**3GPP TSG-SA3 Meeting #100e *S3-201889***

**e-meeting, 17 -28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0924** | **rev** | **<Rev#>** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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 |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Correction to Clause 6.10.2.1. SN Addition or modification | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Lenovo, Motorola Mobility | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 07.08.2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Release 15 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | TS 33.501 Clause 6.10.2.1. SN Addition or modification states that, ‘The UE shall also compute the needed RRC and UP keys and activate the UP protection as per the indications received for the associated DRBs and/or SRB.’, which gives an incorrect notion that an UP protection may be activated based on the associated SRB. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is clarified that UP and RRC protection is activated as per the indications received for the associated DRBs and SRB respectively | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The specification will describe incorrect operation | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Clause 6.10.2.1. | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **x** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*Start of Change\*\*\*\*\*

#### 6.10.2.1 SN Addition or modification

When the MN is executing the Secondary Node Addition procedure (i.e. initial offload of one or more radio bearers to the SN), or the Secondary Node Modification procedure (as in clauses 10.2.2 and 10.3.2 in TS 37.340 [51]) which requires an update of the KSN, the MN shall derive an KSN as defined in clause 6.10.3.2 The MN shall maintain the SN Counter as defined in Clause 6.10.3.1

When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN shall, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last KSN change. If the MN cannot allocate an unused radio bearer identity for a new radio bearer in the SN, due to radio bearer identity space exhaustion, the MN shall increment the SN Counter and compute a fresh KSN, and then shall perform a SN Modification procedure to update the KSN.

The dual connectivity procedure with activation of encryption/decryption and integrity protection follows the steps outlined on the Figure 6.10.2.1-1.



Figure 6.10.2.1-1. Security aspects in SN Addition/Modification procedures (MN initiated)

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

2. The MN sends SN Addition/Modification Request to the SN over the Xn-C to negotiate the available resources, configuration, and algorithms at the SN. The MN computes and delivers the KSN to the SN if a new key is needed. The UE security capabilities (see subclause 6.10.4) and the UP security policy received from the SMF shall also be sent to SN. In case of PDU split, UP integrity protection and ciphering activation decision from MN may be also included as described in subclause 6.10.4.

3. The SN 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. If a new KSN was delivered to the SN then the SN calculates the needed RRC. The UP keys may be derived at the same time when RRC key derived. The SN shall activate the UP security policy as described in subclause 6.10.4.

4. The 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 and/or SRB for the UE. The UP integrity protection and encryption indications shall be send to the MN.

5. The MN sends the RRC Connection Reconfiguration Request to the UE instructing it to configure the new DRBs and/or SRB for the SN. The MN shall include the SN Counter parameter to indicate a new KSN is needed and the UE shall compute the KSN for the SN. The MN forwards the UE configuration parameters (which contains the algorithm identifier(s) received from the SN in step 4) , and UP integrity protection and encryption indications(received from the SN in step 4) to the UE (see subclause 6.10.3.3 for further details).

NOTE 3: Since the message is sent over the RRC connection between the MN and the UE, it is integrity protected using the KRRCint of the MN. Hence the SN Counter cannot be tampered with.

6. The UE accepts the RRC Connection Reconfiguration Request after validating its integrity. The UE shall compute the KSN for the SN if an SN Counter parameter was included. The UE shall also compute the needed RRC and UP keys and activate the RRC and UP protection as per the indications received for the associated SRB and/or DRBs respectively. The UE sends the RRC Reconfiguration Complete to the MN. The UE activates the chosen encryption/decryption and integrity protection keys with the SN at this point.

7. MN sends SN Reconfiguration Complete to the SN over the Xn-C to inform the SN of the configuration result. On receipt of this message, SN may activate the chosen encryption/decryption and integrity protection with UE. If SN does not activate encryption/decryption and integrity protection with the UE at this stage, SN shall activate encryption/decryption and integrity protection upon receiving the Random Access request from the UE.

\*\*\*\*\*End of Change\*\*\*\*\*