**3GPP TSG-SA3 Meeting # 90-LI *s3i230406***

**Prague, , th -**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **1** | **Current version:** | **18.4.0** |  |
|  |
| *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:***  | Clarifications for AKMA LI Stage 2 |
|  |  |
| ***Source to WG:*** |   |
| ***Source to TSG:*** |  |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** |  |
|  |  |  |  |  |
| ***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 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | The present text is somewhat unclear about handling of SUPI-based AFs vs non-SUPI-based AFs. The text gives expectence of finding a description for provisioning of SUPI-based AFs, while in reality, all AFs are always triggered. Provisioning would be possible for SUPI-based AFs, but is currently not in scope. |
|  |  |
| ***Summary of change:*** | Clarifying of provisioning/triggering handling and applicability as well as scope of present document. |
|  |  |
| ***Consequences if not approved:*** | Risk of incorrect implementations. |
|  |  |
| ***Clauses affected:*** | 7.15.3.1.2, 7.15.3.1.3.1, 7.15.3.1.3.2 |
|  |  |
|  | **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:*** | s3i230383 |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* BEGIN CHANGES \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.15.3 LI for specific services

#### 7.15.3.1 LI for general AKMA-based service

##### 7.15.3.1.1 Background

In the specific case of AKMA (see TS 33.535 [47]), the KSF of the general architecture described above corresponds to the AAnF (AKMA Anchor Function). The STF corresponds to the AKMA Application Function (AF), identified by an application identifier AKMA AF\_ID. Key requests from external AFs are routed to AAnF via the NEF.

An AKMA Anchor Key is provided to the AAnF and is referred to as KAKMA.The Anchor Key Identifier (A-KID) is used to identify the key KAKMA.  A-KID can by TS 33.535 [47] be assumed to be globally unique. The AAnF derives, from the anchor key, one or more application-dependent keys referred to as KAF and provides the same to the AF.

The A-KID (and the associated KAKMA) of a specific UE can be modified by running 5G primary authentication. The A-KID can also become invalid at the AAnF due to specific AKMA Context Removal request from some duly authorized NF.

##### 7.15.3.1.2 LI architecture



NOTE: If the AF is located outside the PLMN (not shown) the LI\_T2 and LI\_T3 interfaces are not used but LI\_X2 from IRI-POI in AAnF can still be used to provide IRI with key management information such as decryption keys via MDF2.

Figure 7.15.3.1-1: General AKMA LI Architecture

Table 7.15.3.1-1: Mapping functions between the general architecture and AKMA

|  |  |  |
| --- | --- | --- |
| Function in the general architecture of 7.15.2  | Corresponding AKMA function  | Reference |
| KSF | AAnF | TS 33.535 [47] clause 4.2.1 |
| STF | AF  | TS 33.535 [47] clause 4.2.2 |

The LIPF present in the ADMF provisions the IRI-POI present in the AAnF and the MDF2/MDF3 over LI\_X1 interfaces. The LIPF may interact with the SIRF (over LI\_SI) to find the correct instances of these functions. Depending on the warrant received from LEA, provisioning could be restricted to only specific services/AFs or could be general.

The LIPF also provisions IRI-TF and CC-TF present in the AAnF. The IRI-TF and CC-TF are capable of mapping AKMA key identifiers (A-KID) to/from SUPI. When a UE presents A-KID to the AAnF, via the AF, the IRI-TF and CC-TF present in the AAnF trigger the IRI-POI and CC-POI present in the AF respectively when LI is active on the SUPI associated with the A-KID.

The AAnF only provides xIRI comprising key management events (creation, modification, deletion, etc, of encryption keys), as well as cryptographic keys themselves (KAKMA and/or KAF) and key identifiers (A-KID). The AF can provide both xIRI and xCC. The xIRI from the AF can comprise both auxiliary security parameters (Ua\* security protocol parameters, see below) and any other application specific information as set out in the general case described in clause 7.15.2.

Providing decrypted xCC depends on details of the security protocol used between the target UE and AF. This protocol is in AKMA referred to as the Ua\* security protocol. Below, the generic term "Ua\* security protocol parameters" is used to denote the complete set of auxiliary security parameters, besides the AKMA-related key material itself, necessary to decrypt the application traffic.

EXAMPLE: The Ua\* security protocol can be a profile of TLS version 1.2.

NOTE: AFs making use of AKMA for security purposes provide various services/applications toward subscribers. Details of LI related to the specifics of such services/applications are outside the scope of the present document, Only LI for the AKMA key management service itself is described in the present clause.

3GPP-defined Ua\* security protocols and protocol identifiers are defined in annex B of TS 33.535 [47] and currently cross-reference protocols defined in TS 33.222 [49].

Table 7.15.3.1-2: Mapping xIRI between the general architecture and AKMA

|  |  |  |
| --- | --- | --- |
| IRI-parameter in the general architecture of 7.15.2  | Corresponding AKMA IRI  | Reference |
| KLI | KAKMA and/or KAF  | TS 33.535 [47] clause 6.1, 6.2 |
| Key identifier, KID | A-KID | TS 33.535 [47] clause 4.4.2 |
| auxiliary security parameters | Ua\* security protocol parameters | TS 33.535 [47] clause 4.4.1 |

##### 7.15.3.1.3 Target identities

###### 7.15.3.1.3.1 Provisioning

The LIPF present in the ADMF provisions the intercept information associated with the following target identity to the IRI-POI, IRI-TF and CC-TF present in the AAnF:

- SUPI.

Provisioning of AKMA AF, as an alternative to the triggering described in clause 7.15.3.1.3.2, could be possible for certain types of AFs. This is however service specific and outside the scope of the present document.

###### 7.15.3.1.3.2 Triggering

AFs making use of AKMA can use either SUPI or some other form of identifier as basis for providing their services. The AAnF maintains a mapping from valid AKMA key identifiers (A-KID) to the SUPI.

When the IRI-TF in the AAnF receives an A-KID, it shall use said mapping to determine whether or not to trigger the IRI-POI in the AF. Thus, this is done independently of the type of subscriber identifier used locally at the AF.

CC intercept and CC-TF behaviour is service specific and outside the scope of the present document. Non-service-specific CC intercept can be achieved as described in clause 7.15.3.1.8.

An initial trigger for a new Task shall be issued to POIs of AFs matching the scope of the warrant when an A-KID for a target is first created. Since all such AFs might not be known in advance, this triggering can alternatively be performed dynamically, when a previously unknown AF requests key material related to a specific A-KID, from the AAnF.

Each time the A-KID of a target changes (due to primary authentication), the TF shall issue a new Task to the AF POI containing the new A-KID.

##### 7.15.3.1.4 IRI events

The IRI-POI present in the AAnF shall generate xIRI when it detects the following specific events or information related to an LI target:

- Anchor key register: AAnF receives AKMA-related key material from AUSF. This event can occur each time a target UE performs successful primary authentication to 5GC and then overwrites previous AKMA parameters stored at the AAnF.

- AKMA application key get: AAnF receives request for AKMA-related key material from a network-internal AF, or, from a network-external AF (via NEF).

- Start of intercept with established AKMA key material: AAnF detects that interception is activated on a target UE that has already established AKMA key material.

- AKMA context removal: An NF requests AAnF to remove AKMA-related key material.

The conditions under which the IRI-POI present in the AF generates xIRI is application-specific, but shall include at least the following events relating to xIRI with auxiliary security parameter:

- Application key refresh: AF performs local KAF refresh with the target UE.

- Start of intercept with established AKMA application key: the AF detects that interception is activated on a target UE that already has an established KAF.

- Auxiliary security parameter establishment: establishment or update of "Ua\* security protocol parameters" between the UE and the AF (e.g. nonces, selected security algorithms, etc.).

- Application key removal: the AF terminates the connection and does not make further use of KAF.

##### 7.15.3.1.5 Common IRI parameters

All xIRI shall include at least the following information:

- Target identity.

- Additional identities associated with the target as observed by the IRI-POI.

NOTE: This applies mainly for the AF.

- Time stamp.

- Correlation information.

##### 7.15.3.1.6 Specific IRI parameters

Additionally, to the common IRI parameters, the following xIRI shall be provided by the IRI-POI of the AAnF for the specific IRI events.

The Anchor key register shall include:

- A-KID, Anchor key identity of the currently valid anchor key associated with the event, see TS 33.535 [47].

- The AKMA anchor key KAKMA itself as defined in TS 33.535 [47], unless LI has been provisioned only for specific services or specific AFs.

The AKMA application key get shall include:

- Type: internal or external AF.

- AKMA AF\_ID (Application Function Identity), of the requesting application function. AF\_ID has format
AF\_ID = FQDN of the AF || Ua\* security protocol identifier, as defined in TS 33.535 [47].

- A-KID.

- KAF, the Application Function specific key delivered to the requesting application function, as defined in TS 33.535 [47].

- KAF Expiration Time, the expiry time of KAF, as defined in TS 33.535 [47].

NOTE 1: If the TLS-based Ua\* security protocols of annex B in TS 33.535 [47] is used between a target UE and STF, it could likely be the case that KAF itself is insufficient as decryption key for xCC. Further key material only available as part of the "Ua\* security protocol parameters" element of xIRI obtained from the STF, see below, are then likely also needed.

- The Start of intercept with established AKMA key material shall include:A-KID (currently valid).

NOTE 2: While a new primary authentication overwrites old AKMA contexts (KAKMA and A-KID), the expiry time of earlier application specific keys (KAF), derived from an old AKMA context (with an old A-KID) could still lie in the future when the Start of intercept with established AKMA key material occurs.

- The AKMA anchor key KAKMA associated with currently valid A-KID, unless provisioning has been made service- or AF-specific.

- The set of all (AKMA AF\_ID, KAF, KAF Expiration Time)-tuples associated with the target and satisfying all of:

- Being available at AAnF,

- AF\_ID is within scope of previous LI-provisioning, and

- KAF Expiration Time has not yet been passed.

The AKMA context removal xIRI shall include:

- A-KID.

- NF identity, of the NF requesting the removal.

Additionally, to the common IRI parameters, the following xIRI shall be provided by the IRI-POI of an AF for the specific IRI events:

- Application key refresh:AKMA AF\_ID.

- A-KID.

- New KAF.

- The set of "Ua\* security protocol parameters", if updated alongside KAF.

- Start of intercept with established AKMA application key:The FQDN part of the AKMA AF\_ID.

NOTE 3: Since a given application function could have several parallel secured sessions with a target UE, the FQDN part of AF\_ID is reported separately, while details of each session, e.g. "Ua\* security protocol parameters", is reported in the information elements below.

- A-KID (currently valid).

- The set of all (A-KID, KAF, KAF expiry, "Ua\* security protocol parameters")-tuples where A-KID is associated with the target and satisfying all of:

- Being available in the AF and not having expired, and

- The "Ua\* security protocol parameters" are associated with the specific A-KID / KAF.

Auxiliary security parameter establishment:

- AKMA AF\_ID.

- A-KID associated with the "Ua\* security protocol parameters" being established or updated (i..e with KAF).

- KAF associated with the "Ua\* security protocol parameters" being established or updated.

- The actual set of "Ua\* security protocol parameters" associated with the event.

Application key removal:

- AKMA AF\_ID.

- A-KID.

- Cause (reason for removal, e.g. key expiration).

For both Start of intercept with established application key and Auxiliary security parameter establishment, if other cryptographic key material (besides KAF) is required to decrypt xCC, then it shall be ensured that all such key material is included as part of "Ua\* security protocol parameters".

EXAMPLE: One example when KAF alone is insufficient is when the Ua\* security protocol deploys a separate "base secret" (e.g. from a stand-alone Diffie-Hellman key exchange), which is used by UE/AF when producing traffic encryption keys. In such case, also this base secret is needed for decryption.

##### 7.15.3.1.7 Network topologies

The AAnF shall provide the IRI-POI, IRI-TF, and CC-TF functions, and the network-internal AF shall provide the IRI-POI function in the following network topology cases:

- Non-roaming case.

NOTE: Handling of AKMA-based services in the roaming case is currently not defined in TS 33.535 [47].

##### 7.15.3.1.8 Provision of CC

Since AKMA is a non-service specific framework, interception of (decrypted) xCC at an AF for AKMA-secured services is not specified in further detail as part of clause 7.15.3.1. Non-service specific intercept of encrypted UP traffic could in some cases however be accomplished by combining the IRI-intercept (in particular, intercepted key material) of clauses 7.15.3.1.3 to 7.15.3.1.6 with the general solution for network layer xCC-intercept at the UPF as defined in clause 6.2.3.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END ALL CHANGES \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*