**3GPP TSG-CT WG1 Meeting #141eC1-232084v1**

**Online 17– 21 April 2023**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **5185** | **rev** | **1** | **Current version:** | **18.2.1** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | 5G AKA based primary authentication and key agreement procedure initiation |
|  |  |
| ***Source to WG:*** | ZTE, Huawei |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc18 |  | ***Date:*** | 2023-04-07 |
|  |  |  |  |  |
| ***Category:*** | **D** |  | ***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 canbe 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | In TS 24.501 subclause 5.4.1.3.1, it specifies that“*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 5G AKA based primary authentication and key agreement procedure is initiated by an AUTHENTICATION REQUEST message without the EAP message IE.*”The highlighted sentence overlaps with the highlighted sentences as the highlighted sentences have already clearly specified how the 5G AKA based primary authentication and key agreement procedure is initiated. |
|  |  |
| ***Summary of change:*** | Remove the highlighted sentence above. |
|  |  |
| ***Consequences if not approved:*** | Redundant paragraph regarding how the 5G AKA based primary authentication and key agreement procedure is initiated. |
|  |  |
| ***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:*** |  |

\* \* \* First 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.

NOTE 1: Generation of the new KAUSF and the new KSEAF does not result into deletion of the valid KAUSF and the valid KSEAF, if any.

Upon successful completion of the 5G AKA based primary authentication, the AMF shall initiate a security mode control procedure (see subclause 5.4.2) to take the new partial native 5G NAS security context into use.

NOTE 2: The AMF immediately initiates a security mode control procedure (see subclause 5.4.2) after 5G AKA primary authentication is successful to avoid KAUSF key mismatch between the UE and the network.

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