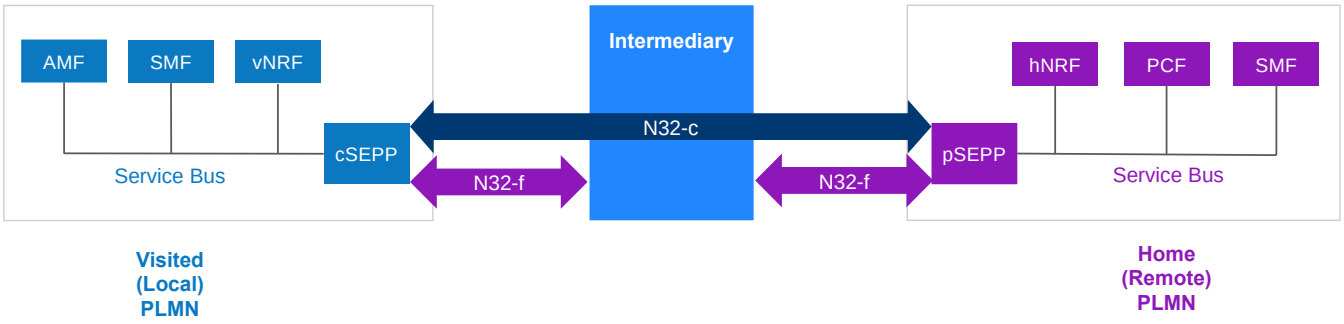

Figure 2: Application Layer Security using PRINS

CONCLUSION

Network security has been a consistent challenge for Mobile Network Operators (MNOs), primarily the roaming interfaces which are outside their control. Traditionally, the roaming interconnects have been a major source of fraud, vulnerability and attacks that steal or destroy data, or make services unavailable

On 5G networks, the internet-based HTTP/2 protocol used in the core networks is widely adopted by the internet and has been around for decades. Since hackers are well-versed with this protocol, it imperative for MNOs to deploy SEPP to address all interconnect use cases and secure the network edge to enable protection from attacks that originate outside their networks.

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

