**3GPP TSG-SA3 Meeting #106-e *S3-220110-r1***

e-meeting, 14 – 25 February 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**](mailto:3GPPLiaison@etsi.org)

**Attachments:** TR 33.809 v0.17.0

# 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., #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 of solution #27, particularly on 6.27.2.1.6 (Delivering signatures and short-lived public keys). More specifically:

1. Is it feasible to include a timestamp (e.g., of 4 bytes) and a digital signature (e.g., of 64 bytes) in SIB1?
2. Is it feasible to introduce a new SIB for carrying a public key (and some other small amount of data) that can be requested by a UE on demand to verify the digital signature of SIB1?
3. Is it feasible to schedule a new SIB with the same periodicity of SIB1 so that a UE can always acquire the new SIB after acquiring a SIB1 to validate the SIB1?

# 2 Actions

**To : RAN2**

**ACTION:** Please kindly review solution #27 in TR 33.809 and provide the answers to the above questions. Any comments and suggestions that may help improve and evaluate the solution are welcome.

# 3 Dates of next TSG SA WG 3 meetings

SA3#106-e-Bis 4 - 8 April 2022 Online

SA3#107-Bis 27 June - 1 July 2022 TBD