**3GPP TSG-SA3 Meeting # 90-LI *s3i230409***

**Prague, , th -**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.128** | **CR** | **0551** | **rev** | **1** | **Current version:** | **17.9.0** |  |
|  |
| *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 3 R17 |
|  |  |
| ***Source to WG:*** | SA3LI (NDRE, Nokia, Nokia Shanghai Bell)  |
| ***Source to TSG:*** | SA3 |
|  |  |
| ***Work item code:*** | LI17 |  | ***Date:*** | 2023-06-27 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *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 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. |

Some missing or unclear provisioning/triggering steps.Some editorial fixes, e.g. "AKID" -> "A-KID". |
|  |  |
| ***Summary of change:*** | Changes to clarify provisioning/triggering applicability and handling as well as scope of present document. Editorials. |
|  |  |
| ***Consequences if not approved:*** | Risk of incorrect implementations. |
|  |  |
| ***Clauses affected:*** | 7.9.1.2, 7.9.1.4, 7.9.1.5 |
|  |  |
|  | **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:*** | s3i230384 |

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

## 7.9 LI for services encrypted by CSP-provided keys

### 7.9.1 LI for general AKMA-based service

#### 7.9.1.1 General

This clause describes basic IRI-intercept for a generic, encrypted service between a target UE and an application in the CSP network, making use of AKMA-provided cryptographic keys according to TS 33.535 [65].

#### 7.9.1.2 Provisioning over LI\_X1

##### 7.9.1.2.1 General

The IRI-POI in the AAnF (AKMA Anchor Function), the IRI-TF in the AAnF, and the MDF2 shall be provisioned.

Details of provisioning of an IRI-POI at a network internal AF (Application Function) making use of AKMA services of the AAnF is in general service specific and not part of the present clause. Generally, triggering, rather than provisioning, could in some cases be necessary for the AF. An application independent generic triggering mechanism is defined in clause 7.9.1.2.3.

Provisioning of CC-intercept at the AF is service specific and not covered in the present document.

##### 7.9.1.2.2 Provisioning of the IRI-POI and IRI-TF in AAnF

The IRI-POI and IRI-TF present in the AAnF are provisioned over LI\_X1 by the LIPF using the X1 protocol as described in clause 5.2.2.

The IRI-POI and IRI-TF in the AAnF shall support the following target identifier formats:

- SUPI, given in either SUPIIMSI or SUPINAI formats as defined in ETSI TS 103 120 [6] clause C.2.

Table 7.9.1.2-1 shows the minimum details of the LI\_X1 ActivateTask message used for provisioning the IRI-POI and IRI-TF in the AAnF.

Table 7.9.1.2-1: ActivateTask message for the IRI-POI and IRI-TF in the AAnF

|  |  |  |
| --- | --- | --- |
| ETSI TS 103 221-1 [7] field name | Description | M/C/O |
| XID | XID assigned by LIPF. | M |
| TargetIdentifiers | One of the target identifiers listed in the paragraph above. | M |
| DeliveryType | Set to "X2Only". | M |
| ListOfDIDs | Delivery endpoints for LI\_X2 for the IRI-POI in the AMF. These delivery endpoints are configured using the CreateDestination message as described in ETSI TS 103 221-1 [7] clause 6.3.1 prior to the task activation. | M |

##### 7.9.1.2.3 Triggering of the IRI-POI in AF

The IRI-POI present in the AF shall be triggered by the IRI-TF present in the AAnF over LI\_T2 using the X1 protocol as described in clause 5.2.2. This shall be done by sending an ActivateTask when the IRI-TF detects that the AF performs an AKMA application key get associated with a targeted A-KID. An AAnF can provide services for several different types of applications. Triggering could be service/application specific, which can effect whether or not certain conditional fields are included in the xIRI described in clause 7.9.1.4 below.

When the IRI-TF in the AAnF detects that an A-KID has been associated with a SUPI (see clause 7.9.1.3.2), it shall send an ActivateTask message to the IRI-POI present in the AF. The same shall apply if the AAnF detects that the A-KID of a target changes due to primary authentication. The ActivateTask message shall contain at least the following information.

NOTE: AFs providing services based on SUPI could, as an alternative to triggering, be directly provisioned by the LIPF as part of service-specific provisioning. This is however outside the scope of the present document.Table 7.9.1.2-2: ActivateTask message for triggering the IRI-POI in the AF

|  |  |  |
| --- | --- | --- |
| ETSI TS 103 221-1 [7] field name | Description | M/C/O |
| XID | Allocated by the IRI-TF as per ETSI TS 103 221-1 [7]. | M |
| TargetIdentifiers | A-KID associated with the AKMA Anchor Key (see table 7.9.1.3-3 below). | M |
| DeliveryType | Set to “X2Only”. | M |
| ListOfDIDs | Delivery endpoints for LI\_X2. These delivery endpoints shall be configured by the IRI-TF in the SMF using the CreateDestination message as described in ETSI TS 103 221-1 [7] clause 6.3.1 prior to first use. | M |
| implicitDeactivationAllowed | Shall be set to "True". | M |
| ProductID | Shall be set to the XID of the Task Object associated with the interception at the CC-TF. This value shall be used by the CC-POI in the UPF to fill the XID of X3 PDUs. | M |

Table 7.9.1.2-3: Target Identifier Types for LI\_T3

|  |  |  |  |
| --- | --- | --- | --- |
| Identifier type | Owner | ETSI TS 103 221-1 [7] TargetIdentifier type | Definition |
| A-KID | 3GPP | TargetIdentifierExtension / AKID | AKID (see XSD schema) |

When the IRI-POI present in the AF detects that a UE has requested the use of a targeted A-KID, it shall continue to generate xIRI events for that A-KID until it detects that the UE has requested the use of a different A-KID, at which point it shall implicitly deactivate the previous Task. In addition, the AAnF may at any time issue a DeactivateTask message against the Task, at which point the AF shall cease interception of the A-KID and remove the Task as per ETSI TS 103 221-1 [7] clause 6.2.3.

#### 7.9.1.3 Generation of xIRI at IRI-POI in AAnF over LI\_X2

##### 7.9.1.3.1 General

The IRI-POI present in the AAnF shall send the xIRIs over LI\_X2 for each of the events listed in TS 33.127 [5] clause 7.9.3.1, the details of which are described in the following clauses.

##### 7.9.1.3.2 AAnF Anchor Key Register

The IRI-POI in the AAnF shall generate an xIRI containing an AAnFAnchorKeyRegister record when the IRI-POI present in the AAnF detects reception of an AKMA-context, i.e. an (A-KID, KAKMA)-pair associated with a target, from the AUSF, see TS 33.535 [65] clause 7.1.2.

Table 7.9.1.3-1: AAnFAnchorKeyRegister record

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| aKID | AKMA Anchor Key Identifier (see TS 33.535 [65] clause 4.4.2). | M |
| SUPI | SUPI associated with the A-KID. | M |
| kAKMA | AKMA Anchor Key (see TS 33.535 [65] clause 5.1). Shall be included if availableNOTE: Whether kAKMA is included could also depend on whether provisioning is general or service specific. | C |

##### 7.9.1.3.3 AAnF AKMA application key get

The IRI-POI in the AAnF shall generate an xIRI containing an AAnFAKMAApplicationKeyGet record when the IRI-POI present in the AAnF detects an AKMA application key get from an AF (directly or via NEF), see TS 33.535 [65], clauses 7.1.3 and 7.3.1.

Table 7.9.1.3-2: AAnFKAKMAApplicationKeyGet record

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| Type | Indicates whether the AF requesting the key is internal to the network or external. | M |
| aKID | AKMA Anchor Key Identifier. | M |
| keyInfo | Key information for the requested derived AF-specific key (see table 7.9.1.3-3). | M |

Table 7.9.1.3-3: AFKeyInfo structure

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| aFID | AKMA AF identifier of the AF associated with the derived AF-specific key. | M |
| kAF | Derived AF-specific key (see TS 33.535 [65] clauses 5.1 and A.4). | M |
| kAFExpTime | Expiry time associated with the derived AF-specific key. | M |

##### 7.9.1.3.4 AAnF Start of intercept with established AKMA key material

The IRI-POI in the AAnF shall generate an xIRI containing an AAnFStartOfInterceptWithEstablishedAKMAKeyMaterial record when the IRI-POI present in the AAnF detects that interception is activated on a target UE that has already established AKMA key material.

Table 7.9.1.3-4: AAnFStartOfInterceptWithEstablishedAKMAKeyMaterial record

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| aKID | AKMA Anchor Key Identifier (currently valid). | M |
| kAKMA | AKMA Anchor Key associated with aKID. | C |
| aFKeyList | List of all available (aFID, kAF, kAFExpTime)-tuples which are available, have not expired and complies with provisioning. | C |

##### 7.9.1.3.5 AAnF AKMA context removal

The IRI-POI in the AAnF shall generate an xIRI containing an AAnFAKMAContextRemovalRecord when the IRI-POI present in the AAnF receives a request from an NF to delete AKMA context, see TS 33.535 [65] clause 7.1.4.

Table 7.9.1.3-5: AAnFAKMAContextRemovalRecord record

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| aKID | AKMA Anchor Key Identifier. | M |
| nFInstanceID | Identity of NF originating the request encoded as per TS 29.571 [17] clause 5.3.2. | M |

#### 7.9.1.4 Generation of xIRI at IRI-POI in AF over LI\_X2

##### 7.9.1.4.1 General

The IRI-POI present in the AF shall send the xIRIs over LI\_X2 for each of the events listed in TS 33.127 [5] clause 7.9.3.1, the details of which are described in the following clauses.

##### 7.9.1.4.2 AF Application key refresh

The IRI-POI in the AF shall generate an xIRI containing an AFAKMApplicationKeyRefresh record when the IRI-POI present in the AF detects that a KAF-key previously obtained from an AAnF is being locally refreshed by the Ua\* security protocol in use, see TS 33.535 [65] clause 6.4.3.

Table 7.9.1.4-1: AFAKMAApplicationKeyRefresh record

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| aFID | AKMA AF identifier. | M |
| aKID | AKMA Anchor Key Identifier. | M |
| kAF | New value of the AF-specific key, after refresh. | M |
| uaStarParams | Set of new Ua\* security protocol parameters associated with kAF, if updated. | C |

##### 7.9.1.4.3 AF Start of intercept with established AKMA application key

The IRI-POI in the AF shall generate an xIRI containing an AFStartOfInterceptWithEstablishedAKMAApplicationKey record when the IRI-POI present in the AF detects interception is being triggered on a target UE that has already established AKMA application key.

Table 7.9.1.4-2: AFStartOfInterceptWithEstablishedAKMAApplicationKey record

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| aFFQDN | FQDN-part of AKMA AF identifier. | M |
| aKID | AKMA Anchor Key Identifier. | M |
| kAFParamList | List of all available all AFSecurityParams (see table 7.9.1.4-3) which have not expired and where the Ua\* security protocol parameters corresponds to the set of security parameters used on the Ua\* security protocol instance associated with KAF, see TS 33.127 [5] clause 7.9.3.1.5.NOTE: At least one such tuple exists when this event occurs. | M |

Table 7.9.1.4-3: AFSecurityParams structure

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| aFID | AF identifier. | M |
| aKID | AKMA Anchor Key Identifier. | M |
| kAF | AKMA derived AF-specific key associated with aKID and Ua\* security protocol. | M |
| uaStarParams | Set of Ua\* security protocol parameters after complete establishment/update.NOTE: Generic and TLS 1.2 [66] specific formats are provided in Annex A. | M |

##### 7.9.1.4.4 AF Auxiliary security parameter establishment

The IRI-POI in the AF shall generate an xIRI containing an AFAuxiliarySecurityParameterEstablishment record when the IRI-POI present in the AF detects that security parameters for the Ua\* security protocol in use have been established with the target UE, or, when they have been updated without the associated AKMA application key having been refreshed according to clause 7.9.1.4.3.

Table 7.9.1.4-4: AFAuxiliarySecurityParameterEstablishment record

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| aFSecurityParams | Auxiliary security parameters established (see table 7.9.1.4-3). | M |

##### 7.9.1.4.5 AF Application key removal

The IRI-POI in the AF shall generate an xIRI containing an AFApplicationKeyRemoval record when the IRI-POI present in the AF detects that an AKMA-derived AF-specific key is deleted or otherwise decommissioned.

Table 7.9.1.4-5: AFApplicationKeyRemoval record

|  |  |  |
| --- | --- | --- |
| Field name | Value | M/C/O |
| aFID | AF identifier. | M |
| aKID | AKMA Anchor Key Identifier associated with removed key. | M |
| removalCause | Reason for the removal of the application key. | M |

#### 7.9.1.5 Generation of IRI over LI\_HI2

When an xIRI is received over LI\_X2 from the IRI-POI in the AAnF or AF, the MDF2 shall send the IRI message over LI\_HI2 without undue delay. The IRI message shall contain a copy of the relevant record received from LI\_X2. The record may be enriched by other information available at the MDF.

The timestamp field of the ETSI TS 102 232-1 [9] PSHeader structure shall be set to the time at which the AAnF/AF event was observed (i.e. the timestamp field of the xIRI).

Table 7.9.1.5-1 shows the IRI type (see ETSI TS 102 232-1 [9] clause 5.2.10) to be used for each record type.

Table 7.9.1.5-1: IRI type for AAnF originated messages

|  |  |
| --- | --- |
| Record type | IRI Type |
| AAnFAnchorKeyRegister | BEGIN |
| AAnFKAKMAApplicationKeyGet | CONTINUE |
| AAnFStartOfInterceptWithEstablishedAKMAKeyMaterial | BEGIN |
| AAnFAKMAContextRemovalRecord | END |

IRI messages associated with the same A-KID from the same AAnF shall be assigned the same CIN.

Table 7.9.1.5-2: IRI type for AF originated messages

|  |  |
| --- | --- |
| Record type | IRI Type |
| AFAKMAApplicationKeyGet | BEGIN |
| AFAKMAApplicationKeyRefresh | CONTINUE |
| AFStartOfInterceptWithEstablishedAKMAApplicationKey | BEGIN |
| AFAuxiliarySecurityParameterEstablishment | CONTINUE |
| AFApplicationKeyRemoval | END |

IRI messages associated with the same A-KID from the same AF shall be assigned the same CIN.

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