**3GPP TSG-SA3 Meeting #115 *S3-240790-r1***

**Athens, February 26 - March 01, 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.535** | **CR** | **0209** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Routing indicator update issue in the A-KID construction procedure Release 18 (mirror) | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Xiaomi | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA\_Ph2 | | | | |  | ***Date:*** | | | 2024-2-05 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***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 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:*** | | In AKMA scenarios, the AF/NEF/AUSF needs to leverage the routing indicator (RID) in the A-KID to select the AAnF set.  According to clause 6.1 of TS 33.535, on the core network side, the AUSF constructs the A-KID during the primary authentication procedure. The AUSF discovers the target AAnF using the RID in the A-KID and sends the A-KID to the target AAnF.  Refering to clauses 6.1 and 6.2 of TS 33.535, UE should construct the A-KID based on the RID when the UE initiates the connection between UE and the AF.  As described in clause 4.20.2 of TS 23.502, the UDM can update the routing indicator (RID) for a specific UE by triggering the UE Parameters Udpate(UPU) procedure.  If the UDM updates the RID to the UE, the A-KID constructed by the UE is different from the one constructed during the primary authentication procedure.  In other words, while the AUSF selects AAnF1 based on RID1 which is used during the primary procedrue, the NEF/AF may select AAnF2 based on RID2 that is updated to the UE via UPU procedure. As a result, the NEF/AF will choose an AAnF that does not contain the UE's A-KID.  **The RID update issue is not handled by the O&M procedure. In clause 4.20.2 of TS 23.502, the following mechanism is used to handle the RID update issue.**  If the UE parameter update is performed due to "Routing Indicator update data" and the updated Routing Indicator value is not supported by the UDM where the AMF is currently registered, the UDM shall request the UE to re-register after updating the data.  Therefore, to mitigate the potential impacts on 5GS, and to ensure the NEF/AF selects the right AAnF, UE should leverage the RID that is used during the primary procedure to construct the A-KID. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The following sentence is updated to address the aforementioned RID update issue.  The UE shall generate the AKMA Anchor Key (KAKMA) and the A-KID from the KAUSF after the primary authentication procedure is successfully completed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | NEF/AF cannot select the right AAnF when the UDM updates the RID of the UE via the UPU procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1, 6.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 the 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 the AKMA Anchor key needs to be generated for the UE. If the AKMA indication is included, the UDM shall also include the RID of 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 selects the AAnF as defined in clause 6.7, and 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 RID and the A-TID (AKMA Temporary UE Identifier), and the realm part shall include Home Network Identifier.

NOTE X: If the UE parameter update is performed due to "Routing Indicator update data" and the updated Routing Indicator value is not supported by the AAnF that is located by the original RID, the UE parameter update is performed by requesting the UE to re-register after updating the data by reusing the mechanism defined in clause 4.20.2 of TS 23.502.

The A-TID shall be derived from KAUSF as specified in Annex A.3.

The AUSF shall use the RID received from the UDM as described in step 2 to derive A-KID.

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 the Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*