**3GPP TSG-SA3 Meeting #105-e *S3-214234-r3***

e-meeting, 8 - 19 November 2021

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0113** | **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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification on AKMA Application Key retrieval | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | S3 | | | | | | | | | |
| ***Source to TSG:*** | Samsung | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA | | | | |  | ***Date:*** | | | 2021-10-21 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***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:*** | | If the KAF is generated for a particular AF ID and later if the KAF lifetime gets expire, then the AAnF should not consider any request from the AF with same A-KID to generate it, as the same key will get generated again at the AAnF. i.e. Once KAF lifetime is expired then the Key becomes invalid and should not be used further.  After KAF lifetime expiry, AF is expected to inform UE over Ua\* that key has expired and it should connect with it using new A-KID. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | * A NOTE is proposed in clause 6.4.2 to address the above specified issue and corresponding changes are captured in clause 5.2. * Clause 6.4.3 is updated to capture the AF behaviour, when it receives a KAF request after the lifetime expiry. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | AAnF response in above mentioned scenario remains unaddressed and creates ambiguity in AKMA Application key retrieval. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.1.1, 5.2, 6.4.2, 6.4.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | R3 includes merger of S3-213899 and partial merger of S3-213938 | | | | | | | | |

\*\*\* Start of Changes \*\*\*

### 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.

-

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

## 5.2 AKMA key lifetimes

The KAKMA and A-KID are valid until the next successful primary authentication is performed (implicit lifetime), in which case the KAKMA and A-KID are replaced.

AKMA Application Keys KAF shall use explicit lifetimes based on the operator's policy. The lifetime of KAF shall be sent by the AAnF as described in clauses 6.2 and 6.3. In case that a new AKMA Anchor Key KAKMA is established, the AKMA Application Key KAF can continue to be used When the KAF lifetime expires, a new AKMA Application Key is established based on the current AKMA Anchor Key KAKMA.

NOTE: When the KAF lifetime expire and the KAKMA does not change in AAnF, according to the Annex A.4, the AKMA Application Key which is established based on the current AKMA Anchor Key KAKMA is not a new one, then the AAnF rejects the key request from the AF.

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

### 6.4.2 KAF re-keying

The KAF re-keying depends on the lifetime of the KAF and may be trigged by the AF, which means that when a new KAKMA is derived, the KAF will not be re-keyed automatically.

When the lifetime of KAF expires, the AF shall reject UE’s access to the AF (to indicate the KAF expiry) and refresh the KAF as described in clause 6.4.3 based on its policy.

If the AF reject the UE’s access to the application due to expire of lifetime of KAF and KAF refresh using Ua\* protocol is not supported, then only if there has been a change of KAUSF (e.g., due to a successful run of primary authentication), the UE may re-try accessing the AF by using the A-KID derived from the new KAUSF.

NOTE: When the AAnF maintains the AF ID along with KAF lifetime and if the KAF lifetime expires, then the AAnF rejects the request for the KAF from the AF.

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

6.4.3 KAF refresh

Ua\* protocol may support refresh of KAF. If the Ua\* protocol supports refresh of KAF, the AF may refresh the KAF at any time using the Ua\* protocol.

If Ua\* protocol does not support refresh of KAF, the AF shall reject the UE’s access to the application, upon KAF lifetime expiry. KAF cannot be refreshed until next primary authentication.

\*\*\* End of Changes \*\*\*