ORACLE

Oracle Communications Security Edge Protection Proxy

Oracle Communications Security Edge Protection Proxy is a cloud native, 5G core solution that acts as a non-transparent proxy at the perimeter of the public land mobile network (PLMN) and enables a secure connection between 5G networks. The Oracle Communications SEPP ensures end-to-end confidentiality and integrity between source and destination networks for all 5G interconnect roaming messages and can be used by the following entities on a 5G network:

MNO and MVNO operators

Due to mandatory regulatory compliance in most countries' MNOs need to provide MVNOs with access to their 5G network. SEPP ensures security by not exposing NFs to the external networks.

Operator roaming hubs

Group network operator companies that reside in the same security domain can utilize SEPP to consolidate and secure operator group roaming.

IPX providers

Intermediaries enable operators to avoid entering a multitude of roaming agreements with other operators. Oracle Communications SEPP supports multitenancy enabling a large roaming coverage area.

Oracle Communications SEPP is equipped with the Global System for Mobile Communications (GSMA) recommended firewall capabilities and other security hardening measures which combine the common practices of encryption **in transit** and encryption **at rest**. The former guards against data exposure in the network, and the latter secures data from attack on storage media.

Oracle Communications SEPP certified on OCI

With Oracle Communications SEPP available to run on Oracle Cloud Infrastructure, service providers will have multiple options for deployment. While the most likely deployment of 5G core network functions will involve multiple cloud regions using true public cloud regions, there are a myriad of options to suit the preferences of each provider. Whether a split of on-premises and public cloud is the best path forward or a hybrid private and public cloud, Oracle's interoperability and options make every variation within the art of the possible.

With built-in security services and capabilities Oracle Cloud Infrastructure provides new advanced machine learning capabilities for threat management, cloud security for IaaS and SaaS, and firewall services. These capabilities further ensure that organizations can easily secure their cloud deployments and applications with simple, prescriptive services that do not require additional investment.

> "Oracle's capabilities will essentially serve as a control tower of our network core, enabling our customers to consume software on demand, facilitating the advanced core functions required to power a truly autonomous network."

Marc Rouanne
Chief Technology Officer, DISH Wireless

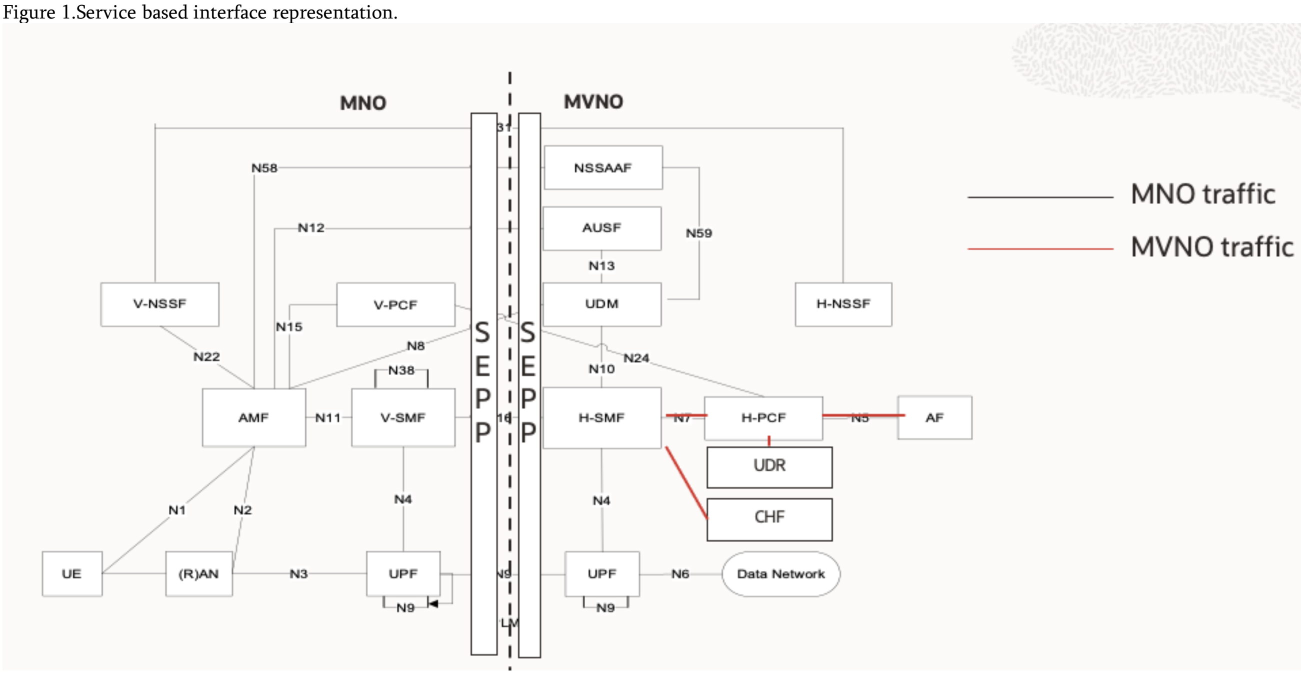
Oracle Communications SEPP in the 5G network

Oracle Communications SEPP provides end-to-end application-level security, making it impervious to read, alter, or manipulate message content without prior agreement from the Mobile Network Operators (MNO) as it traverses to other networks across multiple, external hops. Oracle Communications SEPP is akin to the Diameter Edge Agent (DEA) of 4G, which was used to provide hop by hop transport encryption using Transport Layer Security.

Oracle Communications SEPP supports interconnection between different network deployments and provides a single point of intersection reducing operational complexity and enhancing reliability in the 5G core. Oracle Communications SEPP also supports seamless integration between different affiliates of an operator, and even different deployment models, including a hosted model (Multiple PLMN).

Oracle Communications SEPP **eases operations** through automatic installation and upgrades while following the CI/CD pipeline with automated testing. It also **enhances resiliency** by protecting the network from signalling storms, using rate limiting features, and providing **advanced security** through countermeasures (as defined by **GSMA FS.36**) to prevent unauthorized access into the network.

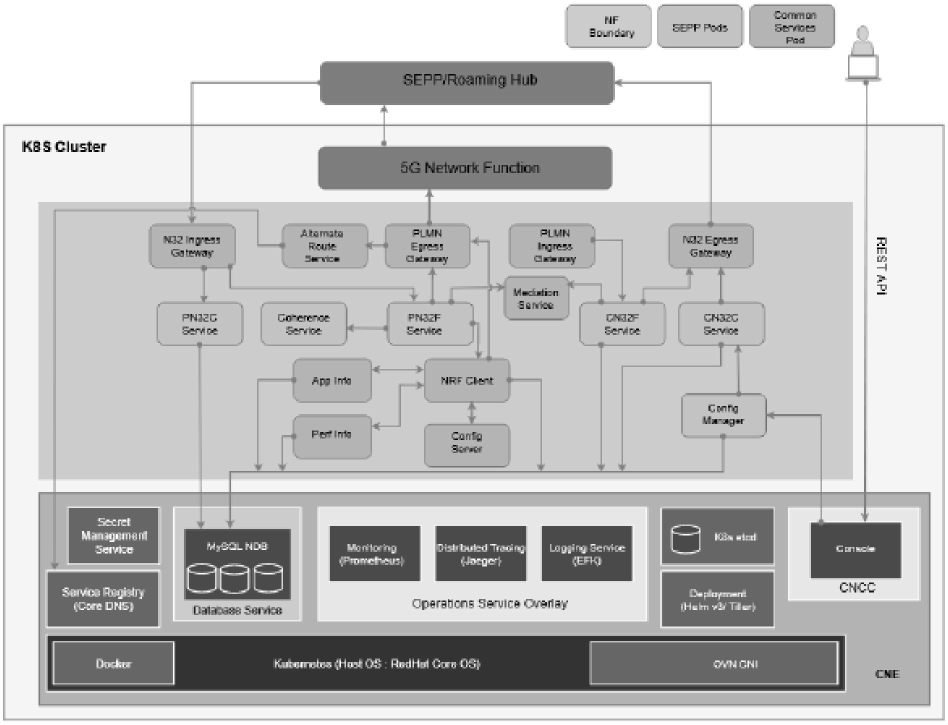
Figure 1.Service based interface representation.



Oracle Communications SEPP architecture

Oracle Communications SEPP has a three tier architecture: a connectivity tier (API gateway), a business tier (SEPP microservices), and a data tier.

Figure 2. SEPP architecture



Oracle Communications SEPP's connectivity layer is used for ingress and egress roaming partners. The solution provides two interfaces: a control plane interface, and a forwarding interface. The control plane interface goes between the Oracle Communications SEPP to introduce PLMNA and PLMNB and negotiate the security parameters to be applied. The forwarding interface communicates between the NF service consumer and the NF service producer after applying application-level security.

The business logic layer assists in mapping ingress requests to the corresponding egress route, then matching and routing the ingress request to the roaming partner, or the 5G core as required, to perform topology hiding, etc.

The data layer is responsible for storing all data and configurations required for the NFs to function.

Features and benefits

Oracle Communications SEPP is based on Cloud Native Computing Foundation (CNCF) principles. The prominent features are listed below:

Ease of operation

- Deploy onto different cloud native platforms with flexibility and scalability. This includes Oracle cloud (OCI) providing a single SLA for the product and the infrastructure.
- Supports cloud native templates and lifecycle management approaches and can be onboarded easily into a CSP's existing management and orchestration stack.
- Enables canary release through CI/CD, inspects the API version attributes of the NF service profile published by the NFs during NF registration, or update it as needed. In the event there is a new version of the API, Oracle Communications SEPP identifies the version as a canary version if the version matches the configured value. When the canary version's deployment is complete, the production version is upgraded to the canary version.
- Automation of certificate management by integration with operators PKI using CMPv2. Automation of certificate management is key for 5G as all interfaces are secured. Renewal or rejection of certificates can lead to unexpected outages. The automation of the certificate management is critical for the maintaining of SLAs.

Enhanced resiliency

- Enables alternate routing across remote SEPPs, thereby increasing the resiliency of the network.

- Ensures disaster recovery, reduces risks, and assists in times of failure of the Oracle Communications SEPP.
- Optimizes and scales resources to prevent overutilization by dedicated gateways for intra-PLMN and inter-PLMN traffic.
- Support of SBI Message Priority Header by modifying the respective headers to ensure that routing doesn't fail in the core network.
- Enhanced functionality allows routing to or from multiple PLMNs that can be associated with a particular remote Oracle Communications SEPP.
- Ingress and egress rate limiting to protect the operator network from overflooding with roaming messages coming from a roaming partner.

Advanced security

- Provides ingress rate limiting at the gateway and secures the network when aggregated ingress traffic from any registered NF instance/remote SEPP exceeds the allowed traffic rate limit. If the traffic exceeds the limit, Oracle Communications SEPP does not process the traffic and responds with an error code. Ingress global rate limiting functionality of the OCSEPP allows the user to configure the acceptable traffic rate from a consumer NF instance. Oracle Communications SEPP also enables users to configure the maximum number of incoming messages allowed during a given time period.
- Enables topology hiding and secures communication between inter-Public Land Mobile Network (PLMN) messages. Oracle Communications SEPP provides message filtering and policing on inter-PLMN control plane interfaces and topology hiding. Topology hiding secures the address of the network elements and can prevent the attacks intended for unauthorized access to network elements or interruption of the network service. Topology hiding conceals identity information from all messages leaving a PLMN.
- Supports NF authentication using TLS certificate, and supports HTTPS, which is a minimum requirement for 5G NFs as defined in 3GPP TS 33.501. HTTPS enables end-to-end encryption of messages to ensure security of data.
- Support for category 0,1 and 2 countermeasures according to GSMA FS.36

Protect traditional roaming business

- Support for outsourced SEPP
- Support for IPX providers and roaming hubs
- Consolidate and secure operator group roaming
- Integration with traditional roaming value added services; SMS Welcome, Steering of Roaming, etc.
- Traffic monitoring and integration with Oracle Data Director and other analytics solutions

Summary

The next generation network will come with a plethora of connected devices which will bring multiple security threats to the network. The edge of the network is the first point of contact to ensure robust protection against external threats. Operators need a strong partner with experience in the critical signalling areas of the network as well as cloud, and cloud native environments. Oracle Communications SEPP at the edge of 5G core complies with GSMA FS.36 security countermeasures. In addition, it provides flexibility in deployment models as expected by operators and IPX providers such as Hosted SEPP. It is going to provide flexibility in connectivity such as Protocol for N32 Interconnect Security (PRINS) though it is still being defined at 3GPP.

Starting with MNO to MVNO integrations and followed by operator groups and roaming hubs Oracle Communications SEPP has been deployed in many networks across the globe for tier 1 operators like DISH, and Orange. Oracle Communications combines 40+ years of heritage in network experience with cloud innovation to deliver highly secure, robust, and flexible cloud native 4G/5G core network solutions. For the best solutions and support, Oracle is a preferred partner that has a dual understanding of 5G core network challenges and the IT challenges that come with a cloud native infrastructure.

Related Network Functions

- Oracle Communications Cloud Native Core, Binding Support Function (BSF)
- Oracle Communications Cloud Native Core, Service Communication Proxy (SCP)
- Oracle Communications Cloud Native Core, Policy Control Function (PCF)
- Oracle Communications Cloud Native Core, Policy, and Charging Rules Function (cnPCRF)
- Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)
- Oracle Communications Cloud Native Core, Network Exposure Function (NEF)
- Oracle Communications Cloud Native Core, Network Slice and Selection Function (NSSF)

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle