**3GPP TSG-SA3 Meeting #104-e S3-212642-r1**

**e-meeting, 16 – 27 August 2021, Online**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | 1167 | **rev** | **1** | **Current version:** | **17.2.1** |  |
|  | | | | | | | | |
| *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 |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | UP Security policy requirement on the IMS data network | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2021-08-9 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | It is proposed to add the requirement that the UP security policy of the UP confidentiality and UP integrity protection for the IMS Data Network is recommended to set to "required", in order to protect the IMS data transferred via the user plane. That would be a security enhancement on the IMS data protection from the security point of view, no matter whether the protection between UE and IMS network is implemented or not. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding the requirement that the UP security policy of the UP confidentiality and UP integrity protection for the IMS Data Network is recommended to set to "required". | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The UP protection may not be activated for the IMS data. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.6.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\* \* \* First Change \* \* \* \*

### 6.6.1 UP security policy

The SMF shall provide UP security policy for a PDU session to the ng-eNB/gNB during the PDU session establishment procedure as specified in TS 23.502 [8].

The UP security policy shall indicate whether UP confidentiality and/or UP integrity protection shall be activated or not for all DRBs belonging to that PDU session. The UP security policy shall be used to activate UP confidentiality and/or UP integrity for all DRBs belonging to the PDU session.

The ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per each DRB, according to the received UP security policy, using RRC signalling as defined in clause 6.6.2. If the user plane security policy indicates "Required" or "Not needed", the ng-eNB/gNB shall not overrule the UP security policy provided by the SMF. If the ng-eNB/gNB cannot activate UP confidentiality and/or UP integrity protection when the received UP security policy is "Required", the ng-eNB/gNB shall reject establishment of UP resources for the PDU Session and indicate reject-cause to the SMF. If the received UP security policy is "Not needed ", then the establishment of the PDU Session shall proceed as described in TS 23.502 [8]. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the ng-eNB can activate UP integrity protection.

NOTE 1: Local SMF can override the confidentiality option in the UP security policy received from the home SMF based on its local policy, roaming agreement and/or regulatory requirements.

At an Xn-handover from the source ng-eNB/gNB to the target ng-eNB/gNB, the source ng-eNB/gNB shall include in the HANDOVER REQUEST message, the UE's UP security policy. If the UP security policy is ‘Required’, the target ng-eNB/gNB shall reject all PDU sessions for which it cannot comply with the corresponding received UP security policy and indicate the reject-cause to the SMF. For the accepted PDU sessions, the target ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per DRB according to the received UE's UP security policy and shall indicate that to the UE in the HANDOVER COMMAND by the source ng-eNB/gNB. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection.

If the UE receives an indication in the HANDOVER COMMAND that UP integrity protection and/or UP encryption for a PDU session is enabled at the target ng-eNB/gNB, the UE shall generate or update the UP encryption key and/or UP integrity protection key and shall activate UP encryption and/or UP integrity protection for the respective PDU session.

NOTE 2: If the security 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 ng-eNB/gNB shall send the UE's UP security policy and corresponding PDU session ID received from the source ng-eNB/gNB to the SMF. The SMF shall verify that the UE's UP security policy received from the target ng-eNB/gNB is the same as the UE's UP security policy that the SMF has locally stored. If there is a mismatch, the SMF shall send its locally stored UE's UP security policy of the corresponding PDU sessions to the target ng-eNB/gNB. This UP security policy information, if included by the SMF, is delivered to the target ng-eNB/gNB in the Path-Switch Acknowledge message. The SMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm.

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

In case of the target ng-eNB/gNB receives both UE security capability and UP security policy, then ng-eNB/gNB initiates the intra-cell handover procedure which contains selected algorithm and an NCC to the UE. New UP keys shall be derived and used at both the UE and the target ng-eNB/gNB.

At an N2-handover the SMF shall send the UE's UP security policy to the target ng-eNB/gNB via the target AMF. The target ng-eNB/gNB shall reject all PDU sessions for which it cannot comply with the corresponding received UP security policy and indicate the reject-cause to the SMF via the target AMF. For all other PDU sessions, the target ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per DRB according to the received UE's UP security policy. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection.

For the IMS data transferred via the user plane, it is recommended to set the UP security policy of the UP confidentiality and UP integrity protection for the IMS Data Network to "required".\* \* \* End of Changes \* \* \* \*