**3GPP TSG-CT WG1 Meeting #128-eC1-21xxxx**

**Electronic meeting, 25 February – 5 March 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **3064** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  |
| *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 | **x** |

|  |
| --- |
|  |
| ***Title:***  | Mandating SMC following successful AKA |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon, Qualcomm Incorporated |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc17 |  | ***Date:*** | 2021-02-10 |
|  |  |  |  |  |
| ***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:*** | As per requested in the SA3 LS C1-210531/S3-210706 as below:"*SA3 is considering a solution, where only after identifying that the primary (re)authentication is successful in the network side, the UE shall store the KAUSF, SOR counter and UE parameter update counter on the USIM (or in the non-volatile memory of the ME, if no corresponding file is present on the USIM). The UE identifies that the primary (re)authentication is successful in the network side, upon receiving a valid NAS Security Mode Command message.* *The solution under consideration mandates performing NAS SMC procedure, after the successful run of primary authentication. Running of the NAS SMC procedure after primary authentication as soon as possible is essential to keep the stored KAUSF aligned between the UE and home network. On this new mandatory requirement under consideration, SA3 would like to have feedback from CT1 and CT4, on the feasibility to perform NAS SMC procedure immediately after successful run of primary authentication.* "Note that though as indicated in the original CT1 LS C1-207764, the open issue is only for 5G AKA procedure, but SA3 LS does not mention which specific AKA procedure the above SA3 requirement applies. Hence, by default it is applied to both EAP AKA-based and 5G AKA-based procedures. This could provide a simpler and consistent network handling on confirming the successful AKA to the UE.For EAP AKA, if now mandating to initiate the SMC procedure following a successful EAP AKA, then there is no need to carry the EAP-success message via AUTHENTICATION RESULT message to the UE. |
|  |  |
| ***Summary of change:*** | 1. It proposes that after a successful primary authentication and key agreement procedure (including EAP AKA and 5G AKA), the network shall initiate the security mode control procedure to confirm the successful AKA to the UE.
2. It proposes to remove using the AUTHENTICATION RESULT message to carry the EAP-success message to the UE following a successful EAP AKA procedure.
3. It proposes to add a NOTE to indicate the AMF to initiate the SMC procedure after the successful AKA procedure as soon as possible.
 |
|  |  |
| ***Consequences if not approved:*** | SA3 requirement was not implemented and the issue on when the new generated KAUSF is stored at the UE was not resolved. |
|  |  |
| ***Clauses affected:*** | 5.4.1.2.1, 5.4.1.2.5.1, 5.4.1.2.5.2, 5.4.2.1 |
|  |  |
|  | **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:*** |  |

\* \* \* First Change \* \* \* \*

##### 5.4.1.2.1 General

The purpose of the EAP 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]).

Extensible authentication protocol (EAP) as specified in IETF RFC 3748 [34] enables authentication using various EAP methods.

EAP defines four types of EAP messages:

a) an EAP-request message;

b) an EAP-response message;

c) an EAP-success message; and

d) an EAP-failure message.

Several rounds of exchanges of an EAP-request message and a related EAP-response message can be required to achieve the authentication (see example in figure 5.4.1.2.1.1).

The EAP based primary authentication and key agreement procedure is always initiated and controlled by the network.

The EAP-request message, the ngKSI and the ABBA are transported from the network to the UE using the AUTHENTICATION REQUEST message of the EAP message reliable transport procedure.

The EAP-response message is transported from the UE to the network using the AUTHENTICATION RESPONSE message of the EAP message reliable transport procedure.

If the authentication of the UE completes successfully, the serving AMF shall initiate a security mode control procedure after the EAP based primary authentication and key agreement procedure to bring into use the partial native 5G NAS security context created by the EAP based primary authentication and key agreement procedure, then the EAP-success message and the ngKSI are transported from the network to the UE using the SECURITY MODE COMMAND message of the security mode control procedure (see subclause 5.4.2).

If the authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE using the AUTHENTICATION RESULT message or the AUTHENTICATION REJECT message of the EAP result message transport procedure or in a response of the initial 5GMM procedure as part of which the EAP based primary authentication and key agreement procedure is performed.

The AMF shall set the authenticator retransmission timer specified in IETF RFC 3748 [34] subclause 4.3 to infinite value.

NOTE 1: The EAP message reliable transport procedure provides a reliable transport of EAP messages and therefore retransmissions at the EAP layer do not occur.

The AUSF and the AMF support exchange of EAP messages using N12.

The UE shall detect and handle any duplication of EAP message as specified in IETF RFC 3748 [34].

Figure 5.4.1.2.1.1: EAP based primary authentication and key agreement procedure

\* \* \* Next Change \* \* \* \*

###### 5.4.1.2.5.1 General

The purpose of the EAP result message transport procedure is to provide an EAP-failure message, and ngKSI from the network to the UE, when the EAP message cannot be piggybacked by another NAS message.

The EAP result message transport procedure is initiated:

- by an AUTHENTICATION RESULT message with the EAP message IE carrying the EAP-failure message; or

- by an AUTHENTICATION REJECT message with the EAP message IE carrying the EAP-failure message.

\* \* \* Next Change \* \* \* \*

###### 5.4.1.2.5.2 EAP result message transport procedure initiation by the network

In order to initiate the EAP result message transport procedure, the AMF shall create an AUTHENTICATION RESULT message or an AUTHENTICATION REJECT message.

The AMF shall set the EAP message IE of the AUTHENTICATION RESULT message to an EAP-failure message to be sent to the UE. The AMF shall set the EAP message IE of the AUTHENTICATION REJECT message to an EAP-failure message to be sent to the UE. The AMF shall set the ngKSI IE of the AUTHENTICATION RESULT message or the AUTHENTICATION REJECT message to the ngKSI value selected in subclause 5.4.1.2.2.2, subclause 5.4.1.2.3.1 or subclause 5.4.1.2.3A.1.

The AMF shall send the AUTHENTICATION RESULT message or the AUTHENTICATION REJECT message to the UE (see example in figure 5.4.1.2.5.2.1).



Figure 5.4.1.2.5.2.1: EAP result message transport procedure

Upon receipt of an AUTHENTICATION RESULT message or an AUTHENTICATION REJECT message with the EAP message IE, the UE handles the EAP message received in the EAP message IE and the ABBA if received of the AUTHENTICATION RESULT message or in the AUTHENTICATION REJECT message.

\* \* \* Next Change \* \* \* \*

#### 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.

After a successful primary authentication and key agreement procedure as specified in subclauses 5.4.1.2 and 5.4.1.3, the network shall initiate the security mode control procedure to take the new partial native 5G NAS security context into use.

NOTE: It is recommended that the AMF initiates a security mode control procedure as soon as possible after a successful primary authentication and key agreement procedure in order to avoid cases when the KAUSF at the UE and the KAUSF at the network can become misaligned.

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.

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