**3GPP TSG-CT WG1 Meeting #131-eC1-214966**

**E-meeting, 19-27 August 2021 (was C1-214553)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **3503** | **rev** | **1** | **Current version:** | **17.3.1** |  |
|  |
| *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 | **x** |

|  |
| --- |
|  |
| ***Title:***  | SMC after Primary Authentication |
|  |  |
| ***Source to WG:*** | Samsung, NEC, Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc17 |  | ***Date:*** | 2021-08-12 |
|  |  |  |  |  |
| ***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 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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | SA3 requested CT1 to check about feasibility to initiate security mode command after the primary authentication. CT1 shared response in C1-211518 indicating that AMF initiating a security mode control procedure as soon as possible after a successful primary authentication and key agreement procedure to take the new partial native 5G NAS security context into use is feasible. Based on CT1 response, SA3 shared LS S3-212291 with attachment S3-212290 suggesting the below change. SA3 response.Based on the answer for CT1(S3-211375/C1-211518), SA3 has agreed the attached Rel-17 CR (S3-212290, CR#1138) to TS 33.501, to mandate the AMF to initiate a security mode control (SMC) procedure soon after a successful primary authentication and key agreement procedure to take the new partial native 5G NAS security context into use. Mandating the AMF to initiate a SMC procedure as soon as possible after a successful primary authentication is applicable only when using **5G AKA based authentication** and not for **EAP based authentication**  |
|  |  |
| ***Summary of change:*** | AMF to initiate security mode command after 5G AKA authetication is successful |
|  |  |
| ***Consequences if not approved:*** | UE will not know if the authentication is successful or not. This will cause KAUSF keys mismatch between UE and network. |
|  |  |
| ***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 5G AKA based primary authentication and key agreement procedure

##### 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.

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

Upon successful completion of the 5G AKA 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 shall immediately initiate 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

\*\*\*\*\* Next change \*\*\*\*\*

### 5.4.2 Security mode control procedure

#### 5.4.2.1 General

The purpose of the NAS security mode control procedure is to take a 5G NAS security context into use, and initialise and start NAS signalling security between the UE and the AMF with the corresponding 5G NAS keys and 5G NAS security algorithms.

Furthermore, the network may also initiate the security mode control procedure in the following cases:

a)- in order to change the 5G NAS security algorithms for a current 5G NAS security context already in use;

b) in order to change the value of uplink NAS COUNT used in the latest SECURITY MODE COMPLETE message as described in 3GPP TS 33.501 [24], subclause 6.9.4.4; and

c) in order to provide the Selected EPS NAS security algorithms to the UE.

For restrictions concerning the concurrent running of a security mode control procedure with other security related procedures in the AS or inside the core network see 3GPP TS 33.501 [24], subclause 6.9.5.If the security mode control procedure is initiated after successful 5G AKA based primary authentication and key agreement procedure and the security mode control procedure intends to bring into use the partial native 5G NAS security context created by the 5G AKA based primary authentication and key agreement procedure and the UE accept received security mode command (see subclause 5.4.2.3), the ME shall:

a) delete the valid KAUSF and the valid KSEAF, if any; and

b) consider the new KAUSF to be the valid KAUSF, and the new KSEAF to be the valid KSEAF, reset the SOR counter and the UE parameter update counter to zero, and store the valid KAUSF, the valid KSEAF , the SOR counter and the UE parameter update counter as specified in annex C and use the valid KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received.

\*\*\*\*\* End change \*\*\*\*\*