**3GPP TSG-SA3 Meeting #116 *draft\_S3-242386-r1***

Jeju, South Korea, 20th - 24th May 2024 was S3-241999

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **1** | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Editorial and clarificaiton of SCPAC | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2024-05-13 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | This contribution gives editorial changes and clarifications to SCPAC feature. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This contribution gives editorial changes and clarifications to SCPAC feature. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | some places are not capable to convey the original meaning of the mechanism. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.10.2.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **N** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **N** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **N** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*START OF 1st CHANGE\*\*\*

#### 6.10.2.4 Security mechanism and procedures for SCPAC

##### 6.10.2.4.1 General

In subsequent CPAC (SCPAC), the MN may provide one or several candidate SCG configuration(s) for one or multiple candidate SN(s) to the UE. The UE may select and execute precisely one of these conditional reconfigurations to change PSCell based on the measurement results on candidate target PSCells. The conditional reconfiguration for the selected PScell remains valid after the UE selects the target and executes the target cell access procedure. Thus, the UE can connect to the same SN several times without any further reconfiguration by the network.

##### 6.10.2.4.2 Security context initialization for selective SCPAC

To prevent key-stream reuse when the UE switches back and forth to the same PSCell or SN, the MN shall assign a sequence of distinct SN Counter values (maintained for dual connectivity detailed in clause 6.10.3.1 of this document) per candidate SN during the SCPAC procedure. The same SN Counter as used for DC shall be used to generate the keys also for SCPAC and the MN shall ensure that no generated SN Counter value will accidentally be used to derive a KSN more than once. Each SN Counter value is unique, and the sequences (i.e. sequences of SN Counter values of candidate SNs) are non-overlapping. These sequences shall be provided to the UE by the MN. The UE shall store these sequences.

The MN shall derive the KSN keys corresponding to the SN Counter values from the KgNB of the UE as described in Annex A.16. The MN shall send the KSN keys associated with the SN together with their corresponding SN Counter values to that SN in the SN Addition Request. The SN shall store the received KSN keys and the SN Counter values of the UE. The MN shall maintain the largest assigned SN Counter value and monotonically increment it either for the next KSN calculation for DC as described in clause 6.10.3.1 of this document or for further assignment for the SCPAC detailed in this clause.

When a new AS root key, KgNB, in the associated 5G AS security context of the UE is established, and the SN Counter is set to ‘0’ as specified in clause 6.10.3.1, the MN derives a new sequence of distinct SN Counter values per candidate SN and sends these to the UE in the same RRC Reconfiguration as the one that activates the new KgNB. The UE shall delete the stored SN Counter value sequences and store the received new SN Counter values. Further, the MN derives the corresponding KSN for each target SN, and the derived KSN keys and the corresponding SN Counter values are sent to the SN from the MN. Each SN shall delete the stored KSNs and corresponding SN Counter values and store the received new KSNs and the corresponding SN Counter values.

##### 6.10.2.4.3 Security mechanism for UE to access target PSCell or SN

A UE can access a SN, disconnect to it and then access it again. Regardless of whether the UE has accessed the SN earlier, the UE shall select the first unused SN Counter value in the sequence of SN Counter values (i.e. sequence per SN) associated with the SN. Because all counter values are distinct, selecting the first unused one ensures that it is not previously used with the current KgNB. The UE shall then derive the corresponding KSN using the SN Counter value as described in Annex A.16 of this document and shall initiate the access procedure.

In parallel, UE shall inform the SN Counter value utilized for KSN derivation in the RRC Connection Reconfiguration Complete to the MN. The MN, in turn, shall relay the SN Counter value to the SN in the SN Reconfiguration Complete message.

The protected UP messages may reach the SN before the SN has received the SN counter value in the SN Reconfiguration Complete message. In this scenario, the SN chooses the first unused KSN key of the UE to establish the security association with the UE.

The UE and the SN shall derive the user plane encryption key and user plane integrity protection key, when configured, from the KSN for protecting their communications. The SN, upon receiving the SN counter value from the UE via the MN, shall check whether the corresponding SN Counter value of the chosen KSN is the same as the received SN Counter value to determine the KSN mismatch. In case of KSN mismatch, after receiving the SN counter in the SN Reconfiguration Complete message, the SN, having stored the KSN keys and the corresponding SN counter values, selects the appropriate KSN based on the received SN Counter value for subsequent data access under the same reconfiguration.

##### 6.10.2.4.4 Security procedure for UE to access target PSCell or SN

The SCPAC procedure in dual connectivity procedure with activation of encryption/decryption and/or integrity protection follows the steps outlined in Figure 6.10.2.4. 4-1.



Figure 6.10.2.4.4-1: Security procedures for SCPAC

1. The UE and the MN establishes the RRC connection.

2a-b. The MN sends SN Addition/Modification Request to each candidate target SN over the Xn-C to negotiate the available resources, configuration, and security algorithms at each candidate target SN. The MN assigns a sequence of distinct SN Counter values per candidate target SN during the SCPAC procedure. The MN derives the KSN keys corresponding to the sequence of SN Counter values from the KgNB of the UE. The MN delivers the sequence of SN Counter values and corresponding KSN keys of the UE to the respective candidate target SN. The UE security capabilities (see clause 6.10.2.1) and the UP security policy received from the SMF shall also be sent to SN. In case of PDU split, UP integrity protection and/or ciphering activation decision from MN may be also included as described in clause 6.10.2.1.

3. The candidate target SNs store the received sequence of SN Counter values and corresponding KSN keys of the UE and allocates the necessary resources and chooses the ciphering algorithm and integrity algorithm which has the highest priority from its configured list and is also present in the UE security capability as described in clause 6.10.2.1.

4. The respective target SN sends SN Addition/Modification Acknowledge to the MN indicating availability of requested resources and the identifiers for the selected algorithm(s) for the requested DRBs for the UE. The UP integrity protection and encryption indications shall be send to the MN.

5. The MN sends the RRC Reconfiguration Request to the UE, instructing it to configure the new DRBs for the selected target SNs.

The MN also includes all candidate SCG configuration(s) for one or multiple candidate SN(s) in the same RRC Reconfiguration Request message as the one that activates the new KgNB to the UE.

NOTE 1: Since the RRC Reconfiguration Request message is sent over the RRC connection between the MN and the UE, it is integrity-protected. Hence, the candidate SCG configuration(s) for one or multiple candidate SN(s) cannot be tampered with.

6. The UE accepts the RRC Reconfiguration Request after validating its integrity using the KRRCint of the MN.

7. When the UE selects a target SN, the UE shall choose the first unused SN Counter value in the SN Counter values sequence in the SCG configuration for the selected candidate target SN and compute the KSN. The UE shall also compute the needed UP keys and activate the UP protection per the indications received for the associated DRBs.

8. The UE sends the RRC Reconfiguration Complete to the MN, including the SN Counter value used in the derivation of the KSN.

9. The MN shall send the SN Reconfiguration Complete, including the SN Counter value received in step 8, to the target SN over the Xn-C to inform the target SN of the configuration result.

10. The SN shall activate encryption/decryption and integrity protection/verification with the UE upon receiving the SN Reconfiguration Complete message or the Random Access request from the UE.

If the SN activates the UP protection upon receiving the SN Reconfiguration Complete message, then the SN chooses the KSN key of the UE corresponding to the SN Counter value received in SN Reconfiguration Complete message and activates the UP protection after computing the needed UP keys.

11. In case the SN activates the UP protection upon receiving the Random Access request from the UE, then the target SN shall select the first unused KSN key of the UE in the sequence and computing the needed UP keys. Further, upon receiving the SN Reconfiguration Complete message, the SN shall determine the KSN mismatch as described in the clause 6.10.2.4.3. In case of KSN mismatch, the target SN chooses the KSN key of the UE corresponding to the SN Counter value received in SN Reconfiguration Complete message and activates the UP protection after computing the needed UP keys. The SN shall delete the configured KSN and corresponding SN counter value only after determining that there is no KSN key mismatch. The SN shall terminate the connection with the UE if the SN does not receive the SN Reconfiguration Complete message.

\*\*\*END OF CHANGES\*\*\*