**3GPP TSG-SA3 Meeting #XXX S3-22XXXX**

**Berlin, Germany, 22nd – 26th** **April, 2023**

**Source: OPPO**

**Title: Discussion on security for selective SCG activation**

**Document for: Discussion and agreement**

**Agenda Item: 3**

# 1 Decision/action requested

***This paper discusses security for selective SCG activation.***

# 2 References

[1] 3GPP TS 37.340.

[2] 3GPP TS 33.501

[3] S3-231397

[4] S3-230618

# 3 Rationale

For the selective SCG activation, RAN2 and SA3 have exchanged LSs to discuss the security issue, in which the detail still needs to be discussed.

# 4 Discussion

**4.1 Existing CPAC procedure.**

In Rel-18, the selective activation of the cell groups is introduced to support consecutive CPA/CPC procedure to avoid frequently RRC reconfiguration. The UE is configured with several conditional reconfigurations, each with a different candidate PSCell, and based on the evaluation on the execution conditions of candidate PSCells, the UE selects and executes one of these conditional reconfigurations.

As specified in TS 37.340[1], which is defined as a PSCell addition/ change that is executed by the UE when execution condition(s) is met. The existing secondary node addition and change as specified in clause 10.2 and 10.5 of TS 37.340[1] can be used for CPAC configuration and execution. The following figure depicts the existing Conditional Secondary Node Addition procedure which give an example for CPAC configuration and execution.



1. The MN decides to configure CPA for the UE. The MN requests the candidate SN(s) to allocate resources for one or more specific PDU Sessions/QoS Flows, indicating QoS Flows characteristics (QoS Flow Level QoS parameters, PDU session level TNL address information, and PDU session level Network Slice info), indicating that the request is for CPA and providing the upper limit for the number of PSCells that can be prepared by the candidate SN. In NR-DC, the MN always provides all the needed security information to the candidate SN (even if no SN terminated bearers are setup) to enable SRB3 to be setup based on SN decision.

**Observation 1. In legacy CPAC, the sk\_counter associated to each candidate SN is provided to the UE along with CPAC configuration.**

**Observation 2. In NR-DC, the MN always provides all the needed security information to the candidate SN.**

**4.2 Security mechanisms for DC.**

The security mechanisms and procedures for DC is specified in TS 33.501 [2], the MN generates the security key KSN for the SN and sends it to the SN over the Xn-C interface. In order to make KSN aligned between UE and SN, the value of SN counter should be sent to UE over RRC signalling for the derivation of KSN at UE side, i.e., SN Counter in RRCReconfiguration message.

|  |
| --- |
| 6.10.3.1 SN Counter maintenance  The MN shall maintain a 16-bit counter, SN Counter, in its AS security context. The SN Counter is used when computing the KSN.  The MN maintains the value of the counter SN Counter for a duration of the current 5G AS security context between UE and MN. The UE does not need to maintain the SN Counter after it has computed the KSN since the MN provides the UE with the current SN Counter value when the UE needs to compute a new KSN.  The SN Counter is a fresh input to KSN derivation. That is, the UE assumes that the MN provides a fresh SN Counter each time and does not need to verify the freshness of the SN Counter.  NOTE: An attacker cannot, over the air modify the SN Counter and force re-use of the same SN Counter. The reason for this is that the SN Counter is delivered over the RRC connection between the MN and the UE, and this connection is both integrity protected and protected from replay.  The MN shall set the SN Counter to ‘0’ when a new AS root key, KNG-RAN, in the associated 5G AS security context is established. The MN shall set the SN Counter to ‘1’ after the first calculated KSN, and monotonically increment it for each additional calculated KSN. The SN Counter value '0' is used to calculate the first KSN.  If the MN decides to release the offloaded connections to the SN and later decides to re-start the offloading to the same SN, the SN Counter value shall keep increasing, thus keeping the computed KSN fresh.  The MN shall refresh the root key of the 5G AS security context associated with the SN Counter before the SN Counter wraps around. Refreshing the root key is done using intra cell handover as described in subclause 6.7.3.3 of the present document. When the root key is refreshed, the SN Counter is reset to '0' as defined above. |

**Observation 3. The SN Counter is maintained by MN, and monotonically increment it for each additional calculated KSN. There is no need for the UE to maintain the SN Counter.**

**Observation 4. The SN Counter is start from “0”, and monotonically increment for each additional calculated KSN.**

**4.3 Two scenarios for SCG selective activation**

According the coming LS [3] from RAN2, the following two scenarios of SCG selective activation can be supported：

* **Scenario 1:** **Inter-SN SCG selective activation**

For the Inter-SN SCG selective activation, the UE connects to candidate cell 1 of the SN#1 before and after being connected to another SN. As discussed and agreed in the outgoing LS [4] to RAN2, the same S-KgNB shall not be used.

* **Scenario 2:** **Intra-SN SCG selective activation**

For the Intra-SN SCG selective activation, the UE moves from different PScells controlled by the same SN. This scenario without the PDCP anchor changes, the intra-gNB handover as specified in clause 6.9.2.3.1 of TS 33.501 can be used, and the KgNB can be retained.

**Observation 5. For inter-SN** **SCG selective activation, the KSN shall be updated.**

**4.4 Conclusion**

In conclusion, the existing way can be followed for SCG selective activation, i.e.

**Proposal 1: The MN preconfigures SN Counter for each candidate PSCell.**

**Proposal 2: Based on execution conditions evaluation for candidate PSCell, the UE selects and executes one of these conditional reconfigurations, and generates KSN of corresponding candidate PSCell when executes CPAC procedure for Inter-SN SCG selective activation.**

The candidate solutions are listed below:

* **Alternative 1. Single** **SN Counter value per candidate PScell is pre-configured**

In this case, the UE should consider the candidate(s) configuration as invalid when the associated SN Counter value has been applied, especially for the case that UE connect to candidate cell 1 of the SN#1 before and after being connected to another SN.

After the candidate(s) configuration been considered as invalid, whether UE should release the corresponding candidate configuration is FFS. If the MN intends to keep the candidate cell for subsequent SCG selective activation, reconfiguration of the SN Counter for this candidate is required for inter-SN case accordingly. These above questions should be left to RAN2 to design.

* **Alternative 2.** **Multiple SN Counter values per candidate PScell are pre-configured;**

There are two configuration methods for multiple SN Counter values:

1. The MN provides an initial value of SN Counter and the specific scope (optional) to the UE, and UE monotonically increment it for each additional calculated KSN. The current usage of the SN Counter can be retained as mentioned in 4.2. The UE should also maintain this counter as the MN.
2. The MN provides multiple specific SN Counter values to the UE. When the inter-SN SCG selective activation occurs, the unused SN Counter can be applied to generate new KSN.

With multiple pre-configured SN Counter values, there may be one potential issue on **out-of-sync utilization SN Counter for KSN generation between UE and MN, in which the KSN is applied by UE and the target SN.**

To address the potential issue, (1) optimizations on pre-defining SN Counter utilization order, or (2) explicitly indication of selected SN Counter from UE to MN and MN to SN may be required.

With the UE movement, the relationship (i.e., inter-SN and intra-SN) between source PSCell and target PSCell is unfixed. Considering UE has no knowledge of CU/DU deployment, and the UE movement cannot be predicted, inclusion of the inter-SN or intra-SN indication in candidate cell configuration is necessary. The inclusion of the inter-SN or intra-SN indication in candidate cell configuration should be left to RAN2 to further design.

# 5 Proposal for endorsement

Based on the observations detailed above, it is proposed to follow the existing way as much as possible to reduce the impact.

**Proposal 1: The MN preconfigures SN Counter for each candidate PSCell.**

**Proposal 2: Based on execution conditions evaluation for candidate PSCell, the UE selects and executes one of these conditional reconfigurations, and generates KSN of corresponding candidate PSCell when executes CPAC procedure for Inter-SN SCG selective activation**

According to these potential solutions listed, we propose to apply the **Alternative 1(Single SN Counter value per candidate PScell is pre-configured)**, which will bring as less impact as possible, meanwhile the security requirement raised in the outgoing LS [4] can be met.