**3GPP TSG-SA3 Meeting #100e *S3-202039-r1***

**e-meeting, 17 -28 August 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.535** | **CR** | **0034** | **rev** | **-** | **Current version:** | **16.0.0** |  |
|  |
| *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:***  | Several clarifications and editorials |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2020-08-07 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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 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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | The specification contains several points that need clarification or alignment between figures and text.  |
|  |  |
| ***Summary of change:*** | The following clarifications are proposed: - Clarifications on the description of the NEF in clause 4.2.3- Clarifications on the description of the AUSF in clause 4.2.4- Removed the authentication method examples and the expression "implict authentication" and referenced the primary authentication methods in TS 33.501 in clause 4.4. - A new requirement on Ua\* is added in clause 4.4.1 in order to align with the KAF refresh procedures clauses. The requirement states that the Ua\* protocol shall be able to handle KAF expiration.- Editorial corrections in clause 4.4.2- In clause 6.1, the figure was updated to show the optionality of the steps that the AUSF sends AKMA key material to the AAnF. The optionality is due to the AKMA indicator coming from the UDM. If there is no AKMA indicator the AUSF does not generate the A-KID and KAKMA and does not send anything to the AAnF.- In clause 6.1, step numbers were added both in the text and the figure and figure font was enlarged- In clause 6.1, the statement that the UE generates A-KID and KAKMA before initiating the AKMA session request is moved after step 3. - A new step 5 explanation is added to explain the last message exchange between the AAnF and the AUSF. - In clause 6.2 it is clarified in the step 1 that the UE generates A-KID and KAKMA before initiating the application session request.- In clause 6.2, step 2 the NEF is removed as a potential source of authorization policy since clause 6.2 is about internal AFs and NEF is not involved in the procedure. - In clause 6.2, the figure is updated to incorporate different corrections such as the AF\_ID, KAF exptime. Similar changes are reflected in the text.- In clause 6.3, the figure is updated to align with the same terms used other parts of the specification with respect to the AF\_ID, KAF expiration time. - The style of the heading of clause 6.5 is corrected in order for the heading to appear in the table of contents.  |
|  |  |
| ***Consequences if not approved:*** | Unclear specification |
|  |  |
| ***Clauses affected:*** | 4.2.3, 4.2.4, 4.4, 4.4.1, 4.4.2, 6.1, 6.2, 6.3, 6.5 |
|  |  |
|  | **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:*** |  |

\*\*\* 1st CHANGE\*\*\*

4.2.3 NEF

NEF is defined in TS 23.501 [3] with additional functions:

- NEF enables and authorizes the external AF assessing AKMA service and forwards the request towards the AAnF.

- NEF discovers and selects the AAnF.

\*\*\* 2nd CHANGE\*\*\*

### 4.2.4 AUSF

AUSF is defined in TS 23.501 [3] with additional functions:

- AUSF provides the SUPI and AKMA key material (A-KID, KAKMA) of the UE to the AAnF.

\*\*\* 3rd CHANGE\*\*\*

## 4.4 Security requirements and principles for AKMA

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 as defined in TS 33.501 [2]

 - 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. When the AKMA Application Key lifetime is expired, it shall be renegotiated.

NOTE: Roaming aspects are not considered in the present document.

\*\*\* 4th CHANGE\*\*\*

### 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.

- The Ua\* protocol shall be able to handle the expiration of KAF

\*\*\* 5th CHANGE\*\*\*

### 4.4.2 Requirements on AKMA Key Identifier (A-KID)

Requirements for AKMA Key Identifier (A-KID) are:

- A-KID shall be globally unique;

- A-KID shall be usable as a key identifier in protocols used in the reference point Ua\*;

- AKMA AF shall be able to identify the AAnF serving the UE from the A-KID.

\*\*\* 6th 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: Deriving AKMA root key 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.

 (step 1 in clause 6.2)

4. After AKMA key material is generated, the AUSF shall send the generated A-KID, and KAKMA to the AAnF together with the UE SUPI 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.

5. The AAnF sends the response to the AUSF using the Naanf\_AKMA\_KeyRegistration Response service operation.

A-KID identifies the KAKMA key of the UE from which other AKMA keys are derived.

A-KID shall be in NAI format as specified in clause 2.2 of IETF RFC 7542, i.e. username@realm. The username part includes 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 defined in clause 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.

The key derivation of KAKMA shall be performed using the key derivation function (KDF) specified in TS 33.220 [4]. KAKMA is computed (as per Annex A.2) as KAKMA=KDF (KAUSF, "AKMA", SUPI), where the key derivation parameters consist of a static string "AKMA", and SUPI.Since AKMA keys are based on KAUSF from primary authentication run, the AKMA keys can only be refreshed by running a fresh primary authentication.

\*\*\* 7th 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 5GC directly, when the AF is located in 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 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\_AFKey request to AAnF with the A-KID to request the AKMA Application Key for the UE. The AF also includes its identity (AF\_ID) in the request. The AAnF shall authorize AF. 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 succeeds, the following procedures are executed. Otherwise, the AAnF shall reject the procedure.

The AAnF can check whether the subscriber is authorized to use AKMA by the presence of the AKMA anchor key KAKMA that has been received from the AUSF.

If the AAnF is in possession of the AKMA Application Key (KAF), it responds to the AF with the KAF. If not, the AAnF shall check if it has the UE specific KAKMA key identified by the A-KID.

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

 If KAKMA is not available, the AAnF shall continue with step 4 and send an error response.

3. The AAnF derives the AKMA Application Key (KAF) from KAKMA.

 The key derivation of KAF shall be performed using the key derivation function (KDF) specified in TS 33.220 [4]. KAF is computed (as per clause A.4) as KAF=KDF (KAKMA, AF\_ID), where the AF\_ID is constructed as follows: AF\_ID = FQDN of the AF || Ua\* security protocol identifier. The Ua\* security protocol identifier is specified as Ua security protocol identifier in Annex H of TS 33.220 [4]. The key used for the derivation of KAF is KAKMA.

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

5. The AF response the Application Session Establishment request to the UE.

\*\*\* 8th CHANGE\*\*\*

## 6.3 AKMA Application Key request via NEF

Figure 6.3-1 shows the procedure used by the AF to request AKMA Application Key from 5GC 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 5GC, 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 5GC via NEF service API.

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 AKMA Application Key, the NEF discovers and selects an AAnF instance 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 AKMA Application Key request to the selected AAnF.

4. The AAnF generates the AKMA Application Key in clause 6.2 and sends the response to the NEF with the KAF, the KAF expiration time and potentially other parameters.

5. The NEF forwards the response to the AF.

Editor's Note: Whether other parameters are to be returned to the AF via NEF is FFS.

\*\*\* 9th CHANGE\*\*\*

## 6.5 Initiation of AKMA

In case when the UE does not know to use AKMA for a service, then the following procedure applies.



Figure 6.5-1: Initiation of AKMA

1. The UE may start communication over reference point Ua\* with the AF with or without any AKMA-related parameters.

2. If the AF requires the use of shared keys obtained by means of the AKMA, but the request from UE does not include AKMA-related parameters, the AF replies with an AKMA initiation message. The form of this initiation message may depend on the particular reference point Ua\*.

In case the UE knows to use AKMA for a service, then it directly initiates the procedure in clause 6.2.

\*\*\* END OF CHANGES\*\*\*