**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222804-r1***

**e-meeting, 10 - 14 October 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Trust in standalone SCP**

**Document for: Approval, Information, Discussion**

**Agenda Item: 5.24**

# 1 Decision/action requested

***Updating clause on trust to elaborate on standalone SCP.***

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

*Updating clause on trust to elaborate on standalone SCP.*

# 4 Detailed proposal

# \*\*\*\* START OF CHANGES

### 4.3.1 Trust within one PLMN

This clause describes the existing trust relationships within one PLMN.

NOTE: Whether the list of existing trust relationships described below is complete, depends on deployment choices.

NRF is the core entity handling management, discovery and authorization requests by NFs or SCP. The operator needs to apply necessary security measures to secure these operations. It is assumed that there is only one NRF, or all NRFs are within the same trust domain, i.e. all NRFs are in the same security domain and the same entity(-ies) are responsible for all NRFs.

**Registration Management:**

An NF Service Provider needs to trust the NRF that no other NF can register with the identity of NFp.

If there is no direct communication between NF and NRF, an NF Service Provider needs to trust that the SCPs forward NFp profiles unmodified.

If there is no direct communication between NF and NRF, an NF Service Provider needs to trust the SCPs that no other NF can impersonate the identity of NFp towards the SCP, i.e. tempting the SCP to register an NF with the false identity.

**Discovery:**

An NF Service Consumer needs to trust NRF to provide profiles of authenticated NF Service Providers that offer their services to the requesting consumer.

An NF Service Consumer needs to trust SCP to correctly forward the profiles of authenticated NF Service Providers that offer their services to the requesting consumer.

**Access token request:**

Trust in direct communication between NFs, NFs and SCP/SEPP, as well as SCP and SEPP is assumed per 33.501 with mandatory mutual authentication using TLS.

An NF Service Provider needs to trust NRF to provide access tokens for consumption of its services only to those NF Service Consumers that have requested for it and only for those services that are allowed by the registered NRF policy and the registered NF Service Provider policy.

Authentication and confidentiality protection in indirect communication is only achieved between NF and SCP, (potentially between multiple SCPs), SCP and NRF as well as SCP and SEPP, but additional considerations are needed for achieving trust between NFs, NF and NRF, as well as NRF and SEPP, NF and SEPP, when an SCP is on the path. This is because all traffic in indirect communication passes through SCPs, and TLS terminates at SCPs.

Thus, the SCP needs to be trusted by NFc and NFp, to only forward authentication tokens or CCA with the original request, as well as to forward information only between the legitimate endpoints of the communication.

An NF Service Provider needs to trust NRF to provide access tokens for consumption of its services only to those SCPs that are authorized by the NF Service Consumers that have requested for it and only for those services that are allowed by the registered NRF policy and the registered NF Service Provider policy.

It also needs to be distinguished if SCP is co-located to NFs (service mesh) or standalone.

For both standalone and service-mesh, the NFs sending their service requests via an SCP need to trust the SCP to which they send their service requests.

If a SCP is co-located (e.g., a side-car proxy) with a NF, trust of the NF in the SCP is implicit by its co-location. This is, because this SCP is performing many of the functionalities on behalf of the consumer, which already indicates a certain level of trust between NFs with co-located SCPs. Thus, a co-located SCP relies on trust in the SCP implementation per NF. When the SCP is implemented as a service mesh, the security solution between the side-car proxies is out of scope of 3GPP and left to the SCP implementation.

A standalone SCP is serving many NFs, not necessarily in the same infrastructure. Therefore, the standalone SCP deployment is less dependent on trust in a single implementation, but instead needs to provide for all NFs one secure implementation. Trust of many NFs in one SCP is needed.

\*\*\*\* END OF CHANGES