**3GPP TSG-SA3 Meeting #104e** ***draft\_S3-212753-r1***

**e-meeting, 16 - 27 August 2021**

**Source: Ericsson**

**Title: Change request to living document: Credentials holder using AUSF and UDM for primary authentication**

**Document for: Approval**

**Agenda Item: 4.17**

# 1 Decision/action requested

***Approve this contribution to be included in the skeleton/living document for eNPN security normative work***

# 2 References

[1] S3-211752 "Security aspects of eNPN (skeleton for living document)"

# 3 Rationale

This document describes normative text for clause I.2.2.y "Credentials holder using AUSF and UDM for primary authentication" in the skeleton/living document for eNPN security normative work [1]. It also describes how SEPP and interconnect related security procedures apply for SNPNs using AUSF and UDM for primary authentication.

# 4 Detailed proposal

\*\*\* BEGINNING OF CHANGES \*\*\*

#### 5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP)

The SEPP shall act as a non-transparent proxy node.

The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs or SNPNs that use the N32 interface to communicate with each other.

The SEPP shall perform mutual authentication and negotiation of cipher suites with the SEPP in the roaming network.

The SEPP shall handle key management aspects that involve setting up the required cryptographic keys needed for securing messages on the N32 interface between two SEPPs.

The SEPP shall perform topology hiding by limiting the internal topology information visible to external parties.

As a reverse proxy the SEPP shall provide a single point of access and control to internal NFs.

The receiving SEPP shall be able to verify whether the sending SEPP is authorized to use the PLMN ID or SNPN ID in the received N32 message.

The SEPP shall be able to clearly differentiate between certificates used for authentication of peer SEPPs and certificates used for authentication of intermediates performing message modifications.

NOTE 1: Such a differentiation could be done e.g. by implementing separate certificate storages.

The SEPP shall discard malformed N32 signaling messages.

The sending SEPP shall reject messages received from the NF (directly or via SCP) with JSON including "encBlockIndex" (regardless of the encoding used for that JSON request).

The receiving SEPP shall reject any message in which an IPX has inserted or relocated references to encBlockIndex.

The SEPP shall implement rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signaling. This includes SEPP-to-SEPP signaling messages.

The SEPP shall implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g. FQDNs or PLMN IDs).

NOTE 2: An example for such an anti-spoofing mechanism is the following: If there is a mismatch between different layers of the message or the destination address does not belong to the SEPP’s own PLMN, the message is discarded.

The SEPP shall be able to use one or more PLMN IDs. In the situation that a PLMN is using more than one PLMN ID, this PLMN's SEPP may use the same N32-connection for all of the PLMN's PLMN IDs, with each of the PLMN's remote PLMN partners. If different PLMNs are represented by the PLMN IDs supported by a SEPP, the SEPP shall use separate N32-connections for each pair of home and visited PLMN.

\*\*\* NEXT CHANGE \*\*\*

I.2.2.y Credentials holder using AUSF and UDM for primary authentication

The 5G System architecture for SNPN with Credentials Holder using AUSF and UDM for primary authentication and authorization is described in clause 5.30.2.9.3 of TS 23.501 [2].

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the specifications in clause I.2.2.x apply.

\*\*\* NEXT CHANGE \*\*\*

I.a SEPP and interconnect related security procedures

### I.a.1 Credentials holder using AUSF and UDM for primary authentication

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, clause 5.30.2.9.3 of TS 23.501 [2] states that the UE is not considered to be roaming, however SNPN and Credentials Holder communicate via SEPPs.

The following requirements and procedures related to SEPPs and interconnect security apply for SNPNs with Credentials Holder using AUSF and UDM for primary authentication:

- Requirements for Security Edge Protection Proxy (SEPP), clause 5.9.3.2

- Protection between SEPPs, clause 13.1.2.

NOTE: IPX providers are not expected to be used between SNPN and Credentials holder using AUSF and UDM for primary authentication.

\*\*\* END OF CHANGES \*\*\*