ORACLE

Oracle Communications Security Edge Protection Proxy (OCSEPP)

OCSEPP is based on CNCF principles and provides end-to-end application-level security.

Oracle Communications Security Edge Protection Proxy (OCSEPP) 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 OCSEPP ensures end-to-end confidentiality and integrity between source and destination networks for all 5G interconnect roaming messages.

OCSEPP 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.

OCSEPP in the 5G network

OCSEPP 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 as it traverses to other networks across multiple, external hops. OCSEPP is akin to the Diameter Edge Agent (DEA) of 4G, which was used to provide hop by hop transport encryption using Transport Layer Security.

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

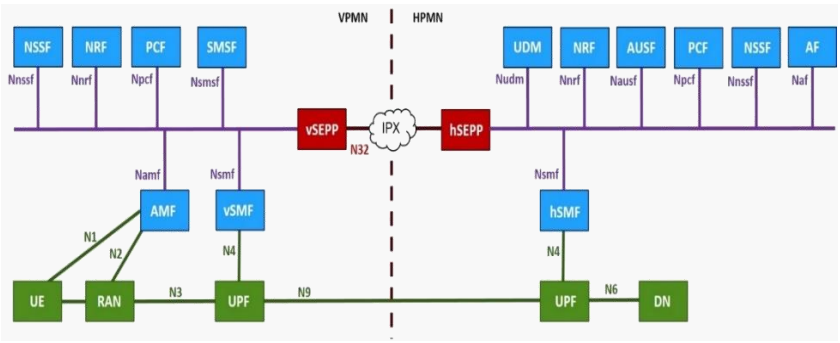

Figure 1. Service Based Interface Representation

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

Marc Rouanne
Chief Network Officer,
DISH Wireless

Key Business Benefits

- Eases the operation by providing a single point of entry into and out of the network.
- Enhances resiliency through alternate routing and disaster recovery.
- Provides advanced security to the networks by not exposing all the NFs to other external network.

OCSEPP **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 signaling storms, using rate limiting features, and providing **advanced security** through countermeasures (as defined by **GSMA' FS36**) to prevent unauthorized access into the network.

OCSEPP architecture

OCSEPP has a three-tier architecture: a connectivity tier (API gateway), a business tier (OCSEPP microservices), and a data tier.

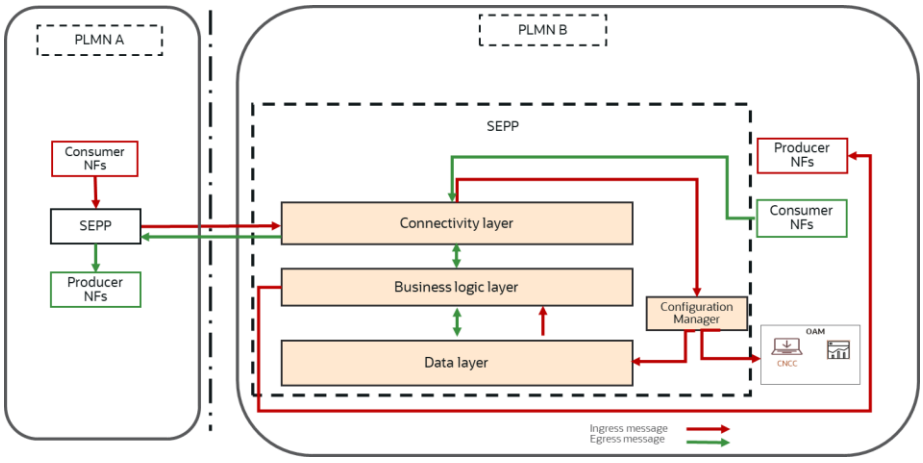

Figure 2. OCSEPP functional diagram

OCSEPP's connectivity layer is used for ingress and egress roaming partners. OCSEPP provides two interfaces: a control plane interface, and a forwarding interface. The control plane interface goes between the OCSEPPs 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

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

- **Ease of operation**
  - Route to either one or many Public Land Mobile Network ID (PLMNIDs) at the same time.

Key Features

The prominent features of OCSEPP are:

- Built in firewall capabilities as recommended by the GSMA.
- Support for different deployment models including hosted model (MULTIPLE PLMN).
- Support for Transport layer security (TLS)hop by hop, which encrypts data over Internet for in-transit and in-store messages.

Oracle Communications solutions and 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)

- Support MNO functionality by providing a single point of entry into and out of the network. Assists in being a point of interconnect to multiple networks on the core and inter-PLMN side.
- Ensures security by not exposing the NFs to the external network.
- Identifies error source by using the server header feature. The Network Function (NF) consumer can ascertain if the error is generated either by the OCSEPP or another NF.
- Supports core networks with or without Service Communications Proxy (SCP) and assists in identifying if the OCSEPP must route the message to the intended producer or just forward it to the SCP.
- Supports Domain Name System (DNS) for remote OCSEPP resolution, allows the configuration of only the Fully Qualified Domain Name (FQDN) for the far end OCSEPP, and subsequently identifies the IP address. This feature enhances flexibility for operators to use DNS instead of providing a static IP address.
- Supports registering into the Network Repository Function (NRF) and deregistering from the NRF when required. This allows for NFs to discover the OCSEPP when routing inter-PLMN traffic.
- Deploy onto different cloud native platforms with flexibility and scalability.
- Supports cloud native templates and lifecycle management approaches and can be onboarded easily into the 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, OCSEPP 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.

- **Enhanced resiliency and security**
  - 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 OCSEPP.
  - 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 OCSEPP.

- **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, OCSEPP 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. OCSEPP 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. OCSEPP 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.

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 signaling areas of the network as well as cloud, and cloud native environments. OCSEPP 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.

OCSEPP 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.

Connect with us

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