**3GPP TSG-SA3 Meeting #108Adhoc-e S3-222850-r8**

**e-Meeting, 10th – 14th October, 2022 merged S3-222475**

**Title: [Draft]Reply LS on authenticity and replay protection of system information**

**Response to: R2-2208985 / S3-222454**

**Release: Rel-18**

**Work Item: Study on 5G security enhancement against false base stations (FS\_5GFBS)**

**Source: Samsung, Deutsche Telekom, Huawei, HiSilicon, Apple, CableLabs…. [to be SA3]**

**To: RAN2**

**Cc: -**

**Contact person: Rajavelsamy R**

**rajvel@samsung.com**

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

**Attachments:** **None**

# 1 Overall description

SA3 would like to thank RAN2 for their reply LS (R2-2208985/S3-222454) on authenticity and replay protection of system information. RAN2 has asked following information from SA3 on the requirements of the security information to be broadcast:

|  |
| --- |
| RAN2 expects to evaluate solutions, evaluate impacts to RRC and related performance aspects, and settle the signaling. Therefore, RAN2 would also like to request SA3 to provide the following information on the requirements of the security information to be broadcast so that RAN2 can make a better analysis for this feature:Size of the security information or feasible ranges for the sizeLatency requirements for the delivery of the security informationHow often and for how long the new information is expected to be sentWhether all SI information or some part need to be protectedWhether the security information should be updated whenever any of the SIB contents change |

SA3 would like to provide information on the above questions as follows:

* *Size of the security information or feasible ranges for the size*

**SA3 response:**

The size of the security information is a range of values, depending on the specific security mechanisms in use. Currently SA3 is considering Digital Signature-based Schemes, in particular, Elliptic Curve-based Certificateless Signatures for Identity-based Encryption (ECCSI) and Certificate based Public Key Signature Schemes. In TR 33.809, the ECCSI scheme is used in, e.g., solution #7 and Certificate based scheme is used, e.g., in solution #20. The feasible ranges for the size of the security information are different for the two schemes. The details are as follows:

In case of ECCSI, the total length of the security information is 1036 bits.

* In case of Certificate based scheme, the size of the digital signature ranges from 260 to 2052 bit depending on the digital signature scheme in use. In addition to the digital signature, the public key certificate used to verify the digital signature needs to be transmitted, whose size ranges from 1200 bits to 4360 bits. For transmission/periodicity/reception efficiency, it should be possible to split the security information and transmit it in different SIBs of different periodicity.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Note that these values are indicative values that might be subject to change depending on the solutions/algorithms finally chosen.

* *Latency requirements for the delivery of the security information*

**SA3 response:**

Periodicity of the security information (i.e., the digital signature) used to verify the authenticity of the system information should be aligned with the periodicity of the system information. For example, at the least the security information used to verify the essential blocks (MIB and SIB1) needs to be broadcasted within 160ms (within the period), as SFN (timing information) of the MIB changes at every 160ms. Further, the time gap between the new SIB carrying the digital signature and the protected SIB should be minimized, so that UE could verify the signature of the protected SIB at the earliest.

* *How often and for how long the new information is expected to be sent*

**SA3 response:**

The security information, i.e., the digital signature used to verify the authenticity of the system information, should be sent as often as the protected system information. It is up to RAN2 to decide on the transmission repetition periodicity of the security information.

* *Whether all SI information or some part need to be protected*

**SA3 response:**

SA3 expects all system information needs to be protected (including the MIB). At the least very essential messages (MIB and SIB1) need to be protected.

* *Whether the security information should be updated whenever any of the SIB contents change*

**SA3 response:**

The security information should be updated whenever any of the contents of the protected SI (e.g., essential blocks such as MIB and SIB1) changes.

SA3 would like to inform RAN2 that, SA3 approved the following conclusions in their SA3#108 Adhoc meeting:

|  |
| --- |
| 🡺 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. 🡺 Details on the inclusion of the digital signature in the SI framework and broadcasting periodicity will be decided in discussion with RAN WGs during normative phase.  |

Further, SA3 would like to request RAN2 clarification on the following question on the UE handling of related SIB(s).

Question to RAN2: When the security information is carried in new SIB(s), i.e. the protected SIB and the new SIB (that carries the security information) are transmitted at different times, what are the UE behaviours on handing of those different SIBs? Does the UE stop the processing of the protected SIB until the new SIBs carrying the security information arrives or when the UE receives the new SIB, the UE does a post verification of the protected SIB received earlier? If the verification fails, the UE leaves the current cell and selects a new cell. If verification succeeds, UE continues in the current cell.

# 2 Actions

**To: RAN2**

**ACTION:** SA3 kindly request RAN2 to take into account the above information when evaluating the potential solutions and provide responses to the SA3 on the evaluations.

Further SA3 kindly request RAN2 to clarify the question on the UE handling of related SIB(s).

# 3 Dates of next TSG SA3 WG 3 meetings

SA3#109 14 -18 November 2022 Toulouse, France

SA3#110e 16 - 20 January 2023 Online (electronic meeting)