**3GPP TSG-SA3 Meeting #115 *draft\_*S3-240754-r2 merges 353 and 731**

Athens, Greece, 26th February - 1st March 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **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 |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | UPU Header Security | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Lenovo, Qualcomm?, Nokia, Nokia Shanghai Bell? | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | UE and network supports UPU data security but UPU header is not protected (in TS 33.501). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Enables UPU header protection without impacting legacy UEs and networks.  UPU Header protection can be enabled by any of the following two means, but this CR is implemented using the later approach (B) to avoid impacts to AUSF. CR can be reused if SA3 prefers Approach A.  Approach A: Reusing principles of SoR Header Protection, is simple and very straight forward.  Approach B: Placing UPU Header as part of UPU data and protecting together, to avoid AUSF impact while ensuring consitent MAC generation and verification between network and UE.  NOTE 1: In Approach B, it is not evident that legacy UDMs can apply UPU header protection. So even if the Rel.18 UE is made to support UPU header protection, if legacy UDM may not apply UPU header protection, the UPU header will not be protected. The UE as soon as it receives the UPU transparent container, it need to verify the UPU-MAC-IAUSF. Unless the UE knows if the UPU header is protected or not, the UE will not know what to use as input for UPU-MAC-IAUSF generation. For e.g., The UE supporting UPU header protection uses UPU header along with UPU data for UPU-MAC-IAUSF, but in this case the legacy UDM may not have applied UPU header protection and the MAC verification will fail. It should be noted that even if the UPU header is placed alongside UPU data to enable UPU header protection, it is expilcit that UPU data and UPU header are two different information for different purpose for UE, so it will be handled differently (See TS 24.501). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | UPU header protection cannot be supported. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.15.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

#### 6.15.2.1 Procedure for UE Parameters Update

The UDM may decide to perform UE parameters update anytime after the UE has been successfully authenticated and registered to the 5G system. The security procedure for the UE parameters update is described below in figure 6.15.2.1-1:



Figure 6.15.2.1-1: Procedure for UE Parameters Update

0) The UE has informed its capability to the UDM, that it supports UPU header protection.

1) The UDM decides to perform the UE Parameters Update (UPU) using the control plane procedure while the UE is registered to the 5G system. If the final consumer of any of the UE parameters to be updated (e.g., the updated Routing ID Data) is the USIM, the UDM shall protect these parameters using a secured packet mechanism (see 3GPP TS 31.115 [65]) to update the parameters stored on the USIM. The UDM shall then prepare the UE Parameters Update Data (UPU Data) by including the parameters protected by the secured packet, if any, as well as any UE parameters for which final consumer is the ME (see TS 24.501 [35]). The UDM shall include the UPU header in the UPU Data (i.e., to protect UPU header along with the UPU data), if the UDM supports UPU header protection and if it received earlier the UE capability on UPU header protection.

2-3) The UDM shall invoke Nausf\_UPUProtection service operation message by including the UPU Data to the AUSF to get UPU-MAC-IAUSF and CounterUPU as specified in sub-clause 14.1.4 of this document. The UDM shall select the AUSF that holds the latest KAUSF of the UE.

If the UDM decided that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM shall include the ACK Indication in the Nausf\_UPUProtection service operation message to signal that it also needs the expected UPU-XMAC-IUE, as specified in sub-clause 14.1.4 of this document.

The details of the CounterUPU is specified in sub-clause 6.15.2.2 of this document. The inclusion of UE Parameters Update Data in the calculation of UPU-MAC-IAUSF allows the UE to verify that it has not been tampered by any intermediary. The expected UPU-XMAC-IUE allows the UDM to verify that the UE received the UE Parameters Update Data correctly.

4) The UDM shall invoke Nudm\_SDM\_Notification service operation, which includes the UPU transparent container if the AMF supports UPU transparent container, or includes individual IEs comprising the UE Parameters Update Data, UPU-MAC-IAUSF, CounterUPU within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected UPU-XMAC-IUE.

5) Upon receiving the Nudm\_SDM\_Notification message, the AMF shall send a DL NAS Transport message to the served UE. The AMF shall include in the DL NAS Transport message the transparent container if received from the UDM in step 4. Otherwise, if the UDM provided individual IEs in step 4, then the AMF shall construct a UPU transparent container.

NOTE: The aspects on transparent container construction for the UPU header protection and its usage by the UE, are outside the scope of stage 2.

6) On receiving the DL NAS Transport message, the UE shall calculate the UPU-MAC-IAUSF in the same way as the AUSF (as specified in Annex A.19) on the received UE Parameters Update Data and the CounterUPU and verify whether it matches the UPU-MAC-IAUSF value received within the UPU transparent container in the DL NAS Transport message. If the verification of UPU-MAC-IAUSF is successful and the UPU Data contains any parameters that is protected by secured packet (see 3GPP TS 31.115 [65]), the ME shall forward the secured packet to the USIM using procedures in 3GPP TS 31.111 [66]. If the verification of UPU-MAC-IAUSF is successful and the UPU Data contains any parameters that is not protected by secure packet, the ME shall update its stored parameters with the received parameters in UDM Updata Data. The UE shall use the protected UPU header (if this is available in the UPU data).7) If the UDM has requested an acknowledgement from the UE and the UE has successfully verified and updated the UE Parameters Update Data provided by the UDM, then the UE shall send the UL NAS Transport message to the serving AMF. The UE shall generate the UPU-MAC-IUE as specified in Annex A.20 and include the generated UPU-MAC-IUE in a transparent container in the UL NAS Transport message.

8) If a transparent container with the UPU-MAC-IUE was received in the UL NAS Transport message, the AMF shall send a Nudm\_SDM\_Info request message with the transparent container to the UDM.

9) If the UDM indicated that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM shall compare the received UPU-MAC-IUE with the expected UPU-XMAC-IUE that the UDM stored temporarily in step 4.

If the UDM supports Home triggered authentication (see clause 6.1.5), the UDM based on its local policy may decide to trigger a primary authentication to refresh the UPU counter based on the value of counter received in step 3.

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