**3GPP TSG-SA3 Meeting #108Adhoc-e S3-222850-r4**

**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, Nokia …. [to be SA3]**

**To: RAN2**

**Cc: -**

**Contact person: Rajavelsamy R**

[**rajvel@samsung.com**](mailto:shrivastava@samsung.com)

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](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 size  Latency requirements for the delivery of the security information  How often and for how long the new information is expected to be sent  Whether all SI information or some part need to be protected  Whether the security information should be updated whenever any of the SIB contents change |

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

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

**SA3 response:**

Currently SA3 is considering two Digital Signature Schemes: 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 detailed in solution #7 and Certificate based scheme is detailed in solution #20. The feasible ranges for the size of the security information are different for both the schemes. The details are as follows:

In case of ECCSI,

* Digital Signature size is: 1032 bits
* Time Count size is : 4 bits

Please note that, for transmission/size/periodicity/reception efficiency, it should be possible to split the Digital Signature into two parts and broadcast the split parts in different SIBs. Like, part 1 of the Digital Signature (Most significant 512 bits) and Time Count in a new SIB X and part 2 of the Digital signature (Least significant 520 bits) in another new SIB Y. Part 1 changes with every change in the system information and part 2 is almost same for a cell for a longer duration (unless network wants to change).

In case of Certificate based scheme,

* Digital Signature size is : 256 to 2048 bits
* Time Count size is : 4 bits
* Digital Certificate size is: at least 1200 bits to 4360 bits

Please note that SA3 is considering system information to carry the digital certificate also, therefore to manage the size, it should be possible to broadcast the security information in different SIBs. Like, Digital Signature and Time Count in a new SIB and Digital Certificate in another new SIB, as digital signature changes with every change in the system information and Digital Certificate is almost same for a cell for a long duration (unless network wants to change).

|  |  |  |  |
| --- | --- | --- | --- |
|  | ECCSI (Solution#7) | Certificate based (Solution#20) | |
|  | SIB Carrying the Signature | SIB Carrying the Signature | SIB Carrying the Digital Certificate |
| Time Count Size | 4 bits | 4bits | 4bits |
| Digital Signature | 1032 bits | 256 – 2048 bits |  |
| Digital Certificate |  |  | 1200 – 4360 bits |
| Periodicity | 160 ms | 160 ms | 160 ms |

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

**SA3 response:**

Periodicity of the security information should be aligned with the periodicity of the essential system information (MIB and SIB1), as the UE requires to verify the authenticity of the essential blocks. In other words, at the least the security information 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 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:**

For any change in the content of MIB and/or SIB(s), it is expected to send the newly generated security information, so that UE can verify the received broadcast signalling messages. If the content of MIB and SIB(s) are not changed, then it is up to RAN2 to decide on the frequency of and period for retransmitting the signature, if needed.

* *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 and #21) are taken as the basis for the normative work.  🡪 Solution#7 to be considered as baseline for normative work.  🡺 It is concluded that Elliptic Curve-based Certificateless Signatures for Identity-based Encryption (ECCSI) [9] is used for signature generation and verification.  🡺 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 confirmation on the following SA3’s understanding on the UE handling of the security information.

When the protected SIB and the new SIB (that carries the security information) are transmitted at different times, the UE does not hold the processing of the acquired protected SIB till the verification of the security information. That is, upon acquiring the protected SIB the UE follows the legacy procedure and simultaneously the UE acquires and verifies the security information. If the verification of the security information fails then the UE aborts the ongoing legacy procedure and tries to move out of the cell. If the verification is successful, then the UE does not interrupt the ongoing legacy procedure.

# 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 confirm SA3’s understanding on the UE handling of the security information when it is provided in a new SIB.

# 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)