**3GPP TSG-SA3 Meeting #107Adhoc-e *S3-221370-r3***

e-meeting, 27th June – 1st July 2022

**Title: LS out on authenticity and replay protection of system information**

**Source: SA3**

**To: RAN2**

**Cc:**

**Contact person: Tao Wan**

 **t.wan@cablelabs.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** TR 33.809 v0.19.0

# 1 Overall description

SA3 is studying how to enhance 5GS to mitigate false base stations. Several Key Issues (KIs) have been identified in TR 33.809, among which is KI#2 on the authenticity and replay protection of System Information (SI). Multiple solutions of TR 33.809, e.g., #7, #20 and #27, addresses KI#2 by digitally signing SIs along with timestamps.

SA3 would like to seek comments and suggestions from RAN2 on some of the design principles. More specifically:

1. How many bytes in each of the existing SIBs can be used to carry security information (e.g., timestamp, digital signature)? A timestamp is of 4 bytes, and the length of a digital signature depends on the algorithm (please see clauses 6.20.3.13 and A.3.14 for more information).
2. Is it feasible to introduce a new SIB for carrying security information (e.g., public key) that can be requested by a UE on demand to validate the security of existing SIBs? The length of a public key or public key certificate depends on its algorithm and format (please see clauses 6.20.2.5.1, 6.27.2.1.2 and A.3.14 for more information).
3. Is it feasible to schedule a new SIB so that a UE can always acquire the new SIB when needed to validate the security of existing SIBs? If yes, please describe briefly about the scheduling of the new SIB (e.g., its periodicity).

# 2 Actions

**To : RAN2**

**ACTION:** Please kindly review TR 33.809 and provide the answers to the above questions. Any comments and suggestions that may help improve and evaluate the related solutions are welcome.

# 3 Dates of next TSG SA WG 3 meetings

SA3#108e 22 -26 August 2022 Online

SA3#108bis-e 10 -14 October 2022 Online