**3GPP TSG-SA3 Meeting #105-e *S3-214091r1***

e-meeting, 8 - 19 November 2021

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **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:***  |  |
|  |  |
| ***Source to WG:*** | Lenovo, Motorola Mobility |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** |  |
|  | *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 canbe 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 UE is roaming in a VPLMN, then the UE builds up a secure tunnel to an AF in the HPLMN and since the credentials used for the encryption are based on the 3GPP derived keys, the VPLMN must be able to perform LI. Further is cannot be implied that the AF is always in the VPLMN for roaming scenarios, for typical deployments it can be a 3rd party AF in a data network. |
|  |  |
| ***Summary of change:*** | The note on the raoming support is removed, the KAKMA key derivation procedure after primary authentication is enhanced to provide the SN name to the AAnF and the KAF generation procedure is enhanced that the AAnF detects whether the UE is roaming and whether a NF in the VPLMN is configured to retrieve the KAF for LI.  |
|  |  |
| ***Consequences if not approved:*** | Roaming is not supported and does not fulfil the LI requriement. |
|  |  |
| ***Clauses affected:*** | 4.4.0, 6.1, 6.2 |
|  |  |
|  | **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:*** |  |

First 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.

Next 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. If the AKMA Ind 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 AAnFas defined in clause 6.7, and shall send the generated A-KID , and KAKMA to the AAnF together with the SUPI of the UE and the SN name where the UE is located 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.

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 step2 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.

Next change

## 6.2 Deriving AKMA Application Key for a specific AF

Figure 6.2-1 shows the procedure used by the AF to request application function specific AKMA keys from the AAnF, when the AF is located inside the operator's network.



Figure 6.2-1: KAF generation from KAKMA

Before communication between the UE and the AKMA AF can start, the UE and the AKMA AF needs to know whether to use AKMA. This knowledge is implicit to the specific application on the UE and the AKMA AF or indicated by the AKMA AF to the UE (see clause 6.5).

1. The UE shall generate the AKMA Anchor Key (KAKMA) and the A-KID from the KAUSF before initiating communication with an AKMA Application Function. When the UE initiates communication with the AKMA AF, it shall include the derived A-KID (see clause 6.1) in the Application Session Establishment Request message. UE may derive KAF before sending the message or afterwards.

2. If the AF does not have an active context associated with the A-KID, then the AF selects the AAnFas defined in clause 6.7, and sends a Naanf\_AKMA\_ApplicationKey\_Get request to AAnF with the A-KID to request the KAF for the UE. The AF also includes its identity (AF\_ID) in the request.

AF\_ID consists of the FQDN of the AF and the Ua\* security protocol identifier. The latter parameter identifies the security protocol that the AF will use with the UE.

The AAnF shall check whether the AAnF can provide the service to the AF based on the configured local policy or based on the authorization information or policy provided by the NRF using the AF\_ID. If it succeeds, the following procedures are executed. Otherwise, the AAnF shall reject the procedure.

The AAnF shall verify whether the subscriber is authorized to use AKMA based on the presence of the UE specific KAKMA key identified by the A-KID.

 If KAKMA is present in AAnF, the AAnF shall continue with step 3.

 If KAKMA is not present in the AAnF, the AAnF shall continue with step 4 with an error response.

3. The AAnF derives the AKMA Application Key (KAF) from KAKMA if it does not already have KAF.

 The key derivation of KAF shall be performed as specified in Annex A.4.

 The AAnF detects based on the SN name that the UE is roaming and if the VPLMN has AKMA LI enhancements, then the AAnF provides the KAF and the KAF expiration time together with the SUPI of the UE to the NF for storing the AKMA LI context, e.g. an AAnF, in the VPLMN.

 VPLMN AKMA capabilities and policies may be configured in the AAnF and may be based on SLAs.

4. The AAnF sends Naanf\_AKMA\_ApplicationKey\_Get response to the AF with KAF and the KAF expiration time.

5. The AF sends the Application Session Establishment Response to the UE. If the information in step 4 indicates failure of AKMA key request, the AF shall reject the Application Session Establishment by including a failure cause. Afterwards, UE may trigger a new Application Session Establishment request with the latest A-KID to the AKMA AF.

End of changes