**3GPP TSG-SA3 Meeting #108-e *draft\_S3-222062-r1***

**e-meeting, 22nd - 26th August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.401** | **CR** | **0711** | **rev** | **-** | **Current version:** | **17.2.0** |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Alignment with RAN3 LS for EN-DC for UPIP | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | UPIP\_SEC\_LTE | | | | |  | ***Date:*** | | | 2022-08-15 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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:*** | | In the latest RAN3 LS S3-221724 to SA3 on the UP IP feature, it is stated that “*RAN3 has agreed not to send an explicit indication of UE support for UP integrity protection in the SgNB Addition Request message or in the SgNB Modification Request message, since RAN3 thinks that the en-gNB can interpret that the UE supports EPS UPIP capability once it receives the Security Indication for any E-RABs to enable UPIP.*” Thereofre,it is proposed to delete the indication for UPIP capability and align the security procedure accordingly. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Deletion of the UP IP indication in EN-DC. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misalignment with RAN3 specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | E.3.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## E.3.3 Activation of encryption/decryption/integrity protection of DRBs and encryption/decryption/integrity protection of SRB

The dual connectivity procedure with activation of encryption/decryption and integrity protection of Split and/or Non-Split SgNB terminated DRB(s) (i.e. a DRB for which PDCP is located in the SgNB) and/or activation of encryption/decryption and integrity protection of an SgNB terminated SRB (i.e. a SRB for which PDCP is located in the SgNB) follows the steps outlined on the Figure E.3.3-1.



Figure E.3.3-1. SgNB encryption/decryption and integrity protection activation

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

2. Before the MeNB decides to use dual connectivity for some DRB(s) and/or an SRB with the SgNB, the MeNB shall check whether the UE has NR capability and is authorized to access NR. The MeNB sends SgNB Addition Request to the SgNB over the X2-C to negotiate the available resources, configuration, and algorithms at the SgNB. The MeNB computes and delivers the S-KgNB to the SgNB if a new key is needed. The UE NR security capability shall also be sent to SgNB. The SgNB Addition Request message shall additionally include UP integrity protection policy (either the one received from other network entities or the locally configured one if no UP integrity protection policy is received from other network entities).

NOTE 1: Void.

NOTE 2: Void

3. The SgNB allocates the necessary resources and chooses the ciphering algorithm and integrity algorithms for the DRB(s) and SRB if an SRB is to be established which has the highest priority from its configured list and is also present in the UE NR security capability. If a new S-KgNB was delivered to the SgNB, then the SgNB calculates KSgNB-UP-int (if needed) and KSgNB-UP-enc as well as KSgNB-RRC-int and KSgNB-RRC-enc if an SRB is to be established. If the SgNB receives UP integrity protection policy from the MeNB, then the SgNB shall use the UP IP policy to determine whether to activate UP integrity protection. The SgNB shall activate UP integrity protection per DRB according to the UP integrity protection policy if it is received and shall indicate that to the UE. If the SgNB does not receive the UP IP policy, then the SgNB shall not activate UP IP.

4. The SgNB sends SgNB Addition Request Acknowledge to the MeNB indicating availability of requested resources and the identifiers for the selected algorithm(s) to serve the requested DRBs and/or SRB for the UE.

5. The MeNB sends the RRC Connection Reconfiguration Request to the UE instructing it to configure the new DRBs and/or SRB for the SgNB. The MeNB shall include the SCG Counter parameter to indicate that the UE shall compute the S-KgNB for the SgNB if a new key is needed. The MeNB forwards the UE configuration parameters (which contains the algorithm identifier(s) and UP integrity indication received from the SgNB in step 4) to the UE (see clause E.3.4.3 for further details).

NOTE 3: Since the message is sent over the RRC connection between the MeNB and the UE, it is integrity protected using the KRRCint of the MeNB. Hence the SCG Counter cannot be tampered with, and the UE can assume that it is fresh.

6. The UE accepts the RRC Connection Reconfiguration Command. The UE shall compute the S-KgNB for the SgNB if an SCG Counter parameter was included. The UE shall also compute KSgNB-UP-enc and KSgNB-UP-int (if needed) as well as KSgNB-RRC-int and KSgNB-RRC-enc for the associated assigned DRBs and/or SRB. The UE sends the RRC Reconfiguration Complete to the MeNB. The UE activates the chosen encryption/decryption and integrity protection at this point.

7. MeNB sends SgNB Reconfiguration Complete to the SgNB over the X2-C to inform the SgNB of the configuration result. On receipt of this message, SgNB may activate the chosen encryption/decryption and integrity protection with UE. If SgNB does not activate encryption/decryption and integrity protection with the UE at this stage, SgNB shall activate encryption/decryption and integrity protection upon receiving the Random Access request from the UE.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*