**3GPP TSG-SA3 Meeting #103-e *S3-211913***

**e-meeting, 17 - 28 May 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.535** | **CR** | **0081** | **rev** | **-** | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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 | **X** | ME | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | AKMA UE aspects | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA | | | | |  | ***Date:*** | | | 2021-05-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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:*** | | The existing specification does not include a lot of AKMA handling nor requirements on the UE side. As a result UE implementations may expose AKMA key material to unauthorized applications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Requirements for the UE side. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear specification. Applications in the UE could get AKMA keys used by other applications, and thereby making the use of AKMA insecure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.4.X (new clause) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* 1st CHANGE \*\*\*

## 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.

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.

- 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.X 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\_IDs (i.e., FQDN and Ua\* protocol identifier combinations) 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.

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