**3GPP TSG-SA3 Meeting #115 *draft\_S3-240915-r3***

Athens, Greece, 26th February - 1st March 2024 is revision of S3-240708 (merging S3-240365)

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.535** | **CR** | **0207** | **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:***  | AKMA roaming policy control in AAnF |
|  |  |
| ***Source to WG:*** | China Mobile, NDRE, Ministère Economie et Finances, National Technical Assistance, Nokia, OTD\_US, Security Service |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI18 |  | ***Date:*** | 2024-1-25 |
|  |  |  |  |  |
| ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | The following roaming requirement has been specified in TS 33.535(Rel-18):*“4.6.1 AKMA roaming requirements**- The home network shall be able to control whether its subscriber is authorized to use the service in the visited network.”*However, how does AAnF get UE’s roaming status in order to allow or deny AKMA service for the roaming subscriber has not been specified.  |
|  |  |
| ***Summary of change:*** | When AAnF receives the AKMA key request from AF,AAnF gets UE’s roaming status from UDM using the existing service Nudm\_EventExposure. |
|  |  |
| ***Consequences if not approved:*** | The AKMA roaming requirement cannot be implemented. |
|  |  |
| ***Clauses affected:*** | 6.1, 6.2.1, 6.3, 7.1.3, 7.3.2 |
|  |  |
|  | **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 1st CHANGE\*\*\*\*\*

## 6.1 Deriving AKMA key after primary authentication

There is no separate authentication of the UE to support AKMA functionality. Instead, AKMA reuses the 5G primary authentication procedure executed e.g. during the UE Registration to authenticate the UE. A successful 5G primary authentication results in KAUSF being stored at the AUSF and the UE. Figure 6.1-1 shows the procedure to derive KAKMA after a successful primary authentication.



Figure 6.1-1: Deriving KAKMA after primary authentication

1) During the primary authentication procedure, the AUSF interacts with the UDM in order to fetch authentication information such as subscription credentials (e.g. AKA Authentication vectors) and the authentication method using the Nudm\_UEAuthentication\_Get Request service operation.

2) In the response, the UDM may also indicate to the AUSF whether the AKMA Anchor key needs to be generated for the UE. If the AKMA indication is included, the UDM shall also include the RID of the UE.

3) If the AUSF receives the AKMA indication from the UDM, the AUSF shall store the KAUSF and generate the AKMA Anchor Key (KAKMA) and the A-KID from KAUSF after the primary authentication procedure is successfully completed.

The UE shall generate the AKMA Anchor Key (KAKMA) and the A-KID from the KAUSF before initiating communication with an AKMA Application Function.

4) After AKMA key material is generated, the AUSF selects the AAnF as defined in clause 6.7, and shall send the generated A-KID, KAKMA to the AAnF together with the SUPI of the UE using the Naanf\_AKMA\_KeyRegistration Request service operation. The AAnF shall store the latest information sent by the AUSF.

NOTE 1: The AUSF need not store any AKMA key material after delivery to the AAnF.

NOTE 1a: When re-authentication runs, the AUSF generates a new A-KID, and a new KAKMA and sends the new generated A-KID and KAKMA to the AAnF. After receiving the new generated A-KID and KAKMA, the AAnF deletes the old A-KID and KAKMA and stores the new generated A-KID and KAKMA.

5) The AAnF sends the response to the AUSF using the Naanf\_AKMA\_AnchorKey\_Register Response service operation.

A-KID identifies the KAKMA key of the UE.

A-KID shall be in NAI format as specified in clause 2.2 of IETF RFC 7542 [6], i.e. username@realm. The username part shall include the RID and the A-TID (AKMA Temporary UE Identifier), and the realm part shall include Home Network Identifier.

The A-TID shall be derived from KAUSF as specified in Annex A.3.

The AUSF shall use the RID received from the UDM as described in step 2 to derive A-KID.

NOTE 2: The chance of A-TID collision is not zero but practically low as the A-TID derivation is based on KDF specified in Annex B of TS 33.220 [4]. The detection of A-TID collision as well as potential handling of collision is not addressed in the present document.

KAKMA shall be derived from KAUSF as specified in Annex A.2. Since KAKMA and A-TID in A-KID are both derived from KAUSF based on primary authentication run, the KAKMA and A-KID can only be refreshed by a new successful primary authentication.

\*\*\*\*\*\*\*\*\*\*\*\* 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 shall subscribe to the UDM to be notified of the roaming status where the UE is currently attached using Nudm\_EventExposure\_Subscribe service.

6. The UDM shall sends the Nudm\_EventExposure\_Subscribe response to the AAnF with the information of roaming, newServingPlmn and accessType. Once the roaming status changes, the UDM shall send a notification to the AAnF about the updated roaming information. The AAnF stores the roaming, newServing PLMN(s) and accessType(s) information.

7. The AAnF checks the roaming status and local policy and determines whether to provide service to the UE. If yes, the AAnF derives the AKMA Application Key (KAF) from KAKMA if it does not already have KAF,

When UE is dual registered, the UE is treated as roaming if at least one of the newServing PLMN indicates the UE is roaming.

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

8. If the AAnF determines to provide AKMA service to the UE, 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.If the AAnF finds that roaming is not allowed, it shall respond the AF containing a failure indication that roaming is not allowed.

9. The AF sends the Application Session Establishment Response to the UE. If the information in step 8 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.3 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. Once receiving the request from the AF, AAnF shall request the UE RoamingStatusReport from UDM as specified in clause 6.2.1, step 5-6. If the AAnF determines to provide AKMA service to the UE, 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. If the AAnF finds that roaming is not allowed, it shall respond the AF containing a failure indication that roaming is not allowed.

5. The NEF forwards the response to the AF, the response contains the KAF, the KAF expiration time (KAF exptime) and optionally GPSI (external ID) or the failure indication of roaming not allowed. 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 3rd CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\* START OF 4th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.1.3 Naanf\_AKMA\_ApplicationKey\_Get service operation

**Service operation name:** Naanf\_AKMA\_ApplicationKey\_Get.

**Description:** The NF consumer requests AKMA Application Key and UE ID from the AAnF.

**Input, Required:** A-KID, AF\_ID

**Input, Optional:** None.

**Output, Required:** .

**Output, Optional:** KAF, KAF expiration time and SUPI or GPSI or failure indication.

\*\*\*\*\*\*\*\*\*\*\*\* END OF 4th CHANGE\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\* START OF 5th CHANGE\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.3.2 Nnef\_AKMA\_ApplicationKey\_Get service operation

**Service operation name:** Nnef\_AKMA\_ApplicationKey\_Get.

**Description:** The NF consumer requests the NEF to provide AF related key material.

**Input, Required:** A-KID, AF\_ID

**Input, Optional:** UEID not needed indication.

**Output, Required:**

**Output, Optional:** KAF, KAF expiration time, GPSI (external ID) or failure indication.

\*\*\*\*\*\*\*\*\*\*\*\* END OF 5th CHANGE\*\*\*\*\*\*\*\*\*\*