**3GPP TSG-SA3 Meeting #108e *draft\_S3-221847-r2***

**e-meeting, 22 - 26 August 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: trust clause – editorial update**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

A new clause on providing a general remark is proposed, shifting some text from the trust clause there. In addition, some editorial updates are proposed.

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

A *new clause on providing a general remark is proposed, shifting some text from the trust clause there. In addition, some editorial updates are proposed.*

# 4 Detailed proposal

\*\*\*\*\*\* START OF CHANGE

## 4.3 Description of the trust assumptions

### 4.3.0 General

### 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 collocated 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. 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.

### 4.3.2 Trust in Inter-PLMN communication

With 5G, a new element has been introduced to handle inter-PLMN communication. The SEPP, i.e. the Secure Edge Protection Proxy acting as perimeter of PLMN, is responsible to secure the signalling message exchange with the SEPP of another PLMN via the Internet.

The SEPP of the sending PLMN needs to trust the SEPP of the receiving PLMN that no other entity on the path has unauthorized access or can modify signalling messages if not permitted to do so by policy.

**Discovery:**

The NRF in the NF Service Consumer PLMN needs to trust the cSEPP to route the request to the pSEPP representing the target PLMN and apply the correct protection policies to the discovery request.

The NRF in the NF Service Provider PLMN needs to trust the pSEPP to authenticate the origin network of the discovery request and ensure that this origin network is correctly represented in the request arriving at the pNRF.

**Access token request:**

When requesting an access token from the NRF in another PLMN, there is always an indirect communication involving the cSEPP and pSEPP. In addition, SCPs can be involved in either network.

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

An NF Service Provider needs to trust cNRF to provide access tokens for consumption of its services only to those NF Service Consumers in another PLMN 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.

An NF Service Provider needs to trust SCP in the Service Consumer PLMN 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.

**Service request:**

An NF Service Provider needs to trust pSEPP to authenticate and verify the NFc's PLMN included in the request in order to be able to perform dynamic authorization.

A pSEPP needs to trust that the cSEPP is not forwarding requests on behalf of foreign PLMNs.

\*\*\*\*\*\* END OF CHANGE