**3GPP TSG-SA3 Meeting #107-e *S3-221143r1***

**e-meeting, 16 - 20 May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.401** | **CR** | **0708** | **rev** | Will be 1 | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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:*** | Avoid linkage between security functions and UE Radio Access Capabilities | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Vodafone | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | UPIP\_SEC\_LTE | | | | |  | ***Date:*** | | | 2022-05-09 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | a) the UE’s security capabilities are sent in specially protected NAS procedures. Hence UPIP should not be able to be disabled by changing the EN\_DC capabilities in the UE’s Radio Access Capabilities.  b) CT1 have renamed the EIA7 bit to EPS-UPIP (see section 9.9.3.34 of TS 24.301 v17.6.0)  c) the Editor’s note seems redundant.  -The MME needs to be able to copy the EPS-UPIP bit into the S1 interface signalling.  - At X2 handover, absence of support in the source eNB is solved by the MME sending the UE’s security capabilities to the target eNB (as descibed in Note 4) | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Note a and the subsequent text is updated.  EIA7 is replaced by EPS-UPIP.  The Editor’s note is deleted. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | An attack on the UE RAC could disable LTE UPIP with a supporting UE. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7.3.3, E.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Rev 1 has S3-220862 merged into it. | | | | | | | | |

7.3.3 UP integrity protection policy

NOTE 1: Only EN-DC capable UEs and EN-DC capable eNBs support UP integrity protection. Therefore, the eNB can only activate UP integrity protection with a UE that is EN-DC capable and supports user plane integrity protection with EPS.

If the UE indicates that it supports user plane integrity protection with EPS by setting the EPS-UPIP bit in the EPS security capability, the MME shall provide UP integrity protection policy for each E-RAB to the eNB during the Attach/Dedicated bearer activation/Dedicated bearer modification procedure as specified in TS 23.401 [2]. The MME receives UP integrity protection policy from SMF+PGW-C via SGW.

NOTE 2: The SMF+PGW-C can be locally configured with UP integrity protection and confidentiality policy. However, the SMF+PGW-C only sends UP integrity protection policy to the upgraded SGW. The SMF+PGW-C, SGW and MME can use GTP-C signalling compatibility concepts to jugde whether to send UP integrity protection policy to the peer.

The UP integrity protection policy shall indicate whether UP integrity protection shall be activated or not for all DRBs belonging to that E-RAB.

The eNB shall be locally configured with UP integrity protection policy. If the eNB receives UP integrity protection policy from the MME, the eNB shall use the received UP integrity protection policy, otherwise, the eNB shall use the locally configured UP integrity protection policy if EPS-UPIP in the EPS security capability indicates that the UE supports user plane integrity protection with EPC.

The locally configured UP integrity protection policy on eNB should be set as "preferred".

The eNB shall activate UP integrity protection per each DRB, according to the UP integrity protection policy, using RRC signalling as defined in clause 7.3.4. If the UP integrity protection policy indicates "Required", the eNB shall activate UP integrity protection. If the eNB cannot activate UP integrity protection, and when the UP integrity protection policy is "Required", the eNB shall reject establishment of UP resources for the E-RAB and indicate reject-cause to the MME. If the UP integrity protection policy is " Not needed ", the eNB shall not activate UP integrity protection.

At an X2-handover from the source eNB to the target eNB, the source eNB shall include in the HANDOVER REQUEST message, the UP integrity protection policy, the UE EPS security capability and the corresponding E-RAB ID, if the UP integrity protection policy is received from other entities. If the target eNB does not receive the UP integrity protection policy, but the EPS-UPIP in the EPS security capability indicates that the UE supports user plane integrity protection with EPC, the target eNB shall use its locally configured UP integrity protection policy to activate or deactivate the UP integrity protection for all DRBs belonging to the E-RAB.

If the received UP integrity protection policy is ‘Required’, the target eNB shall reject all E-RABs for which it cannot comply with the corresponding UP integrity protection policy and indicate the reject-cause to the MME. For the accepted E-RABs, the target eNB shall activate UP integrity protection per DRB according to the UP integrity protection policy and shall indicate that to the UE in the HANDOVER COMMAND by the source eNB.

If the UE receives an indication in the HANDOVER COMMAND that UP integrity protection for an E-RAB is enabled at the target eNB, the UE shall generate or update the UP integrity protection key and shall activate UP integrity protection for the respective E-RAB.

NOTE 3: If the UP integrity protection policy is ‘Preferred’, it is possible to have a change in activation or deactivation of UP integrity after the handover.

Further, in the Path-Switch message, the target eNB shall send the UE's UP integrity protection policy and corresponding E-RAB ID to the MME. The sent UP integrity protection policy can either be the one received from source eNB or the locally configured one if the target eNB does not receive it from the source eNB, but the EPS-UPIP in the EPS security capability indicates that the UE supports user plane integrity protection with EPC. If the MME receives UP integrity protection policy, the MME shall verify that the UP integrity protection policy received from the target eNB is the same as the UP integrity protection policy that the MME has locally stored. If there is a mismatch, the MME shall send its locally stored UE's UP integrity protection policy of the corresponding E-RABs to the target eNB. This UP integrity protection policy, if included by the MME, is delivered to the target eNB in the Path-Switch Acknowledge message. The MME may support logging capabilities for this event and may take additional measures, such as raising an alarm.

NOTE 4: An upgraded target eNB may not receive UE’s UP integrity protection policy from a legacy source eNB, thus, mismatch of UP integrity protection policy may not be regarded as an abnormal case. The upgraded target eNB can get UE’s UP integrity protection policy from the MME.

If the target eNB receives UE's UP integrity protection policy from the MME in the Path-Switch Acknowledge message, the target eNB shall update the UE's UP integrity protection policy with the received UE's UP integrity protection policy. If UE's current UP integrity protection activation is different from the determination of received UE's UP integrity protection policy, then the target eNB shall initiate intra-cell handover procedure which includes RRC Connection Reconfiguration procedure to reconfigure the DRBs to activate or de-activate the UP integrity as per the received policy from MME.

At an S1-handover, the source MME shall send the UE's UP integrity protection policy and the UE EPS security capability to the target eNB via the target MME. Besides, the source eNB shall also send the UE’s UP integrity protection policy if received from the source MME to the target eNB in a source-to-target container. The target eNB shall use the UE capability indicating support of UP IP in EPS together with the UP integrity protection policy received from the MME and ignore the UP integrity protection received in the source-to-target container. If the target eNB does not receive the UP integrity protection policy from the MME, the target eNB shall use the UE capability indicating support of UP IP in EPS together with the UP integrity protection policy received from the source eNB. If both policies from MME and source eNB are absent, but EPS-UPIP in the EPS security capability indicates that the UE supports use of user plane protection with EPC, the eNB shall use locally configured UP integrity protection policy. The target eNB shall reject all E-RABs for which it cannot comply with the corresponding UP integrity protection policy and indicate the reject-cause to the source MME via the target MME. For all other E-RABs, the target eNB shall activate UP integrity protection per DRB according to the used UP integrity protection policy. If the target MME detects in a TAU procedure following S1-handover, and becomes aware of that there is a mismatch between the UE EPS security capabilities received from the source MME and the one received from the UE, and that the target eNB may not have the UE capability indicating UP IP support in UE EPS security capabilities, then the MME shall send an S1 CONTEXT MODIFICATION REQUEST message to inform the eNB about the correct UE EPS security capabilities and the target eNB shall take the new UE EPS security capabilities into account.

At interworking-handover from 5GS to EPS, the SMF+PGW-C provides the UE's UP integrity protection policy to the target eNB via the target MME. The target eNB shall determine from the UP integrity protection policy received from the SMF+PGW-C via the MME together with indication that the UE supports use of user plane protection with EPC whether to activate user plane integrity protection with the UE or not. If the target eNB does not receive the UP integrity protection policy from the SMF+PGW-C via the MME, but the UE indicates support of UP integrity protection with EPS , the eNB shall use locally configured UP integrity protection policy. The target eNB shall reject all E-RABs for which it cannot comply with the corresponding UP integrity protection policy and indicate the reject-cause to the source AMF via the target MME. For all other E-RABs, the target eNB shall activate UP integrity protection per DRB according to the used UP integrity protection policy.

\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## E.2.3 Activation of encryption/decryption

The DRB offload procedure with activation of encryption/decryption follows the steps outlined on the Figure E.2.3-1.



Figure E.2.3-1. SeNB encryption/decryption activation

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

2. The MeNB decides to offload the DRB(s) to the SeNB. The MeNB sends SeNB Addition Request to the SeNB over the X2-C to negotiate the available resources, configuration, and algorithms at the SeNB. The MeNB computes and delivers the S-KeNB to the SeNB as necessary. UE EPS security capability shall also be sent to SeNB. The SeNB 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).

3. The SeNB allocates the necessary resources and chooses the ciphering algorithm which has the highest priority from its configured list and is also present in the UE EPS security capability. If the UE supports user plane integrity protection, then the SeNB shall use the UP IP policy received from the MeNB together with the UE EPS security capabilities (i.e. the EPS-UPIP bit) to determine whether to activate UP integrity protection. The SeNB 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.

4. The SeNB sends SeNB Addition Request Acknowledge to the MeNB indicating availability of requested resources and the identifiers for the selected ciphering algorithm and integrity algorithm to serve the requested DRB for the UE.

5. The MeNB sends the RRC Connection Reconfiguration Request to the UE instructing it to configure a new DRB for the SeNB. The MeNB shall include the SCG Counter parameter to indicate that the UE shall compute the S-KeNB for the SeNB, the KUPenc and the KUPint associated with the assigned bearer. The MeNB forwards the UE configuration parameters (which contains the algorithm identifier received from the SeNB in step 4) to the UE (see section E.2.4.3 for further details).

NOTE: 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 and shall compute the S-KeNB for the SeNB. The UE shall also compute the KUPenc and the KUPint for the associated assigned DRB on the SeNB. The UE sends the RRC Reconfiguration Complete to the MeNB. The UE activates encryption/decryption and integrity protection once S-KeNB and KUPenc are derived.

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

\*\*\*\*\*\*\*\*\* end of changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*