**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220402-r2***

**e-meeting, 14 – 25 February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1340** | **rev** | **1** | **Current version:** | **15.14.1** |  |
|  | | | | | | | | |
| *For* [***HELP***](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:*** | Clarification on unspecified expiration of AV in 5G AKA | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI15 | | | | |  | ***Date:*** | | | 2022-02-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-15 |
|  | *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:*** | | Last meeting CR S3-214498 proposed to remove the first 2 sentences in step 11 with the following reason: “How AUSF verify the expiration of AV in 5G AKA is not specified further and has not been implemented by stage 3 as well.”  Discussion:  Only one 5G AV can be requested, and AUSF will wait for a response before deleting it. In the initial registration request, a requested 5G AV should be used immediately. But in a reauthentication case, there is no rule defined, when AMF/AUSF would request the 5G AV. Thus, checking the expiry of an 5G AV at the home operator side makes sense, even though it is implementation specific and not an interoperability issue. Same in visited network, it is responsibility of the SN operator to manage the lifetime of the requested 5G SN AV.  Therefore, it is proposed to keep the respective text in step 11, and add a note for clarification.  Thus, this update of the CR suggests to maintain the text, because in step 3 the RES\* storage is mentioned and it is necessary to give some guidance on the comparison of RES\* and XRES\* in the operator domain.  There needs to be clarification on the behaviour how to handle the situation in AMF when the authentication is unsuccessful due to expiry of the 5G AV.  The two sentences under discussion in step 11 show an option for the operator how to proper manage 5G AV. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add NOTEs in step 3 and 11 to explain why no stage 3 is needed. Clarify that in case of authentication reject, the visited network AMF/SEAF needs to be informed for the reason, to align with stage 3 existing behaviour and specify both in stage 2: success case and unsuccess case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Clarification missing, why no stage 3 provided. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.3.2.0, 6.1.3.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 CHANGES

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 and Routing indicator in the Nudm\_UEAuthentication\_Get Response.

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

NOTE Aa: How long XRES\* is stored is left to implementation, see also step 11.

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 stores the KAUSF based on the home network operator's policy according to clause 6.1.1.1. AUSF shall compare the received RES\* with the stored XRES\*. If the 5G AV has not expired, and 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).

NOTE X: Storage and expiry handling of 5G AV in AUSF are implementation dependant.

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 RES\* verification failed in step 11 (i.e. RES\* and XRES\* are not equal), the AUSF provides an authentication failure indication to the SEAF. If the authentication was not successful due to other reasons (e.g., 5G AV expiration, SUCI de-concealment, AUSF or UDM internal error), the AUSF shall indicate the reason to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response.

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.

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.

\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

6.1.3.2.2 RES\* verification failure in SEAF or AUSF or both

This clause describes how RES\* verification failure in the SEAF or in the AUSF shall be handled.

In step 9 in Figure 6.1.3.2-1, the SEAF shall compute HRES\* from RES\* according to Annex A.5, and the SEAF shall compare HRES\* and HXRES\*. If they don’t coincide, then the SEAF shall consider the authentication as unsuccessful.

The SEAF shall proceed with step 10 in Figure 6.1.3.2-1 and after receiving the Nausf\_UEAuthentication\_Authenticate Response message from the AUSF in step 12in Figure 6.1.3.2-1, proceed as described below:

- If the AUSF has indicated in the Nausf\_UEAuthentication\_Authenticate Response message to the SEAF that the verification of the RES\* was not successful in the AUSF, or

- if the verification of the RES\* was not successful in the SEAF,

then the SEAF shall either reject the authentication by sending an Authentication Reject to the UE if the SUCI was used by the UE in the initial NAS message or the SEAF/AMF shall initiate an Identification procedure with the UE if the 5G-GUTI was used by the UE in the initial NAS message to retrieve the SUCI or if the reason was a network problem, e.g, 5G AV expiry, and an additional authentication attempt may be initiated. The SEAF/AMF may also initiate an additional authentication attempt if the authentication response from the AUSF was providing authentication failure due to a network problem, e.g., in case of 5G AV expiration or AUSF or UDM internal error.

Also, if the SEAF does not receive any Nausf\_UEAuthentication\_Authenticate Response message from the AUSF as expected, then the SEAF shall either reject the authentication to the UE or initiate an Identification procedure with the UE.

\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES