**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222805-r1***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Extend trust in inter-PLMN communication**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

*Updating the trust clause for inter-PLMN communication.*

# 2 References

*TR 33.875*

# 3 Rationale

*Updating the trust clause for inter-PLMN communication.*

# 4 Detailed proposal

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

### 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.

Entities on the path between two SEPPs can be an IPX or roaming hub provider. A SEPP can be hosted by a third party, such as IPX or roaming hub.

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 CHANGES