**3GPP TSG-SA3 Meeting #101-e *S3-202944***

**e-meeting, 9 – 20 November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.535** | **CR** | 0045 | **rev** | **-** | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *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 |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Corrections of clause 6.1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | CATT, ZTE | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA | | | | |  | ***Date:*** | | | 2020-10-26 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | AKMA keys have been divided into two types, the AKMA Anchor Key and AKMA Application Key .But the stated key is ambiguous in clause 6.1.  KAKMA and A-KID can be refreshed by a new successful primary authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clearly indicates the key mentioned in clause 6.1 should be AKMA anchor key.  Add A-KID can be refreshed by a new successful primary authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear specification description on clause 6.1. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\* START OF 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.

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 shall send the generated A-KID, 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 Routing Identifier 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.

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.

\*\*\*\*\*\*\*\*\*\* END OF CHANGE \*\*\*\*\*\*\*\*\*\*