**3GPP TSG-RAN WG2 Meeting #123bis R2-230xxxx**

**Xiamen, China, 9th – 13th October 2023**

**Title: [**DRAFT] Reply LS on security for selective SCG activation

**Response to:** R2-2307070 / S3-233200

**Release:** Rel-18

**Work Item:** NR\_mob\_enh2-Core

**Source:** Nokia (to be RAN2)

**To:** SA3

**Cc: [**RAN3]

**Contact Person:**

Name: Srinivasan Selvaganapathy

E-mail Address: srinivasan.selvaganapathy@nokia.com

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

**Attachments:** None

**1. Overall Description:**

RAN2 would like to thank SA3 on LS which provides the solution details for security key change for selective activation. RAN2 has provided the first LS Reply with initial RAN2 agreements on the signing procedure in [1].

RAN2 has further discussed on the RAN2 signaling aspects for the above solution and made the following agreements.

|  |
| --- |
| * Rel-18 Conditional-Reconfiguration Information element may include
* List of Group-ID (mapping to SN) and associated SK-counter values outside the candidate conditional configurations.
* The Group-ID parameter is included within each candidate conditional configuration(CondConfigAddMod) marked for subsequent CPAC.
* UE include the selected SK-counter value in the MN RRC Reconfiguration Complete message when UE selects new SK-counter value as part of S-CPAC execution.
	+ RAN2 intend to further discuss the action at MN when it identifies the mismatch between the selected SK-counter at UE and the SK-counter selected by MN for the current CPAC execution.
* For Pcell-change /PSCell-change /SCG Release scenarios, if the SCPAC configuration is maintained, UE also maintains the unused SK-counter values.
* RAN2 Understanding: The NW configuration ensures that The SK-counter lists assigned for SCPAC configurations and the SK-counter value assigned for CPAC configurations are uniquely different. No specification changes are needed in this regard.
* No specification changes needed for UE behaviour for the Scenario where free SK-Counter not available at the time of execution. This scenario can be avoided by NW configuration.
 |

RAN2 assumes that the MN also provides to the SN the list of SN keys associated with the sk-counter values provided to the UE, so that the SN can select the first unused SN key to process the UE uplink transmission without waiting for the RRC Reconfiguration Complete message sent to the MN.

The only reason for the UE to provide the selected sk-counter value to the MN in the RRC Reconfiguration Complete message is to allow the network to detect a key mismatch. While RAN2 did not identify any scenario where a key mismatch could occur, RAN2 understands that there is no existing way to detect a key mismatch e.g. when SRB3 and user plane integrity protection are not used.

RAN2 kindly request SA3 to consider the above RAN2 agreements for further SA3 work for the above solution. RAN2 also kindly request SA3 to provide feedback on the actions required at MN in case of mismatch in the selected SK-counter at UE and NW is identified.

**2. Actions:**

**To SA3 group.**

**ACTION:** RAN2 kindly asks SA3 to take the above information into account.

 **3. Date of Next TSG-RAN2 Meetings:**

3GPP TSG RAN WG2#124 13-17 November 2023 Chicago, US

**4. Reference**

[1] R2-2309246R2-Reply LS on security for selective SCG activation