**3GPP TSG-SA3 Meeting #104-e *S3-212597***

**e-meeting, 16 - 27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1158** | **rev** | **1** | **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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clairfication on AS key generation after runing NAS SMC | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2021-08-16 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | To store the Kausf at UE in 5G-AKA procedure, the NAS SMC is mandotary to run. NAS SMC is also used to take new partial native security context into use. Take new partial native security context into use may imply to the reader that both NAS and AS security needs to be refreshed. But according to the principle of TS 33.501, there is no strongly binding the refreshing the NAS security context and AS security context. So a clarification is added to make this clear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add a new sentenct in 5G-AKA to say the mandatory running NAS SMC does not have to refresh the AS security keys. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Not clear | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.1.1, 6.1.3.2.0 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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\*\*\*\*\*\*\*\*\*\*\*

## 6.1 Primary authentication and key agreement

### 6.1.1 Authentication framework

#### 6.1.1.1 General

The purpose of the primary authentication and key agreement procedures is to enable mutual authentication between the UE and the network and provide keying material that can be used between the UE and the serving network in subsequent security procedures. The keying material generated by the primary authentication and key agreement procedure results in an anchor key called the KSEAF provided by the AUSF of the home network to the SEAF of the serving network.

Keys for more than one security context can be derived from the KSEAF without the need of a new authentication run. A concrete example of this is that an authentication run over a 3GPP access network can also provide keys to establish security between the UE and a N3IWF used in untrusted non-3GPP access.

The anchor key KSEAF is derived from an intermediate key called the KAUSF. The KAUSF is established between the UE and HN resulting from the primary authentication procedure. The KAUSF may be securely stored in the AUSF based on the home operator's policy on using such key. e.g. if the control plane solution for Steering of Roaming (see clause 6.14) or UE Parameter Update procedures (see clause 6.15) or AKMA are supported by the HPLMN.

NOTE A: For standalone non-public networks when an authentication method other than 5G AKA or EAP-AKA' is used, Annex I.2 applies.

NOTE 1: This feature is an optimization that might be useful, for example, when a UE registers to different serving networks for 3GPP-defined access and untrusted non-3GPP access (this is possible according to TS 23.501 [2]). The details of this feature are operator-specific and not in scope of this document.

NOTE 2: A subsequent authentication based on the KAUSF stored in the AUSF gives somewhat weaker guarantees than an authentication directly involving the ARPF and the USIM. It is rather comparable to fast re-authentication in EAP-AKA'.

NOTE 2a: Void.

UE and serving network shall support EAP-AKA' and 5G AKA authentication methods.

NOTE 2b: It is the home operator's decision which authentication method is selected.

The USIM shall reside on a UICC. The UICC may be removable or non-removable.

NOTE 3: For non-3GPP access networks USIM applies in case of terminal with 3GPP access capabilities.

If the terminal supports 3GPP access capabilities, the credentials used with EAP-AKA' and 5G AKA for non-3GPP access networks shall reside on the UICC.

NOTE 4: EAP-AKA' and 5G AKA are the only authentication methods that are supported in UE and serving network, hence only they are described in sub-clause 6.1.3 of the present document. For a private network using the 5G system as specified in [7] an example of how additional authentication methods can be used with the EAP framework is given in the informative Annex B.

NOTE 5: For non-public network (NPN) security the Annex I of the present document provides details.

Upon successful completion of the 5G AKA primary authentication, the AMF shall initiate NAS security mode command procedure (see clause 6.7.2) with the UE.

NOTE 6: The reason to mandatory run the NAS SMC procedure after primary authentication is because the UE does not store the new derived KAUSF until receiving the NAS SMC message. The new partial native NAS security context is taken into use. Activating a partial native 5G NAS security context does not have to trigger AS key re-keying procedure as depicted in clause 6.9.4.4.

\*\*\*\*\*\*\*\*\*\*\* End of 1st Change\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\* Start of 2nd Change\*\*\*\*\*\*\*\*\*\*\*

#### 6.1.3.2 Authentication procedure for 5G AKA

##### 6.1.3.2.0 5G AKA

5G AKA enhances EPS AKA [10] by providing the home network with proof of successful authentication of the UE from the visited network. The proof is sent by the visited network in an Authentication Confirmation message.

The selection of using 5G AKA is described in sub-clause 6.1.2 of the present document.

NOTE 1: 5G AKA does not support requesting multiple 5G AVs, neither the SEAF pre-fetching 5G AVs from the home network for future use.



Figure 6.1.3.2-1: Authentication procedure for 5G AKA

The authentication procedure for 5G AKA works as follows, cf. also Figure 6.1.3.2-1:

1. For each Nudm\_Authenticate\_Get Request, the UDM/ARPF shall create a 5G HE AV. The UDM/ARPF does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1" as defined in TS 33.102 [9]. The UDM/ARPF shall then derive KAUSF (as per Annex A.2) and calculate XRES\* (as per Annex A.4). Finally, the UDM/ARPF shall create a 5G HE AV from RAND, AUTN, XRES\*, and KAUSF.

2. The UDM shall then return the 5G HE AV to the AUSF together with an indication that the 5G HE AV is to be used for 5G AKA in a Nudm\_UEAuthentication\_Get Response. In case SUCI was included in the Nudm\_UEAuthentication\_Get Request, UDM will include the SUPI in the Nudm\_UEAuthentication\_Get Response after deconcealment of SUCI by SIDF.

If a subscriber has an AKMA subscription, the UDM shall include the AKMA indication in the Nudm\_UEAuthentication\_Get Response.

3. The AUSF shall store the XRES\* temporarily together with the received SUCI or SUPI.

4. The AUSF shall then generate the 5G AV from the 5G HE AV received from the UDM/ARPF by computing the HXRES\* from XRES\* (according to Annex A.5) and KSEAF from KAUSF(according to Annex A.6), and replacing the XRES\* with the HXRES\* and KAUSF with KSEAF in the 5G HE AV.

5. The AUSF shall then remove the KSEAF and return the 5G SE AV (RAND, AUTN, HXRES\*) to the SEAF in a Nausf\_UEAuthentication\_Authenticate Response.

6. The SEAF shall send RAND, AUTN to the UE in a NAS message Authentication Request. This message shall also include the ngKSI that will be used by the UE and AMF to identify the KAMF and the partial native security context that is created if the authentication is successful. This message shall also include the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. The ME shall forward the RAND and AUTN received in NAS message Authentication Request to the USIM.

NOTE 2: The ABBA parameter is included to enable the bidding down protection of security features.

7. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102[9]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [9], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME then shall compute RES\* from RES according to Annex A.4. The ME shall calculate KAUSF from CK||IK according to clause A.2. The ME shall calculate KSEAF from KAUSF according to clause A.6. An ME accessing 5G shall check during authentication that the "separation bit" in the AMF field of AUTN is set to 1. The "separation bit" is bit 0 of the AMF field of AUTN.

NOTE 3: This separation bit in the AMF field of AUTN cannot be used anymore for operator specific purposes as described by TS 33.102 [9], Annex F.

8. The UE shall return RES\* to the SEAF in a NAS message Authentication Response.

9. The SEAF shall then compute HRES\* from RES\* according to Annex A.5, and the SEAF shall compare HRES\* and HXRES\*. If they coincide, the SEAF shall consider the authentication successful from the serving network point of view. If not, the SEAF proceed as described in sub-clause 6.1.3.2.2. If the UE is not reached, and the RES\* is never received by the SEAF, the SEAF shall consider authentication as failed, and indicate a failure to the AUSF.

10. The SEAF shall send RES\*, as received from the UE, in a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF.

11. When the AUSF receives as authentication confirmation the Nausf\_UEAuthentication\_Authenticate Request message including a RES\* it may verify whether the 5G AV has expired. If the 5G AV has expired, the AUSF may consider the authentication as unsuccessful from the home network point of view. Upon successful authentication, the AUSF shall store the KAUSF. AUSF shall compare the received RES\* with the stored XRES\*. If the RES\* and XRES\* are equal, the AUSF shall consider the authentication as successful from the home network point of view. AUSF shall inform UDM about the authentication result (see sub-clause 6.1.4 of the present document for linking with the authentication confirmation).

NOTE 4: It is left to implementation to temporarily store the KAUSF received in step 2 in AUSF until the RES\* verification is done successfully (i.e., at step 11).

12. The AUSF shall indicate to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response whether the authentication was successful or not from the home network point of view. If the authentication was successful, the KSEAF shall be sent to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response. In case the AUSF received a SUCI from the SEAF in the authentication request (see sub-clause 6.1.2 of the present document), and if the authentication was successful, then the AUSF shall also include the SUPI in the Nausf\_UEAuthentication\_Authenticate Response message.

If the authentication was successful, the key KSEAF received in the Nausf\_UEAuthentication\_Authenticate Response message shall become the anchor key in the sense of the key hierarchy as specified in sub-clause 6.2 of the present document. Then the SEAF shall derive the KAMF from the KSEAF, the ABBA parameter and the SUPI according to Annex A.7. The SEAF shall provide the ngKSI and the KAMF to the AMF. If the AUSF indicates that the authentication was successful from the home network point of view, then the AMF shall initiate NAS security mode command procedure (see clause 6.7.2) with the UE, to take the newly generated partial native 5G NAS security context into use. Upon receiving the valid NAS Security Mode Command message from the AMF, the UE shall consider the performed primary authentication as successful.NOTE 5: Activating a partial native 5G NAS security context does not have to trigger AS key re-keying procedure as depicted in clause 6.9.4.4.

If a SUCI was used for this authentication, then the SEAF shall only provide ngKSI and KAMF to the AMF after it has received the Nausf\_UEAuthentication\_Authenticate Response message containing KSEAF and SUPI; no communication services will be provided to the UE until the SUPI is known to the serving network.

The further steps taken by the AUSF after the authentication procedure are described in sub-clause 6.1.4 of the present document.

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