**3GPP TSG-SA3 Meeting #108e-AdHoc *S3-222853-r2***

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

**Source: Samsung, Intel, Apple, Deutsche Telekom**

**Title: Conclusion for key issue#2**

**Document for: Approval**

**Agenda Item: 5.1**

1 Decision/action requested

***Proposed to approve the conclusion for key issue#2 in 5GFBS TR 33.809***

2 References

Null

3 Rationale

This pCR proposes to add the conclusion for key issue#2.

4 Detailed proposal

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

7.2 Conclusions on Key Issue #2

Following conclusions are made on Key Issue #2 "Security protection of system information":

🡺 It is concluded that Digital Signatures are used for protection of system information

🡪 Signature-based solutions (#7, #11, #12, #20, #21, and #27) are taken as the basis for the normative work.

🡺 It is concluded that both Elliptic Curve-based Certificateless Signatures for Identity-based Encryption (ECCSI) [9] and Certificate based Public Key Signature Schemes are supported.

🡪 UE supports both the schemes

🡪 Network supports at least Certificate based Public Key Signature Schemes

🡪 Solutions #7 and #12 to be considered as baseline for normative work for ECCSI and Solutions #21 and #27 to be considered as baseline for normative work for Certificate based Public Key Signature Scheme

🡺 It is concluded that Elliptic Curve Digital Signature Algorithm (ECDSA) is the signature algorithm to be used

🡪 Support for further signature algorithms to be decided during normative phase

🡺 RAN WGs based on the inputs from SA3 during study phase (Rel-18) will decide details on the inclusion of the digital signature in the SI framework and broadcasting periodicity.

Following conclusions are made on the normative work timeline:

🡺 Alternative 1: Normative work for the above conclusions to be done in Rel-18.

🡺 Alternative 2: Normative work for the above conclusions to be done in Rel-19.

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