**3GPP TSG-SA3 Meeting #116 *S3-241824r1***

Jeju, South Korea, 20th - 24th May 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **0210** | **rev** | **-** | **Current version:** | **18.3.0** |  |
|  |
| *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:***  | AF disabling the encryption when roaming |
|  |  |
| ***Source to WG:*** | Nokia, Verizon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | AKMA |  | ***Date:*** | 2024-05-10 |
|  |  |  |  |  |
| ***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:*** | AKMA service disable notification is defined where it is mentioned that AF may stop the UE service when roaming.However, it is up to the AF. AF may stop the UE service or stop the security.  |
|  |  |
| ***Summary of change:*** | Add: Once the AKMA service disable (roaming) indication is received at the AF, the AF can disable the security.Add: AF is also informed about the roaming so that AF can take the decision to stop the AKMA service or the security.  |
|  |  |
| ***Consequences if not approved:*** | Unclear specification |
|  |  |
| ***Clauses affected:*** | 6.8, 6.2.1, 6.3, 7.1.3, 7.1.5, 7.1.6 |
|  |  |
|  | **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\*\*\*\*\*\*\*\*\*\*\*

## 6.8 Notification about AKMA service disabling

This procedure is used when the AKMA sessions have already been started (before roaming was detected), and as soon as PLMN change is detected at the AAnF, the AAnF may execute this procedure based on the roaming policy.



Figure 6.8.1-1: AAnF notification to AF about AKMA service disable

1. UE registers with a (H)PLMN.

2. UE is accessing the AF and key material is provided to AF as described in 6.2.1. While accessing the AAnF, AF may also provide the Notification URI.

3. UE is getting registered in a VPLMN and AAnF detects the PLMN change via the Nudm\_EventExposure\_Notification received from UDM.

4. AAnF determines if AF(s) have subscribed to receive notifications for AKMA service disabling and/or roaming policy is configured and restrict the AKMA access in the VPLMN; if yes, steps 6 and 7 are executed. Otherwise, steps 6 and 7 are skipped.

5. If AF(s) are determined at step 5, the AAnF shall send notifications to the subscribed AF(s) about AKMA roaming via Naanf\_AKMA\_ServiceDisableNotification with A-KID and VPLMN identifier(s).

7. The AF shall send the response and based on the notification and internal policy, the AF may stop the UE service, may stop the encryption, or may stop the security.

NOTE: By stopping the encryption (TLS 1.2) or security, LI interception will work in the VPLMN.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*NEXT CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 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. If AF wants to receive a notification for AKMA service disabling, the AF shall include AKMA service disable URI in the Naanf\_AKMA\_ApplicationKey\_Get request. Based on the AKMA service disable URI, the AAnF shall create an implicit subscription for the AF for the AAnF to later notify the AF about AKMA service disable as defined in 6.x. Implicit subscription has an expiration time set by operator policy.

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. Once receiving the request from the AF, the AAnF shall send a Nudm\_EventExposure\_Subscribe request to UDM with SUPI/GPSI to request the RoamingStatusReport from the UDM.

6. The UDM shall send the Nudm\_EventExposure\_Subscribe response to the AAnF with the information of roaming status.

NOTE: Later on, when the roaming status changes, the UDM also sends a notification to the AAnF about the updated roaming information.

7. Once the AAnF receives the roaming status from the UDM, it checks the 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. The AAnF shall store the KAF expiration time as part of UE’s AKMA context.

When UE is dual registered, the UE is treated as roaming if at least one of the serving PLMNs 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 ,the KAF expiration time and VPLMN identifier(s). 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.

If a VPLMN identifier is received, based on internal policy, the AF may stop the AKMA service, may stop the encryption, or may stop the security based on internal policy.\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*NEXT CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 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 roaming status report 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),SUPI and VPLMN identifier(s) . The AAnF shall store the KAF expiration time as part of UE’s AKMA context. 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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*NEXT CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 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:** Service Disable URI.

**Output, Required:** .

**Output, Optional:** KAF, KAF expiration time, SUPI or GPSI, VPLMN identifier(s) or failure indication.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*NEXT CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.1.5 Naanf\_AKMA\_ApplicationKey\_ AnonUser\_Getservice operation

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

**Description:** The NF consumer requests only the AKMA Application Key from the AAnF. This service is for allowing anonymous user access to the AF based on A-KID (i.e., UE identification is not required at the AF). The A-KID functions as a temporary user identifier.

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

**Input, Optional:** Service Disable URI.

**Output, Required:**

**Output, Optional:** KAF, KAF expiration time, VPLMN identifier(s), or failure indication.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*NEXT CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.1.6 Naanf\_AKMA\_ServiceDisableNotification service operation

**Service operation name:** Naanf\_AKMA\_ServiceDisableNotification

**Description:** AAnFnotifies the NF consumer about AKMA service disable

NOTE: The AF is implicitly subscribed to receive Naanf\_AKMA\_ServiceDisableNotification service operation.

**Input, Required:** A-KID

**Input, Optional:** None, VPLMN identifier(s)

**Output, Required:** None

**Output, Optional:** None

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