**3GPP TSG-SA3 Meeting #124** *draft\_S3-253662-r1 merges 3577, 3277 in* **S3-253144**

Wuhan, China, 13-17 October 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Alignment CR for UPU Header Security | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Lenovo, Nokia?, Ericsson? | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2025-08-17 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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:*** | | CT1 LS C1-253719 clarifies that, UE indicates whether it supports UPU header protection via the UPU header i.e., CT1 agreed (C1-253696) UE parameters update header security aspects in TS 24.501. In TS 33.501, we have the following text but not clarified how.  *0) The UE has informed its capability to the UDM, that it supports UPU header protection.*  But now this agreed CT1 CR clarifies the necessary details of how the UE can indicates its UPU header protection support to the network. Further the UE behaviour is clarified as follows in the agreed CT1 CR.  *i0) if the UE supports UE parameters update header protection and the UE parameters update list includes a UE parameters update data set with the UE parameters update data set type indicating "protected UE parameters update header information", then the UE shall use header information from the UE parameters update data set with the UE parameters update data set type indicating "protected UE parameters update header information", otherwise the UE shall use header information from the UE parameters update header in the UE parameters update transparent container;*  Hence the related alignment is done in this CR along with the related clarifications and citation. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarifications and citations added related to UE capability on UPU header protection [similar to the other clarification format in Clause 6.15.2.1 as highlighted for reference.] | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete specification | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.15.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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\*\*\*\*\*

#### 6.15.2.1 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 may have informed its capability to the UDM, that it supports UPU header protection according to TS 24.501 [35].

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]). If the UDM supports UPU header protection and if it received earlier the UE capability on UPU header protection is supported, the UDM may include the UPU header information in the UPU Data (i.e., to protect UPU header along with the UPU data). If the UDM supports UPU header protection but the UE capability on UPU header protection is unknown, the UDM shall not include the UPU header information in the UPU Data and shall require the UE to send an acknowledgement.

NOTE 1: Further aspects on transparent container construction for the UPU header protection and its correct usage by the UE are outside the scope of the present document.

NOTE 2: The UDM including the UPU header info in the UPU Data in Step 1, ensures protection of the UPU header when the transport of the UPU Data within the 5GC transparent container is supported.

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. If the UE is performing initial registration or emergency registration and the UDM supports UPU header protection, the UDM shall request an acknowledgement.

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.

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. If the UE supports UPU header protection and if the UPU data contains protected UPU header information ( see TS 24.501 [35]), then the UE shall use the protected UPU header information as the UPU header.

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. If the UE supports UPU header protection, the UE includes the UE capability on UPU header protection as supported within the acknowledgment.

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 acknowledgment includes the UE capability on UPU header protection, the UDM shall store it for future use.

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\*\*\*\*\*