**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *S3-233405***

**Berlin, Germany, 22 -26 May 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.535** | **CR** | 0154 | **rev** |  | **Current version:** | **17.8.0** |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | AKMA phase 2 security enhancement |
|  |  |
| ***Source to WG:*** | China Mobile |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | AKMA\_Ph2 |  | ***Date:*** | 2023-05-30 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***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:*** | Adding AKMA R18 related feature |
|  |  |
| ***Summary of change:*** | AKMA R18 related feature |
|  |  |
| ***Consequences if not approved:*** | Incomplete feature |
|  |  |
| ***Clauses affected:*** | 4.1, 4.4, New clauses 4.X, 4.Y |
|  |  |
|  | **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:*** | Convert from the living document S3-233383 |

4 Architecture for AKMA

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 of HPLMN and (b) external AFs**

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

The AKMA Architecture in Figure 4.1-2 is applicable to both roaming scenario and non-roaming scenario:

- non-roaming: UE is in HPLMN and accessing an AF;

- roaming scenario#1: UE is in VPLMN and accessing an internal HPLMN AF;

- roaming scenario#2: UE is in VPLMN and accessing an internal VPLMN AF;

- roaming scenario#3: UE is in VPLMN and accessing an external AF in the Data Network.

4.2 Network elements

4.2.1 AAnF

The AAnF is the anchor function in the HPLMN. The AAnF stores the AKMA Anchor Key (KAKMA) and SUPI for AKMA service, which is received from the AUSF after the UE completes a successful 5G primary authentication. The AAnF also generates the key material to be used between the UE and the Application Function (AF) and maintains UE AKMA contexts. The AAnF sends SUPI of the UE to AF located inside the operator's network according to the AF request or sends to NEF.

4.2.2 AF

The AF is defined in TS 23.501 [3] with additional functions:

- AF with the AKMA service enabling requests for AKMA Application Key, called KAF, from the AAnF using A-KID.

- AF shall be authenticated and authorized by the operator network before providing the KAF to the AF.

- The AF located inside the operator's network performs the AAnF selection.

4.2.3 NEF

The NEF is defined in TS 23.501 [3] with additional functions:

- The NEF enables and authorizes the external AF assessing AKMA service and forwards the request towards the AAnF.

- The NEF performs the AAnF selection.

4.2.4 AUSF

The AUSF is defined in TS 23.501 [3] with additional functions:

- AUSF provides the SUPI and AKMA key material (A-KID,KAKMA) of the UE to the AAnF.

- AUSF performs the AAnF selection.

4.2.5 UDM

The UDM is defined in TS 23.501 [3] with the additional functions:

 - UDM stores AKMA subscription data of the subscriber.

4.3 AKMA Service Based Interfaces(SBIs)

4.3.0 General

The following interfaces are involved in AKMA network architecture:

**- Nnef:** Service-based interface exhibited by NEF.

**- Nudm:** Service-based interface exhibited by UDM.

NOTE 1: UDM services related to AKMA service are defined in TS 33.501 [2] clause 14.2.2.

**- Naanf:** Service-based interface exhibited by AAnF.

The AAnF interacts with the AUSF and the AF using Service-based Interfaces. When the AF is located in the operator's network, the AAnF shall use Service-Based Interface to communicate with the AF directly. When the AF is located outside the operator's network, the NEF shall be used to exchange the messages between the AF and the AAnF.

4.3.1 Void

4.4 Security requirements and principles for AKMA

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.

4.4.1 Requirements on Ua\* reference point

The Ua\* reference point is application specific. The generic requirements for Ua\* are:

- Ua\* protocol shall be able to carry AKMA Key Identifier (A-KID) .

- The UE and the AKMA AF shall be able to secure the reference point Ua\* using the AKMA Application Key derived from the AKMA Anchor Key.

NOTE 1: The exact method of securing the reference point Ua\* depends on the application protocol used over reference point Ua\*.

NOTE 2: Void

- The Ua\* protocol shall be able to handle the expiration of KAF.

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.

4.4.3 Requirements on the UE

The requirements on the UE are:

- Applications on the UE shall not be able to get access to KAKMA.

- An application on the UE shall only get the KAF keys related to specific AF Identifiers (AF\_IDs) that the application is authorized to get.

- An application on the UE shall not be able to get access to the KAF keys that belong to other applications.

NOTE: How these requirements are satisfied is out of scope of 3GPP.

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.

**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.

## 4.X Roaming

### 4.X.1 AKMA roaming requirements

- The roaming subscriber shall be able to utilize the AKMA feature provided by the home network.

- The home network shall be able to control whether its subscriber is authorized to use the service in the visited network.

## 4.Y Use of Authentication Proxy

### 4.Y.1 Architecture of using AP

An Authentication Proxy (AP) is a proxy which takes the role of an AF and delegates a group of Application Servers (ASs). It may reside between the UE and the AS as depicted in the figures below. The AP helps the ASs behind the AP to execute AKMA procedures to save the consumption of signalling resources and AAnF computing resources. It may also relieve the AS of security tasks. The use of an AP is fully compatible with the architecture specified in this document.

The AP can assure the ASs that the request is coming from an authorized subscriber of the MNO.



Figure 4.Y.1-1: Environment and reference points of AP when AP is internal



Figure 4.Y.1-2: Environment and reference points of AP when AP is external

If the Ua\* is HTTP based, the UE is configured with the FQDN of AS, and the AP is a reverse proxy to handle the communication between the UE and the AS. The AP takes the role of an AF. The AKMA Application Key (i.e. KAF), which is utilized between the UE and the AP, is derived based on the FQDN of the AS.

If the Ua\* is not HTTP based, it’s left to implementation, e.g., how the AP identifies the traffic towards corresponding AS may be pre-configured in the AP by the operator who deploys the AP.

### 4.Y.2 AP-AS reference point

The HTTP protocol is run over the AP-AS reference point.

Confidentiality and integrity protection can be provided for the reference point between the AP and the AS using NDS/IP mechanisms as specified in TS 33.210 [5]. For traffic between different security domains, the Za reference point shall be operated. For traffic inside a security domain, it is up to the operator to decide whether to deploy the Zb reference point.

### 4.Y.3 Example of using AP for TLS tunnels

When the TLS based protocol is used as Ua\* profile, the AP can be used to handle the TLS security relation with the UE and relieves the AS of this task. When an HTTPS request is destined towards an AS behind an AP, the AP terminates the TLS tunnel and performs UE authentication. The AP proxies the HTTP requests received from UE to one or many application servers. The AP may add an assertion of identity of the subscriber for use by the AS, when the AP forwards the request from the UE to the AS.



Figure 4.Y.3-1: Environment and reference points of AP for TLS tunnels when AP is internal



Figure 4.Y.3-2: Environment and reference points of AP for TLS tunnels when AP is external