**3GPP TSG-SA3 Meeting #105-e *S3-214236-r1***

**e-meeting, 8 - 19 Novemeber 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.535** | **CR** | **0114** | **rev** | **-** | **Current version:** | **17.3.0** |  |
|  | | | | | | | | |
| *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:*** | AKMA service support for roaming UE | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | S3 | | | | | | | | | |
| ***Source to TSG:*** | Samsung | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA | | | | |  | ***Date:*** | | | 2021-11-18 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | | <Release> |
|  | *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:*** | | AKMA service support for the roaming UE is not covered in TS 33.535.  NOTE:      Roaming aspects are not considered in the present document. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The changes are as follows:   1. A new clause is introduced to define vAAnF as the anchor function in the VPLMN which function as a proxy between the AF and the AAnF in the home network of the UE 2. A new clause is introduced to add the requirements on the vAAnF 3. The UDM provides indication whether the AKMA service is supported if the UE is roaming   Clause 6.1, 6.2, 6.3 and 6.7 procedures are updated in order to include the roaming support in AKMA services for the UE | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The roaming aspects will remain unaddressed and it may lead to not using AKMA services in romaing for various use cases. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.1, 4.2.x (new), 4.4.0, 4.4.y, 4.5, 6.1, 6.2, 6.3, 6.7 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\***

## 4.1 Reference model

Figure 4.1-1 shows a fundamental network model of AKMA, as well as the interfaces between them.



Figure 4.1-1: Fundamental Network Model for AKMA

NOTE: Figure 4.1-1 shows the case where AAnF is deployed as a standalone function. Deployments can choose to collocate AAnF with AUSF or with NEF according to operators' deployment scenarios.

Figure 4.1-2 shows the AKMA architecture using the reference point representation.



 

Figure 4.1-2: AKMA Architecture in reference point representation for (a) internal AFs, (b) external AFs, (c) internal AFs (via vAAnF) and (d) external AFs (via vAAnF)

The AKMA service requires a new logical entity, called the AKMA Anchor Function (AAnF).

**\*\*\*\* 2nd Change \*\*\*\***

### 4.2.x vAAnF

The vAAnF is the anchor function in the VPLMN. The vAAnF relays the Naanf\_AKMA\_ApplicationKey\_Get request and response between the AF in the visited network and the AAnF in the UE’s home network.

**\*\*\*\* 3rd Change \*\*\*\***

## 4.4.0 General

The following security requirements are applicable to AKMA:

- AKMA shall reuse the same UE subscription and the same credentials used for 5G access.

- AKMA shall reuse the 5G primary authentication procedure and methods specified in TS 33.501 [2] for the sake of implicit authentication for AKMA services.

- The SBA interface between the AAnF and the AUSF shall be confidentiality, integrity and replay protected.

- The SBA interface between AAnF and AF/NEF shall be confidentiality, integrity and replay protected.

- The AKMA Application Key (KAF) shall be provided with a maximum lifetime.

**\*\*\*\* 4th Change \*\*\*\***

### 4.4.2 Requirements on AKMA Key Identifier (A-KID)

Requirements for AKMA Key Identifier (A-KID) are:

- A-KID shall be globally unique;

- A-KID shall be usable as a key identifier in protocols used in the reference point Ua\*;

- AKMA AF shall be able to identify the AAnF serving the UE from the A-KID.

AAnF shall be able to identify the serving network of the UE from the A-KID.

**\*\*\*\* 4A Change \*\*\*\***

### 4.4.y Requirements on the vAAnF

The requirements on the vAAnF are:

- vAAnF shall be able to function as a proxy between the visited AF and the AAnF in the home network of the UE.

- vAAnF shall be able to locate the AAnF in the home network of the UE and communicate with it over secure channel.

- vAAnF shall be able to validate that the visited AF is authorized to participate in AKMA.

**\*\*\*\* 5th Change \*\*\*\***

## 4.5 AKMA reference points

The AKMA architecture reuses the following reference point from the 5GC for the execution of the primary authentication procedure:

**N1:** Reference point between the UE and the AMF.

**N2:** Reference point between the (R)AN and the AMF.

**N12:** Reference point between AMF and AUSF.

**N13:** Reference point between the UDM and the AUSF.

**N33:** Reference point between NEF and an external AF.

The AKMA architecture defines the following reference points:

**N61**: Reference point between the AAnF and the AUSF.

**N62**: Reference point between the AAnF and an internal AF.

**N63**: Reference point between the AAnF and NEF.

**N64**: Reference point between the AAnF and vAAnF.

**Ua\***: Reference point between the UE and an AF.

NOTE: The reference point Ua\* carries the application protocol, which is secured using the key material agreed between UE and AAnF as a result of successful AKMA procedures.

**\*\*\*\* 6th 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 AKMA Anchor keys need to be generated for the UE and also indicate whether AKMA service is supported if the UE is roaming. If the AKMA Ind 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 AAnFas defined in clause 6.7, and shall send the generated A-KID, AKMA roaming support indication if received from the UDM and 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, serving network identifier (SN Id) of the UE’s serving PLMN 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 step2 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.

**\*\*\*\* 7th 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 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. 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.

In the case where UE has contacted an AF that is operated in another network than home network, then the visited AF may use vAAnF of the AF’s network to communicate with UE's home AAnF. The AF is locally configured with the API termination point as vAAnF, in the case where the AF cannot directly communicate with the AAnF in the UE’s home network. The vAAnF identifies the AAnF serving the UE from the A-KID, and forwards the Naanf\_AKMA\_ApplicationKey\_Get request to the AAnF with the A-KID and AF\_ID to request the KAF for the UE.

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.

If the AAnF receives the request from the vAAnF, then the AAnF checks whether AKMA roaming support indication is received for the UE before deriving the KAF.

4. The AAnF sends Naanf\_AKMA\_ApplicationKey\_Get response to the AF or to the vAAnF with KAF and the KAF expiration time. The AAnF sends the response to the vAAnF, only if it received the AKMA roaming support indication for the UE from the AUSF. Upon receiving the response, the vAAnF forwards it to the AF.

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, UE may trigger a new Application Session Establishment request with the latest A-KID to the AKMA AF.

**\*\*\*\* 8th 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, 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.

NOTE: In the case of architecture without CAPIF support, the AF is locally configured with the PLMN’s API termination points for the service. The AF discovers the VPLMN of the UE based on the SN Id in the A-KID.

2. If the AF is authorized by the NEF to request KAF, the NEF discovers and selects an AAnF as defined in clause 6.7.

In the case of architecture without CAPIF support and in the case where UE has contacted an AF that is operated in another network than home network, then the visited NEF may use vAAnF within its network to communicate with UE's home AAnF. The NEF utilize the NRF to discover the vAAnF instance(s) unless vAAnF information is available by other means, e.g. locally configured on the NEF.

3. The NEF forwards the KAF request to the selected AAnF or to the selected vAAnF.

If the NEF forwards the KAF request to the vAAnF, then the vAAnF identifies the AAnF serving the UE from the A-KID, and forwards the KAF request to the AAnF in the home network of the UE to request the KAF for the UE.

The AAnF shall process the request in the same way as specified in clause 6.2 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 and sends the response to the NEF or to the vAAnF with the KAF, the KAF expiration time (KAFexptime) and potentially other parameters.

The AAnF generates the KAF and sends the response to the vAAnF, only if it received the AKMA roaming support indication for the UE from the AUSF. Upon receiving the response, the vAAnF forwards it to the AF.

5. The NEF forwards the response to the AF.

Editor's Note: Whether other parameters are to be returned to the AF via NEF is FFS.

For lawful interception, in the case of architecture without CAPIF support, when the UE is in the VPLMN and the UE has contacted an AF that is operated in home network then the AAnF in the home network sends the derived KAF to the vAAnF in the VPLMN of the UE. The AAnF discovers the vAAnF based on the SN Id in the A-KID.

In the case of architecture with CAPIF support, the AF shall obtain 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]. In the case where UE has contacted an AF that is operated in another network than home network, then the visited AF shall obtain the N33 service API information of the UE’s home network from the CAPIF core function in the UE’s visited network via CAPIF-1e reference point, as specified in TS 23.222 [5]. The AF (API invoker) shall interact directly with the NEF in the UE’s home network via the N33 interface which implements the service specific aspects of CAPIF-2e reference points for the corresponding service API interactions of the NEF.

**\*\*\*\* 9th Change \*\*\*\***

## 6.7 AAnF Discovery and Selection

The NF consumer or the SCP performs AAnF discovery to discover an AAnF instance.

In the case of NF consumer-based discovery and selection, the following applies:

- Internal AFs, vAAnF and the NEF performs AAnF selection to discover an AAnF Instance that handles the AKMA request for the UE. The AF/NEF shall utilize the NRF to discover the AAnF instance(s) unless AAnF information is available by other means, e.g. locally configured on the AF/NEF.

- The AUSF performs AAnF selection to allocate an AAnF Instance to send the AKMA key material related to the UE. The AUSF shall utilize the NRF to discover the AAnF instance(s) unless AAnF information is available by other means, e.g. locally configured on the AUSF.

The AAnF selection functionality in NF consumer or in SCP should consider the following factor:

- the UE's Routing Indicator.

NOTE 1: The AF/NEF obtains the Routing Indicator as part of the A-KID in the AKMA request. The AUSF obtains the Routing Indicator within the Nudm\_UEAuthentication\_Get Response from the UDM.

Internal AFs, the NEF and the AUSF shall select the same AAnF set based on the UE’s Routing Indicator.

When the UE's Routing Indicator is set to its default value as defined in TS 23.003 [9], the AAnF NF consumer can select any AAnF instance within the home network of the UE.

NOTE 2: In scenarios where multiple sets of AAnFs are deployed, it is left up to implementation how to ensure that the AAnF NF consumers select an AAnF instance within the AAnF set the UE belongs to when the UE's Routing Indicator is set to its default value.

In the case of delegated discovery and selection in SCP, the AAnF NF consumer shall send all available factors to the SCP.

**\*\*\*\* End of changes \*\*\*\***