**3GPP TSG-CT WG1 Meeting #130-eC1-213342**

**Electronic meeting, 20 – 28 May 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **3299** | **rev** | **-** | **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 | **x** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | | |
| ***Title:*** | Storage on counters and keys in 5G AKA | | | | | | | | | | |
|  |  | | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | | |
|  |  | | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17 | | | | | |  | ***Date:*** | | | 2021-05-13 |
|  |  | | | | |  | |  | | |  |
| ***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 description about EAP-AKA’, UE is requested to reset the SOR counter and the UE parameter update counter, and store the KAUSF and KSEAF when the EAP-AKA’ procedure is completed successfully. Please see below, quoted from the subclause 5.4.1.2.2.8 of TS 24.501  *The ME shall reset the SOR counter and the UE parameter update counter to zero, and store KAUSF, KSEAF, the SOR counter and the UE parameter update counter as specified in annex C.*  However, there is no similar statement for the 5G AKA procedure, it will let implementers mistakenly think that UE does not need to reset the SOR counter and the UE parameter update counter and store the KAUSF and KSEAF in 5G AKA procedure. | | | | | | | | |
|  | |  | | | | | | | | | |
| ***Summary of change:*** | | UE reset SOR counter and the UE parameter update counter, and store KAUSF, KSEAF when the 5G AKA is completed successfully | | | | | | | | | |
|  | |  | | | | | | | | | |
| ***Consequences if not approved:*** | | ME will not reset the SOR counter/UPU counter, store the KAUSF, KSEAF in 5G AKA | | | | | | | | | |
|  | |  | | | | | | | | | |
| ***Clauses affected:*** | | 5.4.1.3.1 | | | | | | | | | |
|  | |  | | | | | | | | | |
|  | | **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 1st change \*\*\*\*\*

##### 5.4.1.3.1 General

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF (see 3GPP TS 33.501 [24]). The cases when the 5G AKA based primary authentication and key agreement procedure is used are defined in 3GPP TS 33.501 [24].

The network initiates the 5G AKA based primary authentication and key agreement procedure by sending an AUTHENTICATION REQUEST message to the UE without the EAP message IE. The network shall include the ngKSI and the ABBA in AUTHENTICATION REQUEST message.

The 5G AKA based primary authentication and key agreement procedure is always initiated and controlled by the network. However, the UE can reject the 5G authentication challenge sent by the network.

The UE shall proceed with a 5G authentication challenge only if a USIM is present.

A partial native 5G NAS security context is established in the UE and the network when a 5G authentication is successfully performed. During a successful 5G AKA based primary authentication and key agreement procedure, the CK and IK are computed by the USIM. CK and IK are then used by the ME as key material to compute new keys KAUSF, KSEAF and KAMF. KAMF is stored in the 5G NAS security contexts (see 3GPP TS 33.501 [24]) of both the network and in the volatile memory of the ME while registered to the network, and is the root for the 5GS integrity protection and ciphering key hierarchy. When the 5G AKA based primary authentication and key agreement procedure completes successfully, the ME shall reset the SOR counter and the UE parameter update counter to zero, and store KAUSF, KSEAF, the SOR counter and the UE parameter update counter as specified in annex C.

Editor's note: It is FFS how does the UE identify the successful completion of the 5G AKA based primary authentication and key agreement procedure.

The 5G AKA based primary authentication and key agreement procedure is initiated by an AUTHENTICATION REQUEST message without the EAP message IE.

\*\*\*\*\* end of 1st change \*\*\*\*\*