**3GPP TSG-SA3 Meeting #101-e *S3-203191-r1***

**e-meeting, 9th - 20th November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0052** | **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:*** | Sending UE identifier to the AKMA AF | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA | | | | |  | ***Date:*** | | | |  | | --- | | 2020-10-27 | |
|  |  | | | |  | |  | | |  |
| ***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:*** | | For the AKMA AF to identify the UE (e.g., for charging and/or service authorization purposes), a UE identifier needs to be provided to the AKMA AF. This capability is currently missing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Addition of optional capability for the AAnF to provide an UE identifier (either SUPI or GPSI) to the AKMA AF. The existing Editor’s Note on other parameters that are provided to the AKMA AF is deleted. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | AKMA AF not able to identify the UE, thus unable to provide service to the UE using AKMA. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1, 6.2, 6.3, 7 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS/TR 33.501 CR 0996 | | |
| ***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 changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 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 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.

6) Once the AKMA keying material is received, the AAnF may send a Nudm\_SDM\_Get Request to the UDM to fetch the GPSI of the UE.

7) The UDM responds with the GPSI of the UE. The AAnF shall store the received GPSI as part of UE’s AKMA context.

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 AKMA keys are derived from KAUSF based on primary authentication run, the AKMA keys 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.

2. If the AF does not have an active context associated with the A-KID, then the AF 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.

4. The AAnF sends Naanf\_AKMA\_ApplicationKey\_Get response to the AF with KAF, the KAF expiration time and optionally a UE identifier (UE ID). The UE identifier may be the SUPI or the GPSI (if available) of the UE as determined by the AAnF based on its local policy for the AF.

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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.3 AKMA Application Key request via NEF

Figure 6.3-1 shows the procedure used by the AF to request KAF from the AAnF via NEF, when the AF is located outside the operator's network.



Figure 6.3-1: AKMA Application Key request via NEF

1. When the AF is about to request AKMA Application Key for the UE from the AAnF, e.g. when UE initiates application session establishment request as in clause 6.2, the AF discovers the HPLMN of the UE based on the A-KID and sends the request towards the AAnF via NEF service API. The request shall include the A-KID and the AF ID.

NOTE: In the case of architecture without CAPIF support, the AF is locally configured with the API termination points for the service. In the case of architecture with CAPIF support, the AF obtains the service API information from the CAPIF core function via the Availability of service APIs event notification or Service Discover Response as specified in TS 23.222 [5].

2. If the AF is authorized by the NEF to request KAF, the NEF discovers and selects an AAnF based on local configuration or via NRF in the same way as the AF selects the AAnF in clause 6.2.

3. The NEF forwards the KAF request to the selected AAnF.

4. The AAnF generates the KAF as specified in clause 6.2 and sends the response to the NEF with the KAF, the KAF expiration time (KAF\_exptime) and optionally, if available, the GPSI of the UE. The AAnF shall not send the SUPI of the UE to the NEF.

5. The NEF forwards the response to the AF.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 7.1 Services provided by AAnF

### 7.1.1 General

The following table shows the AAnF Services and AAnF Service Operations.

Table 7.1.1-1: List of AAnF Services

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation  Semantics | Example Consumer(s) |
| Naanf\_AKMA | AnchorKey\_Register | Request/Response | AUSF |
| ApplicationKey\_Get | Request/Response | AF, NEF |

### 7.1.2 Naanf\_AKMA\_AnchorKey\_Register service operation

**Service operation name:** Naanf\_AKMA\_AnchorKey\_Register.

**Description:** The NF consumer requests the AAnF to store the AKMA related key material.

**Input, Required:** SUPI, A-KID, KAKMA.

**Input, Optional:** None.

**Output, Required:** None.

**Output, Optional:** None.

## 7.2 Void

## 7.3 Services provided by NEF

### 7.3.1 General

The NEF exposes AKMA Application Key derivation service to the requester NF.

The following table shows the NEF Services and NEF Service Operations related to AKMA service.

Table 7.1.1-1: List of AAnF Services

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation  Semantics | Example Consumer(s) |
| Nnef\_AKMA | ApplicationKey\_Get | Request/Response | AF |

### 7.3.2 Nnef\_AKMA\_ApplicationKey\_Getservice operation

**Service operation name:** Nnef\_AKMA\_ApplicationKey\_Get.

**Description:** The NF consumer requests the NEF to provide AF related key material.

**Input, Required:** A-KID, AF\_ID

**Input, Optional:** None.

**Output, Required:** KAF, KAF expiration time.

**Output, Optional:** GPSI of the UE.

## 7.4 Services provided by UDM

UDM services related to AKMA service are defined in TS 33.501 [2] clause 14.2.2.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*