3GPP TSG-RAN WG2 Meeting #123 draft-R2-230XXXX

Toulouse,France, 21 August – 25 August 2023

**Agenda item:** **7.17.4**

**Source: Nokia, Nokia Shanghai Bell**

**Title: [Post123][046][feMob] subsequent CPAC security (Nokia)**

**Document for: Discussion and Decision**

# 1 Introduction

Following post-e-mail discussion was approved in RAN2-123 to further progress on RAN2 aspects of security key management for subsequent CPAC.

* [Post123][046][feMob] subsequent CPAC security (Nokia)

Scope: Converge on detailed aspects of the security solution, Identify points for agreement and discussion (preferably such that we can have clear Stage-3 CR contents next meeting and can tell SA3 whether they need to capture anything in their security Stage-2). If further questions are needed towards SA3, identify those.

Intended outcome: Report, with agreeable proposals.

Deadline: long

In this discussion, we further analyze the required changes in the RAN2 signaling procedure and relevant UE behavior to implement the proposed SA3 solution. Any further clarifications needed from SA3 on specific scenarios that were not considered in the current SA3 solution are also discussed.

# 2 Contact Information

|  |  |
| --- | --- |
| Company | Email address |
| OPPO | youxin@oppo.com |
| Lenovo | [pmallick@lenovo.com](mailto:pmallick@lenovo.com) |
| ZTE | zhang.mengjie@zte.com.cn |
|  |  |
|  |  |
|  |  |

# 3 Discussion

In current specifications, the security keys used for integrity protection and SCG bearers are generated from the master key (KgNB) and SK counter assigned by MN as part of the RRC Reconfiguration message. For every PSCell-change that involves a change of PDCP anchor point (Security anchor point), MN is expected to provide a new SK counter value. In order to avoid security re-keying issues within active connection the MN needs to ensure that SK counter values are not re-used across successive PSCell changes.

As part of the Rel-18 subsequent CPAC feature, the UE is preconfigured with multiple candidate PSCell configurations along with execution conditions. With this pre-configuration, the UE can execute subsequent PSCell changes without any RRC Reconfiguration message after the cell change. As the SK counter values for S-CPAC need to be pre-configured new solution is needed for SK counter change during PSCell-change that involves (security anchor point change (Inter-SN change). In this regard, SA3 has proposed a solution for SK counter management for the S-CPAC scenario. The solution proposes

* Pre-configuration of the list of SK counters for each SN at UE.
* UE is expected to use unused SK counter values from this list during Inter-SN mobility.

RAN2 has agreed to support the above solution in RAN2 signaling procedures.

## 3.1 Basic Signalling Procedure

**K-SN (S-KgNB) generation for Inter-SN S-CPAC**

Following is the rapporteur's understanding of SK counter selection and K-SN generation during subsequent CPAC as per the proposed solution from SA3. (From UE perspective). This forms the basis for further questions related to defining the RRC signalling aspects.

* A list of SK counter values per security anchor point(i.e SN ) is provided toward the UE when subsequent CPAC is configured with candidate cells belonging to different security anchor points.
* To enable the UE to identify changes of the security anchor point, each candidate configuration is assigned with group ID that points to the specific security anchor point. In other words, the each SK-counter list configured to UE includes Group ID. This group ID is referred in each of the candidate cells that uses the same SK-counter-list.
* During subsequent CPAC, if the UE identifies that the target cell belongs to a different Group-ID than the serving cell , UE selects the first unused entry in the SK-counter list that corresponds to this group-ID. K-SN and subsequent security keys are generated based on this selected SK-counter. The SK-counter is marked as used within the list.

**Q1 : Do companies agree to the above understanding on UE behaviour for SK-counter selection during subsequent CPAC? If not indicate the difference for specific steps.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Answer (Yes/No)** | **Additional comments** |
| OPPO | Yes |  |
| Lenovo | Yes | If the UE identifies that the target cell belongs to same (as serving) SCG (group id), then no security update is required. For DRBs using RLC AM mode PDCP data recovery applies, and for DRBs using RLC UM no action is performed in PDCP. These are done by the UE on its own i.e., without explicit signalling. |
| ZTE | Yes, but | For the third bullet, we think the UE can remove the selected SK-counter from the corresponding SK-counter list after generation of K-SN and subsequent security keys, considering that the used SK-counter is invalid and shall not be used any more. Then the UE is not required to mark/record which SK-counter is used, and can always select the first SK-counter in the corresponding list upon subsequent CPAC execution. |

**Signaling Procedure changes for Inter-SN S-CPAC**

For the above solution, the RRC Reconfiguration message that provides configuration for S-CPAC includes new information element that consists of multiple lists of SK-counters with each list assigned with Group ID. This information element is to be maintained across cell changes. So it is preferred to maintain this information outside the candidate configuration. Each candidate configuration also needs to have a new parameter to indicate its Group ID. As it is MN which is responsible for assigning SK-counter-list and group-ID, this parameter can be a parameter outside the RRC-configuration within the candidate-configuration. Based on the above we propose the following changes to RRC Reconfiguration message.

**Q2. Do companies agree to introduce the following changes in RRC-Reconfiguration**

1. **List of Group-ID and associated SK-Counter list in the RRC Reconfiguration as parameter outside candidate configuration.**
2. **Each candidate configuration includes the Group ID outside the RRC Configuration.**
3. **UE maintains new variable for SCPAC-SK-Counter-list which includes list of counters and index to last used SK-counter value. This variable is maintained until all the S-CPAC configurations are maintained.**

**If not, companies can indicate alternative signaling solutions and the advantages of the same.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Answer (Yes/No)** | **Additional comments** |
| OPPO | See comments | 1. For the first bullet, we agree the “List of Group-ID and associated SK-Counter list” is provided outside candidate configuration since it is provided per SN. While it should be contained in the same message that provides subsequent CPAC configuration, i.e. within *ConditionalReconfiguration.* 2. Suggest to modify the second bullet as following to be more precise:   *“Each candidate configuration includes the Group ID outside the condRRCReconfig includes RRCReconfiguration.”*   1. We see no need to introduce new UE variable for SCPAC-SK-Counter-list configuration maintenance. As the SK counters will always be maintained/released along with subsequent CPAC configuration, single UE variable(i.e. *VarConditionalReconfig)* is sufficient to maintain the SK counter configuration as well as other subsequent CPAC configuration.   Furthermore, we wonder what does ”index to last used SK-counter value” mean. Upon inter-SN PScell change, the used SK-counter should be considered as invalid with no additional spec impact. |
| Lenovo | Yes and… | 1. The last-used-index is incremented monotonically by 1 for inter-SN cases only. The counters in the SK-Counter list for the same group may be contiguous (e.g., 5, 6, 7…) but need not be (e.g., 5, 12, 20…) up to the network. 2. The counter values in two different SK-Counter lists for two different groups must be unique i.e., same counter values can’t be used in two SK-Counter lists. |
| ZTE | See comments | For the first and second bullets, we share the same view with OPPO.  For the third bullet, we also think the existing UE variable VarConditionalReconfig can be used to maintain the subsequent CPAC configuration, including SCPAC-SK-Counter-list, i.e. no need to introduce separate UE variables.  Besides, it seems no need to introduce the index to last used SK-counter value, if the UE removes the selected SK-counter from the corresponding SK-counter list each time after generation of K-SN and subsequent security keys. Please see our comments in Q1. |

As the UE is expected to select the next free available SK counter from the list of SK counters in orderly manner, the new SK counter value selected after the Inter-SN change can also be known to MN implicitly. In this case explicit signalling of selected SK counter to MN after the CPAC execution is not mandatory. It may be needed in some specific scenarios where there may be chances for mis-synchronization of the selected counter. There are different views expressed on the indication of selected SK counter value to MN on SCPAC execution.

**Q3: On execution of target configuration that changes SK counter value,**

1. **Do companies see need for including the selected SK counter value in RRC-Reconfiguration-complete considering the possibility that NW is aware of the selected SK counter value based on the defined UE behaviour?**
2. **If yes, please indicate the scenarios where such indication will be required.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Answer (Yes/No)** | **Additional comments** |
| OPPO | See comments | In SA3 draftCR, they provide three options on the security info interaction among MN and SN as well as the corresponding interaction between UE and MN:  *Option 1: The MN derives the corresponding KSN as described in Annex A.16 based on the corresponding SN Counter values. The KSN keys and the corresponding SN Counter values are sent to the SN from the MN. The SN shall store the KSN keys and the corresponding SN Counter values in its security context.*  *Option 2: After the derivation of sequence of multiple distinct SN Counter values for each candidate SN, the SN Counter values are sent to the UE from the MN. The MN does not need to store the SN Counter values for each SNs after sending them.*  *Option 3: The MN derives the corresponding KSN as described in Annex A.16 based on the corresponding SN Counters values. The KSN keys are sent to the SN from the MN. The SN shall store the KSN keys in its security context.*  *Corresponding to the Option 1 in 6.10.2.X.1: The UE shall inform the MN which SN Counter value it used for KSN derivation when accessing the SCG of the target SN. The MN signals the received SN Counter value to the SN. The SN decides the KSN based on the received SN Counter value.*  *Corresponding to the Option 2 in 6.10.2.X.1 [Alt 1]: When the UE accesses an SCG of a target SN, the MN receives the SN Counter value from the UE. The MN derives KSN using the received SN Counter value. The KSN is sent to the target SN from the MN.*  *Corresponding to the Option 2 in 6.10.2.X.1 [Alt 2]: When the UE accesses an SCG of a target SN, the target SN receives the SN Counter value from the UE. The target SN uses the SN Counter value to request the Ksn derivation from MN.*  *Corresponding to the Option 3 in 6.10.2.X.1: The SN chooses the first unused Ksn key for that UE to establish the security with the UE.*  We understand whether UE shall indicate the selected SK counter rely on which option is selected by SA3. For option 1 and option2, including the selected SK counter in RRC reconfiguration complete message is required. While for option3, target SN may choose the unused Ksn with pre-defined order without the explicit indication from UE/MN. |
| Lenovo | Both alternatives work | Yes (**including the selected SK counter value in RRC-Reconfiguration-complete**): UE provides *next unused* SK-Counter in a **secured** RRC Reconfiguration complete message to the MN. MN generates S-KgNB and provides this to target SN, along with the SN Change complete from the UE. This does not require the MN or SN to remember the SK-Counter sequence/ list.  No (**not including the selected SK counter value in RRC-Reconfiguration-complete**): Since when the execution conditionof one (subsequent) candidate PSCell is satisfied, the UE applies *RRCReconfiguration\** message corresponding to the selected candidate PSCell, and sends an *RRCReconfigurationComplete\** message, including an *RRCReconfigurationComplete\*\** message for the selected candidate PSCell, and information enabling the MN to identify the SN of the selected candidate PSCell…MN can track UE’s movement and should be in a position to determine UE’s SK-Counter to be used for the target PSCell. Here, the MN need not remember the entire history but only the “last” occurrence of the UE in each candidate SN.  We do not see any security issue or race condition/ de-Sync between the UE and the MN/ SN from this aspect. |
| ZTE | No | In our understanding, the SK-counter list is provided by the MN, so the MN can maintain the SK-counter list corresponding to each candidate SN and perform the same handling for the SK-counter selection as the UE (i.e. select the first entry in the list and remove the used SK-counter after generation of the SN key) when knowing the target candidate SN selected by the UE. And then the MN can transfer the generated SN key to the target candidate SN.  Thus, the MN is only required to know which candidate SN is selected by the UE, which has been implemented by including the selected candidate PSCell information (i.e. condReconfigId) in the RRCReconfigurationComplete message to the MN upon CPAC execution. So there is no need to explicitly indicate the selected SK counter value to the NW. And no mis-synchronization will be caused if the MN and the UE handle the selected SK-counter with the same behaviour. |

Depending on the usage of the SK-counter list for a given SN, MN can update the SK-counter list for specific SN via a dedicated RRC signaling message that can update the SK-counter list. It is possible to include additional counter entries via update operation or the complete list can be replaced whenever MN intends to update the list.

## 3.2 Additional Scenarios

RAN2 has agreed that the SCPAC configurations are maintained at UE during Pcell-change /PSCell change and SCG release scenarios unless explicitly specified by NW to release the SK-Counter list. In such scenarios, the SK-counter list along with the current information of unused counters per SN also needs to be maintained UE in similar manner. However, in this case there could be some security concerns for each of the scenarios. Hence RAN2 needs to conclude on the UE behaviour on these scenarios.

**Q4. For Pcell-change /PSCell-change /SCG Release scenarios, if the SCPAC configuration is maintained what is the expected UE behavior on maintaining the SK-counter list.**

1. **UE maintains the current status of the SK-counter list along with used counter status corresponding to the maintained configuration.**
2. **UE releases the SK-counter list by default. If the SCPAC is maintained, NW is expected to provide new SK-counter list to be used after the RRC Reconfiguration in these scenarios.**
3. **Indicate the scenario to SA3 and ask SA3 opinion for any preferred UE action.**
4. **Other Means.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Option** | **Additional comments** |
| OPPO | Option A | The SK-counter list should follow the same behaviour as SCPAC configuration, i.e. rely on NW on release/maintenance/modification. |
| Lenovo | Option A | Seems to work. |
| ZTE | Option A, but | For option A, we think the UE just needs to maintain the current status of the SK-counter list, no need to record the used counter status (see our comments in Q1/2). |

------------------------------------------------------------------------------------------------------------------------------------------------

It is possible that conditional configurations provided to UE may include some configurations which are not to be maintained for SCPAC. For these candidate configurations when MN provides explicit SK counter value, it is possible to assign uniquely different value from the SK-counter-list given to SCPAC OR it can be one of values assigned for SCPAC. Because the UE is expected to release SCPAC when UE execute these normal CPAC or CHO configurations. To decide on specific NW and UE behaviour for this scenario following discussion will be beneficial.

**Q5. Should the SK-counter lists configured for SCPAC purpose and explicit SK-counter configured for Rel-17 CPAC be uniquely different?**

|  |  |  |
| --- | --- | --- |
| **Company** | **Answer (Yes/No)** | **Additional comments** |
| OPPO | Yes | According to current agreements, the SCPAC configuration may be maintained if NW does not explicitly indicate UE to release upon the execution of normal CPAC or CHO. To avoid frequently RRC reconfiguration of SK counter list after CPAC or CHO, uniquely different values should be assigned for the SK-counter-list given to SCPAC. |
| Lenovo | Yes | This is anyway in network’s implementation and unique values (like a SK-counter value not included in any SK-counter-list) can save any potential rekeying issues. This way UE implementation can be simplified. |
| ZTE | Yes | We think it can be up to the NW implementation to ensure unique SK-counter value(s) is provided for each conditional configuration. |

**------------------------------------------------------------------------------------------------------------------------------------------------**

RAN2 is yet to conclude on the failure scenarios related to subsequent CPAC changes as PS-Cell change failure and S-RLF scenario. In such cases depending on the specified UE behaviour there can be additional impacts related to SK-counter management. In the rapporteur view impact to SK-counter management for failure scenario can be revisited once RAN2 concludes on the same. If companies think some failure scenarios require early attention for SK-counter management, it can be indicated here.

**Q6. Do companies think some additional changes or issues to be addressed related to SK-counter management for failure scenarios (S-RLF and SCG-change failure) ? If yes, the issues can be captured here.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Answer (Yes/No)** | **Additional comments** |
| OPPO |  | This can be discussed after we have progress on failure cases. |
| ZTE |  | This can be discussed later after we conclude on failure cases. |

------------------------------------------------------------------------------------------------------------------------------------------------

If any specific scenario /issue not handled in the above list of questions can be provided as part of the below question.

**Q7. Any additional issues /scenarios impacted due to subsequent CPAC for security key management and specific comments for the same.**

|  |  |  |
| --- | --- | --- |
| **Company** | **Answer (Yes/No)** | **Additional comments** |
|  |  |  |

# 4 Conclusion