**3GPP TSG SA WG3 (Security) Meeting #94 ad-hoc S3-190924**

**11 – 15 March 2019, Kista (Sweden)** *revision of S3-190702*

**Source:** **Huawei, Hisilicon**

**Title: Key issue on Key freshness in AKMA**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***It is requested to approve the proposal into TS 33.835.***

# 2 References

 [1] 3GPP TR 33.835 Study on authentication and key management for applications based on 3GPP credential in 5G

# 3 Rationale

A weakness of AKMA as a key agreement scheme is that there is no guarantee of freshness of the application key KAF without forcing a re-run of AKA. That is if an Application Function that requests a key from the Anchor Function, that key might have already been used. In general key freshness is a desirable property of any method used to establish keys and should be included in AKMA.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.X Key Issue #X: Application Key freshness of AKMA

5.X.1 Issue details

A weakness of AKMA as a key agreement scheme is that there is no guarantee of freshness of the application key KAF without forcing a re-run of AKA. That is if an AKMA AF that requests a key from the Anchor Function, that key might have already been used. In general key freshness is a desirable property of any method used to establish keys and should be included in AKMA.

The application key KAF is derived from the anchor key KAKMA. If KAKMA is not expired, it is complicated to refresh KAF through a run of AKA. Thus, it is better to refresh KAF without a new run of authentication.

5.X.2 Security Threats

If a KAF is used without freshness, then a weakness between UE and AKMA AF may allow an attacker to pretend to be a particular AKMA AF and obtain KAF. The attacker can masquerade as the UE towards the real AKMA AF.

5.X.3 Potential security requirements

The application key shall be refreshed without new round of authentication.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*