3GPP TSG-RAN WG2 #119-e R2-220xxxx

Online Meeting, Aug 17th – 29th, 2022

Agenda Item: 8.15

Source: Samsung

Title: [AT119-e][025][NR18] Protection of SI (Samsung)

Document for: Discussion, Decision

# Introduction

This document is to collect companies input for below offline discussion.

* [AT119-e][025][NR18] Protection of SI (Samsung)

Scope: Treat R2-2206976, R2-2207028, R2-2208460, R2-2208482, R2-2208625, Collect Comments, determine possible agreements and discussion points, progress the LS accordingly

Intended outcome: Report, Draft LS out.

Deadline: Online CB TUE W2

Deadline (for companies' feedback): Tuesday 2022-08-23 0700 UTC

Received SA3 LS and related RAN2 contributions are as follows:

1. [R2-2206976](file:///C:\Users\mtk65284\Documents\3GPP\tsg_ran\WG2_RL2\TSGR2_119-e\Docs\R2-2206976.zip) LS out on authenticity and replay protection of system information (S3-221700; contact: CableLabs) SA3 LS in To:RAN2
2. [R2-2207028](file:///C:\Users\mtk65284\Documents\3GPP\tsg_ran\WG2_RL2\TSGR2_119-e\Docs\R2-2207028.zip) Draft Reply LS on authenticity and replay protection of system information Samsung LS out Rel-18 To:SA3
3. [R2-2208460](file:///C:\Users\mtk65284\Documents\3GPP\tsg_ran\WG2_RL2\TSGR2_119-e\Docs\R2-2208460.zip) Protection of system information vivo discussion Rel-18
4. [R2-2208482](file:///C:\Users\mtk65284\Documents\3GPP\tsg_ran\WG2_RL2\TSGR2_119-e\Docs\R2-2208482.zip) Discussion on authenticity and replay protection of system information(SA3 LS) Huawei, HiSilicon discussion Rel-17 FS\_5GFBS
5. [R2-2208625](file:///C:\Users\mtk65284\Documents\3GPP\tsg_ran\WG2_RL2\TSGR2_119-e\Docs\R2-2208625.zip) Discussion on system information security Ericsson discussion Rel-18

# Contact Information

|  |  |
| --- | --- |
| Company | Contact: Name (E-mail) |
| Vodafone | [Alexey.kulakovv1@vodafone.com](mailto:Alexey.kulakovv1@vodafone.com) |
| Huawei, HiSilicon | wangrui46@huawei.com |
| Qualcomm | oozturk@qti.qualcomm.com |
| vivo | kimba@vivo.com |
| Ericsson | felipe.arrano.scharager@ericsson.com |
| Intel | Sudeep.k.palat@intel.com |
| LGE | SungHoon.jung@lge.com |
| MediaTek | nathan.tenny@mediatek.com |
| Apple | fangli\_xu@apple.com |
| Samsung | shrivastava@samsung.com |
|  |  |

# Discussion

RAN2 received a LS from SA3 [1] which concerns approach to enhance 5GS to mitigate false base stations. In the LS, SA3 has asked following questions to RAN2:

|  |
| --- |
| 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? |

Further, we discuss the relevant aspects raised in the LS and contributions submitted to RAN2#119e.

## How many bytes in existing SIBs to carry security information?

This relates to the Q1 in SA3 LS. Following are the observations from different submitted contributions:

* The maximum size of SIB is 2976 bits as specified in TS 38.331. Actual size of the existing SIB depends on the corresponding configurations and parameters, so the remaining bit varies per each SIB. Note that these SIBs are subject to further enhancements for new releases and available space should also be preserved. [2]
* Any new field addition in SIBs message to carry additional security information should comply with the maximum SIBs message size limit of 2976 bits. Reusing current removing SB(s) bits may not sufficient or adequate to carry additional security information, that may be hundreds to thousand bits, for SIB protection. [3]
* It is recommended to introduce a new SIB to carry the security related information instead of using the existing SIBs, considering the size limitation and the possible further extensions. [4]
* RAN2 is not able to answer the exact available information that can be included in each SIB for security purposes. Such task is complex and can incur in a high workload for RAN2. [5]

Based on above inputs, rapporteur understands that there is no clear answer for available bytes in each of the existing SIBs to carry additional security information. Further, existing SIBs carrying security information is not preferred considering size limitation, possible future extensions and configuration/deployment dependencies. It is proposed:

1. Respond to Q1 that the maximum size of SIB is 2976 bits. Actual size of the existing SIBs is dependent on configurations /deployments, and is also subject to further enhancements in future releases. There is no definite answer on available bytes in existing SIBs to carry security information.

Question 1: Do companies agree with the Proposal 1

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Vodafone | partiell | In my view, we should copy the text of 38.331 into the LS back as SA3 is asking about the size only in the first question:  “The physical layer imposes a limit to the maximum size a SIB can take. The maximum SIB1 or SI message size is 2976 bits.“  I think we cant say that this limit will be extended in the future, even of course possible/most likely as long max.size is considered. Not sure what is the intend to of this sentence “**Actual size of the existing SIBs is dependent on configurations /deployments, and is also subject to further enhancements in future releases.”** and how relevant is this for SA3.  **“There is no definite answer on available bytes in existing SIBs to carry security information”**:  I think we should give some examples, e.g. taking observation 1 of R2-2208482 |
| Huawei, HiSilicon | See comments | We share the similar views with Vodafone. In addition to the size limitation due to physical layer restriction, we could give SA3 some hind from RAN2 perspective whether reusing existing SIB is feasible. According to companies’ contribution, there seems a concern that the size required by SA3 solution is too big to bear in the existing SIB. |
| Qualcomm | Comments | Agree with VDF that we can quote the maximum PHY limit in the response. However, SA3 is also asking about the available size in each SIB. This is more difficult to answer. For SIB1, there is no actualy no space left since the maximum SIB1 size is well beyond the PHY limit. We can do similar exercise for other SIBs to correctly respond to the LS. From this question, it seems that SA3 is considering as one the options to add the new security information in every SIB message. |
| vivo | Partially Yes | In general, we are OK with Proposal 1. But please NOTE that 2976 bits are the size limitation due to physical layer restriction. From RAN2 perspective, SIB segmentation has been introduced since Rel-16 (e.g., for SIB12 and SIB17), it is also worthwhile mentioning the SIB segmentation case to support a lager SIB size, which would be up to 2976\*64 segments= 190464bits (23.808KBytes). Please see highlighted as below.  This information could be useful for SA3 to progress in their further work. – *SIB12* SIB12 contains NR sidelink communication/discovery configuration.  *SIB12* information element  -- ASN1START  -- TAG-SIB12-START  SIB12-r16 ::= SEQUENCE {  segmentNumber-r16 INTEGER (0..63),  segmentType-r16 ENUMERATED {notLastSegment, lastSegment},  segmentContainer-r16 OCTET STRING  } – *SIB17* SIB17 contains configurations of TRS resources for idle/inactive UEs.  ***SIB17* information element**  -- ASN1START  -- TAG-SIB17-START  SIB17-r17 ::= SEQUENCE {  segmentNumber-r17 INTEGER (0..63),  segmentType-r17 ENUMERATED {notLastSegment, lastSegment},  segmentContainer-r17 OCTET STRING  } |
| Ericsson | See comment | Agree with the intention (see answers to Q3 for completeness).   We should, however, state that the maximum size restriction is on the SI-message (*“the maximum SIB1 or SI message size is 2976 bits”*).  Additionally, we should clarify what is meant by *“further enhancements in future releases”*. We guess that in this case it is meant that a SIB’s content can evolve in the future, e.g., by adding new fields in a certain Release (?) |
| Intel | Partially | We agree about providing the max possible size but this depends on the solution chosen. Further, we should be careful about the overhead from the security information (it is not just about max SIB size!). So we suggest to add a couple of points:   1. The size available depends on the solution chosen – a separate SIB or added to existing SIB or SI. 2. The overhead from the security information should be minimised |
| LGE | Agree | The proposed answer seems to addresses both appropriately: easy question on max size and difficult one on available size of each SIB. |
| MediaTek | See comment | Citing the requirement from 38.331 makes sense as suggested by Vodafone.  We should emphasise that it is not possible for RAN2 to say how much of this maximum size is “available” for any particular SIB, because configurations can vary widely. It’s clear that in some cases, like SIB1, the existing fields can already approach or reach the size limit, so adding fields to every SIB would have functional impact, and we should indicate this in the response as well. The proposed sentence “Actual size of the existing SIBs is dependent on configurations /deployments, and is also subject to further enhancements in future releases.” is a bit general, and we would suggest something stronger, e.g.:  “Actual size of the existing SIBs/SI messages can vary widely with configurations/deployments. In some cases (including SIB1), the existing fields already allow configurations that approach or reach the PHY size limit, while other cases (SIB12, SIB17) can exceed the size limit and require segmentation. SIBs may also have additional fields added in future releases.”  We are OK with the “no definite answer on available bytes” part as it is. |
| Apple | Agree | We agree with the intention and the proposal 1 in general.  We also agree with other companies to indicate the size limitation (i.e. 2976bit) due to physical layer restriction. |
| Samsung | Yes with comments | Proposal 1 answers on the maximum size for SIB and available size of existing SIBs. There are multiple constructive comments from companies that further improves on the RAN2 response. These can be suitably incorporated to the response. |

Rapporteur’s Summary: TBD

## Impacts of introducing a new SIB for carrying security information

This relates to the Q2 in SA3 LS. Following are the observations from different submitted contributions:

* A new SIB can be introduced by the existing SI framework as defined in TS 38.331. The current SI framework is flexible, and allows both periodic transmission and on-demand transmission for each SIB. The new SIB can carry up to 2976 bits. [2]
* Impact of introducing new SIB to carry security information may be that SIB segmentation and its relative security validity resulting from SIB segmentation delay. [3]
* From RAN2 perspective, a new SIB can be introduced to carry security information, and it can be requested by a UE in the same manner as the existing on-demand SI mechanism. In this new SIB, 372 bytes can be used to carry security information at maximum. [4]
* Regarding Question 2. RAN2 can “always” introduce a new SIB depending on the purpose, the urgency, and the (specification) impact of it. Then again, and going back to what is discussed above, depending on how much information such new SIB would carry lies the amount of available space that would be needed to convey security-related information. [5]

Based on above inputs, rapporteur understands introducing a new SIB is possible for carrying security information. It is noted that there may be impacts due to SIB segmentation delay, if larger space is required. Additionally, [5] also discusses an alternative approach of providing security information in the SI message instead of new SIB. However, given the limited scope and companies view, rapporteur thinks RAN2 just responds to the question asked by SA3 and proposes:

1. Respond to Q2 that a new SIB can be introduced by the existing SI framework for carrying security information. The new SIB can carry up to 2976 bits.

Question 2: Do companies agree with the Proposal 2

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Vodafone | No | I think it would be good to re-formulate it. Existing framework of SI work include many aspects and we think we should be more precise.  “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? “  Proposal 2 VF: RAN WG2 would need to define a new SIB available on demand. The new SIB could carry up to 2976 bits.  If we like to say more, I would propose:  Proposal 2 Alt VF: RAN WG2 would need to define a new SIB available on demand. The new SIB could carry up to 2976 bits.  It is RAN WG2 understanding that proposed enhancements would not be applicable to Legacy UE. At the same time, introduction/addition of security information to existing SIBs might make it difficult to introduce/deploy new features in the future and therefore a separate SIB is preferential to reduce impact on the air interface |
| Huawei, HiSilicon | Yes with comments | We understand the intention in P2 is to confirm the feasibility of new SIB which we agree with. And the revision in Proposal 2 Alt VF looks good to us. |
| Qualcomm | No | SA3 should clarify the requirements the broadcast requirements for the new security information. How often should it be sent? How does this new information get updated? Does it depend on all the broadcasted SIBs? If so, does the new SIB need to be updated when SIBs with dynamic information, e.g. SIB9, changes? How about PWS messages? The impact of a new SIB whose content and broadcasting depends on many other or all SIBs needs more analysis. |
| vivo | Partially Yes | It would be good to clarify that 2976bits for a new SIB is only for the non-segmentation case. Moreover, this could also be part of the RAN2 impact.  Since RAN2 doesn’t see in the LS the whole SA3 solution on how to validate the security of existing SIBs, it may be too early to conclude all the RAN2 impacts are.  As above we make some rewording based on current Proposal, e.g.,  Respond to Q2 that ~~a new SIB can be introduced by the existing SI framework for carrying security information.~~ The new SIB if introduced for carrying security information can carry up to 2976 bits if the new SIB is not segmented, while 23.808KBytes depending on the number of the SIB segments. Further RAN2 impacts can be investigated in the future if needed by SA3. |
| Ericsson | See comment | While, indeed, P2 above addresses the question and we can answer that to SA3… We would like to comment on the Rapporteur’s last paragraph before capturing the proposal.  On that matter, we strongly believe that leaving aside alternative RAN2-centric approaches that could address the issue in perhaps more optimal signaling-ways, is not advisable. We have online time to discuss this.  Therefore, we cannot agree to rule out approaches that differ from those proposed by SA3, without having discussed those beforehand within RAN2. |
| Intel | Partially | We should also provide all three possible solutions – not just one – separate SIB, append to a SIB or SI. And the detailed analysis of these solutions should be in RAN2 after input from SA3 on possible size of the security information. |
| LGE | Yes with comments | The answer is fine in principle. We may need to also mention that, if SIB segmented is used for the new SIB, the size limitation can be extended. Whether the segmented SIB delivery is acceptable to SA3 is up to SA3 discussion (i.e., solution details). |
| MediaTek | See comment | We agree to indicate that RAN2 can introduce a new SIB if needed, but we should indicate the concerns raised by Qualcomm above among others. We suggest the following list of questions:   * How often is the new information expected to be sent? * How large is the new SIB expected to be? * Do SA3 envision a dependency between receiving the new SIB and applying the information from the existing SIBs? (E.g., would there be an expectation that the UE does not apply SIBx until it has verified security information for SIBx?) * How would the new SIB be updated when SI contents change (which can happen dynamically for some SIBs)? * Is the new SIB expected to contain information related to all the broadcasted SIBs? * Would the new SIB need to be broadcasted, or could it be provided only upon request from a UE?   We don’t necessarily need to ask SA3 to answer all these questions immediately, but we will need this information to properly evaluate the RAN2 impact of a hypothetical solution, and we should avoid giving the impression of a blank check by just saying “yes, we can do that”. We would suggest wording like “the feasibility of doing this depends on issues like the following”. |
| Apple | Yes | We share the rapporteur’s view that RAN2 can just respond to the question about the new SIB asked by SA3.  We are fine with proposal 2 to confirm the feasibility to introduce the new SIB for carrying the new security info. We are also fine to indicate the new SIB design should be backward compatible and the SIB segmentaton could be considered if the size of security info exceeds 2976 bits. |
| Samsung | Yes with comments | Proposal 2 answers the SA2 question based on the existing SI framework. We understand once SA3 makes some progress and reverts to RAN2 with proper requirements, RAN2 may pursue further work. It is to be noted that this is Rel-18 SI at SA3 at present, SA3 is expected to further study based on feedback from RAN2 and specify requirements and develop solutions.   * Given this, RAN2 can at best respond on the basis of the existing SI framework and awaits/pursues further work once SA3 asks with specific requirements.   Regarding alternative approaches as mentioned by E/// and Intel, it is clear that RAN2 has not discussed or studied such solutions, therefore it may not be appropriate, at this stage, to indicate new/ alternative solutions to SA3 without feasibility and in-depth analysis. For instance, there are multiple aspects which are not clear or could be of concern with the alternative solution providing security information in SI message e.g.   * MIB and SIB1 are essential system information and UE may have different requirements on other SIBs. This implies each of the SI message is not self-sufficient as security information it carries also needs to be based on MIB/SIB1 to support MIB/SIB1 authenticity verification for UEs. * MIB/SIB1 authenticity verification becomes dependant on periodicity of SI carrying UE’s desired SIBs and in some cases, when concerned SI periodicity is large, it may cause significant delays in MIB/SIB1 verification. * Each SI message has maximum size limitation of 2976 bits implying similar restriction which could happen for existing SIB(s) as in Q1 (i.e. each of the SI messages must have enough available space to carry security information)   On the other hand, as also presented in companies contributions, new SIB in the existing framework offers more flexibility in terms of scheduling and provides maximum space of 2796 bits and further expandability with segmentation.  We think suggestion from VDF is good. As MediaTek commented, RAN2 can enquire to SA3 in general for requirements. |

Rapporteur’s Summary: TBD

## What are the impacts of scheduling a new SIB?

This relates to the Q3 in SA3 LS. Following are the observations from different submitted contributions:

* The existing SI framework schedules SIBs by mapping SIB(s) to SI message(s). The new SIB can be mapped to a separate SI message or can be mapped together with other SIB(s) in an SI message. The existing SI framework supports flexible scheduling periodicities (which can be 80/160/320/640/1280/2560/5120 ms) for the SI message. A specific periodicity for an SI message carrying the new SIB can be selected by the network configuration using the existing SI framework. [2]
* Current SI-SchedulingInfo can be reused as baseline for scheduling of the new SIB carrying security information for SIBs protection.[3]
* In the reply LS to SA3, RAN2 to answer Q3 as: the current SI scheduling mechanism can be used to schedule the new SIB and the scheduling period can be 80, 160, 320, 640, 1280, 2560, 5120 ms. [4]
* Regarding Question 3. SIBs can indeed have different periodicity depending, e.g., on the use cases. But then again, the impact or the design would depend on the purpose of the information that is carried by the SIB. [5]

Based on above inputs, rapporteur proposes:

1. Respond to Q3 that new SIB for carrying security information can be scheduled with a scheduling period which can be 80, 160, 320, 640, 1280, 2560, or 5120 ms. Based on the requirement, a specific periodicity can be selected by the network configuration.

Question 3: Do companies agree with the Proposal 3

|  |  |  |
| --- | --- | --- |
| Company | Yes/No | Comments |
| Vodafone | Addition is needed | I think we should also add that new SIB might be broadcasted just for a small period of time once requested:  38.300. 7.3.2 The Other SI may be broadcast at a configurable periodicity and for a certain duration. |
| Huawei, HiSilicon | Yes | In general we are fine to the proposal. This is just to confirm what can be supported via the existing SI framework. And as Vodafone mentioned, the network can decide when to start/stop broadcasting of the SIB by implementation. |
| Qualcomm | No | As in Q2, we need to know more about the content and requirement of the new security information as well as the related UE and NW procedures. Without that, it is not possible to say that the existing SI framework is sufficient. |
| vivo | Yes |  |
| Ericsson | See comment | As commented in Q2, we are also OK to reply with what is captured in P3 to the concerning SA3 question.  However, we strongly believe that RAN2’s LS reply should allow for further development of the solution, while not blindly taking SA3’s suggested approach as the only way forward.  In this sense, we think that RAN2 could organize the LS reply as follow:   1. Answer to each question, including what is proposed by P1, P2, P3 above (as commented above, some polishing might be needed) 2. Inform SA3 of RAN2 discussions on this matter (e.g., alternative approaches, complexities, disadvantages of having the security information in a new/separate SIB, etc.) 3. Ask for further information that could later aid RAN2 decide on which is the best approach forward (e.g., SA3 expectations of needed size, latency requirements, whether all/some SIBs need to be protected, etc.) |
| Intel | Partially | Again, the response should not be just on “new SIB” and periodicity depends on the solution chosen and what is required. We can simply state that SIB periodicity can be these values and the actual periodicity can be flexible depending on the solution chosen and frequency required. |
| LGE | Yes | The answer is based on the current specification, which seems sufficient and the best we could do. |
| MediaTek | See comment | P3 is not technically wrong, but the questions from Q2 need to be answered before RAN2 can judge what periodicities might make sense. E.g., we should not endorse using a very long periodicity for a new SIB if latency-critical operations might depend on it. SA3’s question also does not appear to consider the on-demand framework (and it is mentioned only in passing in TR 33.809).  We think the proposed answer needs to be expanded, e.g.:  “A new SIB could be scheduled as part of an SI message with a scheduling period of 80, 160, 320, 640, 1280, 2560, or 5120 ms, and/or delivered to the UE on demand. The scheduling period for a SI message is selected by network implementation. RAN2 would need a more detailed understanding of the proposed designs to form a view on what scheduling configuration would be feasible.” |
| Apple | Yes | P3 is correct according to existing SI framework. |
| Samsung | Yes with comments | We understand Proposal 3 responds clearly on the scheduling periodicities and configuration flexibility for the new SIB in the existing SI framework. Addition from VDF seems fine. Point 3 as commented by E/// seems appropriate to enquire in LS.  Regarding alternative approaches as indicated in point 2 by E/// and mentioned by Intel, please refer to our comment to Q2. |

Rapporteur’s Summary: TBD

# Conclusion

Based on the discussion in section 3, we propose the following:

TBD