**3GPP TSG-SA3 Meeting #108Adhoc-e S3-222587-r4**

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

**Source:**  **IDCC**

**Title:** **Key issue on** **SN Name binding for Kausf in SNPN using AAA server for primary authentication**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***It is proposed to approve the key issue described in this document. TR 33.858***

# 2 References

# 3 Rationale

It is proposed to study the issue of binding SN Name for SNPN when using AAA server for primary authentication.

# 4 Detailed proposal

\*\*\* 1st CHANGE \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[x] 3GPP TS 23.501: "System architecture for the 5G System ".

[y] 3GPP TS 33.501: " Security architecture and procedures for 5G system".

\*\*\* END OF 1st CHANGE\*\*\*

\*\*\* 2nd CHANGE \*\*\*

## 5.X Key issue #x: Binding SN Name for Kausf in SNPN using AAA server for primary authentication

### 5.X.1 Key issue details

For the existing 5GS authentication protocol, such as 5G AKA and EAP-AKA’, the serving network name is used as input for deriving Kausf after the successful authentication.

When credentials holder is using AAA server for primary authentication for eNPN with procedures defined in clause I.2.2.2 of 3GPP TS 33.501[y], the SNPN ID/SN Name are not used in key derivation of Kausf from MSK or the derivation of the MSK itself during the EAP authentication exchanges between UE and AAA. The attacker can t launch security attacks such as the one in the following scenario.

Consider the following scenario:

1. Malicious SNPN A is connected to AAA server 1.

SNPN B is connected to AAA server 1.

Malicious SNPN A broadcasts the ID of SNPN B

1. UE intends to access SNPN B, but UE connects to Malicious SNPN A
2. UE then do the authentication with AAA server 1, AAA server 1 will not authenticate the SNPN B ID
3. AUSF of Malicious SNPN A derives keys based on SNPN B ID, the UE is registered to malicious SNPN A.

### 5.X.2 Security threats

TBD

5.X.3 Potential security requirements

TBD

\*\*\* END OF 2nd CHANGE\*\*\*