**3GPP TSG-SA3 Meeting #100e *S3-201943-r1***

**e-meeting, 17 – 28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0023** | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Corrections and clarifications to clause 4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA | | | | |  | ***Date:*** | | | 05/08/2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Unnecessary and inconsistent specification text | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Unnecessary and inconsistent specification text corrected  Miscellanious editorial corrections or improvements | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear specification | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.1, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.3, 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 CHANGES \*\*\*\***

# 4 Architecture for Authentication and Key Management for Applications (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.

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

The AAnF is the anchor function in the HPLMN that generates the key material to be used between the UE and the Application Function (AF) and maintains UE AKMA contexts.

## 4.2 Network elements

### 4.2.1 AAnF

AAnF stores the AKMA Anchor Key (KAKMA) for AKMA service, which is received from the AUSF after the UE completes a successful 5G primary authentication.

### 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.

### 4.2.3 NEF

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

- NEF performs the AAnF selection.

### 4.2.4 AUSF

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

AUSF provides the AKMA Anchor Key (KAKMA) to the AAnF.

### 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 Interface description

### 4.3.0 General

The following interfaces are involved in AKMA network architecture:

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

**- Nausf:** Service-based interface exhibited by AUSF.

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

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

**- Naf:** Service-based interface exhibited by AF.

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 Reference point Ua\*

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.

## 4.4 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.

- AAnF's SBI interface to AUSF shall be confidentiality, integrity and replay protected.

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

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

NOTE: Roaming aspects are not considered in the present document.

### 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: Specifying Ua\* protocol identifier is not considered in the present document.

### 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 AAnF of the UE from the A-KID.

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