**3GPP TSG-SA3 Meeting #104-e *S3-212624***

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.535** | **CR** | **0094** | **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:***  | Correction to Deriving AKMA Application Key for a specific AF |
|  |  |
| ***Source to WG:*** | S3 |
| ***Source to TSG:*** | Huawei, HiSilicon |
|  |  |
| ***Work item code:*** | AKMA |  | ***Date:*** | 2021-08-09 |
|  |  |  |  |  |
| ***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:*** | In the procedure of deriving AKMA Application Key for a specific AF, it defines that if KAKMA is not present for the A-KID in the AAnF, the AAnF shall continue with step 4 with an error response. In this case, the AF shall reject the Application Session Establishment by including a failure cause and the UE may trigger a new Application Session Establishment request with the latest A-KID to the AKMA AF. There are at least two cases as follow which may cause the KAKMA not to be present for the A-KID in the AAnF:* The UE is not subscribed with AKMA service.
* The UE is subscribed with AKMA service, but the AKMA context between the UE and AAnF is out of sync due the re-authentication between the UE and 5GC.

For the first case, there is no need to trigger a new procedure for AKMA application key. For the second case, the new procedure is recommanded.Therefore, we propose to clarify the above cases. |
|  |  |
| ***Summary of change:*** | 1. When KAKMA is not present for the A-KID, the AAnF sends back the A-KID with failure cause.
2. Add the UE triggers the new procedure only when the A-KID is different from the lastest A-KID.
 |
|  |  |
| ***Consequences if not approved:*** | Unclear definition may cause signalling overhead and the UE may access AF with unnecessary delay. |
|  |  |
| ***Clauses affected:*** | 6.2 |
|  |  |
|  | **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 the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.2 Deriving AKMA Application Key for a specific AF

Figure 6.2-1 shows the procedure used by the AF to request application function specific AKMA keys from the AAnF, when the AF is located inside the operator's network.



Figure 6.2-1: KAF generation from KAKMA

Before communication between the UE and the AKMA AF can start, the UE and the AKMA AF needs to know whether to use AKMA. This knowledge is implicit to the specific application on the UE and the AKMA AF or indicated by the AKMA AF to the UE (see clause 6.5).

1. The UE shall generate the AKMA Anchor Key (KAKMA) and the A-KID from the KAUSF before initiating communication with an AKMA Application Function. When the UE initiates communication with the AKMA AF, it shall include the derived A-KID (see clause 6.1) in the Application Session Establishment Request message. UE may derive KAF before sending the message or afterwards.

2. If the AF does not have an active context associated with the A-KID, then the AF selects the AAnFas defined in clause 6.7, and sends a Naanf\_AKMA\_ApplicationKey\_Get request to AAnF with the A-KID to request the KAF for the UE. The AF also includes its identity (AF\_ID) in the request.

AF\_ID consists of the FQDN of the AF and the Ua\* security protocol identifier. The latter parameter identifies the security protocol that the AF will use with the UE.

The AAnF shall check whether the AAnF can provide the service to the AF based on the configured local policy or based on the authorization information or policy provided by the NRF using the AF\_ID. If it succeeds, the following procedures are executed. Otherwise, the AAnF shall reject the procedure.

The AAnF shall verify whether the subscriber is authorized to use AKMA based on the presence of the UE specific KAKMA key identified by the A-KID.

 If KAKMA is present in AAnF, the AAnF shall continue with step 3.

 If KAKMA is not present in the AAnF, the AAnF shall continue with step 4 with an error response.

3. The AAnF derives the AKMA Application Key (KAF) from KAKMA if it does not already have KAF.

 The key derivation of KAF shall be performed as specified in Annex A.4.

4. The AAnF sends Naanf\_AKMA\_ApplicationKey\_Get response to the AF with KAF and the KAF expiration time.

5. The AF sends the Application Session Establishment Response to the UE. If the information in step 4 indicates failure of AKMA key request, the AF shall reject the Application Session Establishment by including a failure cause. Afterwards, if the UE receives a failure casue, and the UE detects the Primary Authentication happened, and then a new A-KID is generated, UE triggers a new Application Session Establishment request with the newA-KID to the AKMA AF. Otherwise, the UE terminates the procedure.

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