**3GPP TSG-SA3 Meeting #107Adhoc-e *S3-221370-r6***

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**](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).

SA3 would like to seek feedback from RAN2 on the following questions:

1. How many bytes in each of the existing SIBs can be used to carry additional security information?
2. What are the impacts of introducing a new SIB for carrying security information that can be requested by a UE on demand to validate the security of existing SIBs? How many bytes in this new SIB can be used to carry security information at maximum?
3. What are the impacts of scheduling a new SIB so that a UE can acquire the new SIB to validate the security of existing SIBs? More specifically, what periodicity can this new SIB be broadcasted?

# 2 Actions

**To : RAN2**

**ACTION:** Please kindly provide the answers to the above questions.

# 3 Dates of next TSG SA WG 3 meetings

SA3#108e 22 -26 August 2022 Online

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