**3GPP TSG SA WG3 (Security) Meeting #94 ad-hoc S3-190962**

**11 – 15 March 2019, Kista (Sweden)**

**Source:** **Huawei, HiSilicon**

**Title: Discussion on NPN authentication**

**Document for: Discussion and endorsement**

**Agenda Item: 5.15**

# 1 Decision/action requested

***It is proposed to achieve a conclusion for the selection of authentication methods for standalone non-public networks.***

# 2 References

[1] 3GPP TR 23.734 v0.4.0: “Study on 5GS Enhanced support of Vertical and LAN Services.”

[2] 3GPP TR 33.819 v0.2.0: “Study on security for 5GS enhanced support of Vertical and LAN Services.”

[3] 3GPP TS 33.501 v15.3.1: “Security architecture and procedures for 5G system.”

# 3 Rationale

Non-public networks (NPN) can be deployed as standalone networks, they may be hosted by a PLMN, or they may be offered as a slice of a PLMN. SA1 requirement mentions that NPNs can use 3GPP authentication methods (EAP-AKA’ and 5G AKA) but are also allowed to use non-AKA based authentications methods such as provided by the EAP framework. However, authentication methods other than AKA based and EAP based methods can also be employed for standalone non-public networks (SNPN). The specifications do not mention which additional authentication methods shall be employed by SNPN. The aim of this discussion paper is to have a conclusion on which authentication methods shall or may be used for SNPN, should the authentication methods be mandatory or should they serve as recommended guidelines, or, is the selection of authentication methods for the SNPN not to be considered in the scope of SA3.

# 4 Detailed proposal

For the selection of authentication methods for SNPNs, we can have the following three options:

1. ~~Mandatory~~ Option A: mandate the usage of AKA based authentication methods (EAP-AKA’ of 5G AKA) or other EAP based authentications methods (as described in annex B of TS 33.501 [3]) for SNPNs.
2. ~~Recommended~~ Option B: provide recommendations for authentication methods including methods other than AKA based and EAP based authentication methods, but mandating the authentication methods is out of the scope of SA3.
3. ~~Out of scope~~ Option C: Selection of authentication methods for SNPNs is out of the scope of SA3.
4. Option D: if the SNPN does not interact with PLMN in any capacity, the selection of the authentication method is up to the operator and SA3 may provide recommendations for different deployment scenarios. If the SNPN interacts with PLMN in any capacity, authentication methods will be mandated.

The decision on which specific authentication method, e.g. EAP based or AKA based to be used for which specific deployment scenario is not in the scope of this discussion paper.

The selected option can serve as a base for further progress in this domain and the corresponding text can be added to the specifications for the guidance of operators in the NPN service deployments.

# 5 Conclusion

It is requested that SA3 endorses one of the above options.