**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250017-r4**

Online, Electronic meeting, 13 -16 January 2025 merger of S3-250017, S3-250102, S3-250116, S3-250160

**Source: Huawei, HiSilicon, Ericsson, Xiaomi, Nokia**

**Title: Further conclusions to KI #1.1 on authentication**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***Approve pCR proposal for TR 33.700-22***

# 2 References

[1] 3GPP TR 33.700-22

# 3 Rationale

This contribution provides conclusions to the KI#1.1 [1] to address the following Editor’s Notes:

Editor’s Note: It is ffs whether a mechanism on how ROF gets the CCF certificate needs to be specified.

Editor’s Note: The conclusion for authentication of the ROF is ffs.

Specifically,

1) TLS is used for the ROF to receive the CCF’s certificate

2) ROF authentication is left for implementation since the cerficates for the ROF may not be available in some use cases, e.g., when the ROF is representing human users or authentication methods are based on password/shared keys.

-- revision is merger with other documents

# 4 Detailed proposal

pCR

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

### 7.1.1 Conclusions for KI#1.1 CAPIF-8 reference point

Normative work is recommended to protect the CAPIF-8 reference point based on the following principles:

CCF and ROF mutually authenticate.

* The authentication of the CCF is based on TLS using the CCF’s certificate.
* The authentication of the ROF is required. Whether to specify authentication of the ROF is left to normative phase.

Editor’s Note: It is ffs how often authentication of the ROF is performed.

The TLS secure channel is used to provide messages exchanged between the ROF and the CCF with integrity protection, confidentiality protection and replay protection.

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