**3GPP TSG-SA3 Meeting #115 *draft\_S3-240449\_r1***

**Athens, Greece, 26 February - 1 March 2024**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.535** | **CR** | **0201** | **rev** | **-** | **Current version:** | **18.2.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)*** *on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | KAF re-keying after expiration triggered by AAnF |
|  |  |
| ***Source to WG:*** | ZTE Corporation |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | HN\_Auth |  | ***Date:*** | 2024-02-19 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-18 |
|  | *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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | According to 3GPP TS 33.535, KAF re-keying may be triggered by the AF when the lifetime of KAF expires. However, if a primary authentication does not take place, the KAUSF and KAKMA remain unchanged since the latest primary authentication, which results in the same KAF as before. In order to re-generate a new KAF after the lifetime of KAF expires, KAKMA shall be re-keyed by AAnF requesting UDM to trigger primary authentication. Therefore, AAnF needs to be aware of the KAF expiration time, so that it can determine whether to re-key KAKMA upon receiving the Naanf\_AKMA\_ApplicationKey\_Get request from AF. |
|  |  |
| ***Summary of change:*** | Adding the KAF expiration time to AKMA context and the operation of store KAF expiration time by AAnF. |
|  |  |
| ***Consequences if not approved:*** | After the lifetime of KAF expires, the re-generated KAF may be the same one as before. |
|  |  |
| ***Clauses affected:*** | 3.1, 6.2.1, 6.2.2, 6.3, 6.4.4 |
|  |  |
|  | **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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**AKMA subscription data:** The data in the home operator's network indicating whether or not the subscriber is allowed to use AKMA.

**AKMA context:** A set of parameters stored in AAnF, including SUPI, GPSI, KAKMA,A-KID and KAF expiration time.

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

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

### 6.2.1 AAnF response with UE Identity

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 need 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. The 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 AAnF as 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 (see Annex A.4). 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 available in the signalling (i.e., Oauth2.0 token). 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 6 with an error response.

3. Once receiving the request from the AF, if the AAnF determines this specific AF needs GPSI, according to its local policy, the AAnF sends a Nudm\_SDM\_Get Request to the UDM to fetch the GPSI of the UE. If the specific AF does not need GPSI, the AAnF shall continue with step 5.

4. The UDM responds with the GPSI of the UE. The AAnF shall store the received GPSI as part of UE’s AKMA context.

5. The AAnF derives the AKMA Application Key (KAF) from KAKMA if it does not already have KAF. The AAnF shall store the KAF expiration time as part of UE’s AKMA context.

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

6. The AAnF sends Naanf\_AKMA\_ApplicationKey\_Get response to the AF with SUPI/GPSI, KAF and the KAF expiration time. Whether to send SUPI or GPSI is determined by AAnF based on the local policy.

7. The AF sends the Application Session Establishment Response to the UE. If the information in step 6 indicates failure of AKMA key request, the AF shall reject the Application Session Establishment by including a failure cause. Afterwards, UE may trigger a new Application Session Establishment request with the latest A-KID to the AKMA AF.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.2.2 AAnF response without UE Identity

In some scenarios, anonymous user access to the AF is desirable (e.g., UE identification is not required at the AF). For allowing such anonymous user access to the AF, the procedure detailed in clause 6.2.1 of the present document is used with the following changes:

- in step 2, instead of Naanf\_AKMA\_ApplicationKey\_Get request, Naanf\_AKMA\_ApplicationKey\_AnonUser\_Get request is used by the AF; and

- in step 6, the AAnF sends Naanf\_AKMA\_ApplicationKey\_AnonUser\_Get response to the AF with KAF and the KAF expiration time. The AAnF shall store the KAF expiration time as part of UE’s AKMA context.

The A-KID functions as a temporary user identifier.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.3 AKMA Application Key request via NEF

Figure 6.3-1 shows the procedure used by the AF to request KAF from the AAnF via NEF, when the AF is located outside the operator's network.



Figure 6.3-1: AKMA Application Key request via NEF

1. When the AF is about to request AKMA Application Key for the UE from the AAnF, e.g. when UE initiates application session establishment request as in clause 6.2.1, the AF discovers the HPLMN of the UE based on the A-KID and sends the request towards the AAnF via NEF service API. The request shall include the A-KID and the AF\_ID and optionally UE Id not needed indication.

NOTE: In the case of architecture without CAPIF support, the AF is locally configured with the API termination points for the service. In the case of architecture with CAPIF support, the AF obtains the service API information from the CAPIF core function via the Availability of service APIs event notification or Service Discover Response as specified in TS 23.222 [5].

2. If the AF is authorized by the NEF to request KAF, including the authorization after verification of the AF\_ID in step 1, the NEF discovers and selects an AAnF as defined in clause 6.7.

3. The NEF sends a Naanf\_AKMA\_ApplicationKey\_Get request to the selected AAnF with the A-KID to request the KAF for the UE.

The AAnF shall process the request in the same way as specified in clause 6.2.1 with following changes:

If KAKMA is present in AAnF, the AAnF shall continue with step 4 in this clause.

If KAKMA is not present in the AAnF, the AAnF shall continue with step 5 in this clause with an error response.

4. The AAnF generates the KAF as specified in clause 6.2.1 and sends the response to the NEF with the KAF, the KAF expiration time (KAF exptime) and SUPI. The AAnF shall store the KAF expiration time as part of UE’s AKMA context.

5. The NEF forwards the response to the AF with the KAF, the KAF expiration time (KAF exptime) and optionally GPSI (external ID). Based on local policy, the NEF uses the Nudm\_SubscriberDataManagement service which is specified in TS 29.503[11] to translate SUPI to GPSI (external ID) and optionally include GPSI (external ID) in the response. If UE Id not needed indication is received in the incoming request, the NEF shall not provide the GPSI (external ID) to AF. The NEF shall not send the SUPI to the AF.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*