**3GPP SA3LI#88-e-a S3i230091**

**eMeeting; January 23-27, 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.127** | **CR** | **0195** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  | | | | | | | | |
| *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:*** | Corrections to the diagrams - Part II | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | SA3-LI (Nokia, Nokia Shanghai Bell) | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | LI18 | | | | |  | ***Date:*** | | | 2023-01-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | ***F*** |  | | | | | ***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 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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Based on a consensus reached at one of the meetingss, the IRI-POI and CC-POI, when present in the same Network Function, were shown to have an undefined internal interface between them unless either of the two POIs are triggered POIs. However, the rule was adopted only a few diagrams. Some of the diagrams where such an interface presentation was missed was corrected in another CR since the same figure had more errors. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Dotted line inferring an undefined internal interface is shown between the IRI-POI and CC-POI in the diagrams in which it was missed. Also, the missing LI\_MDF was added to three diagrams. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Those diagrams will not be aligned with the LI principles adopted in the other correct diagrams. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7.15.2, 7.15.3.1.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | S3i230015 | | | | | | | | |

### \*\* First Change \*\*

### 7.15.2 Architecture

Figure 7.15.2-1 shows the general LI architecture where an IRI-POI in the KSF provides the xIRIs that include key management related information such as the decryption keys to the MDF2 over the LI\_X2 interface. The STF can provide xIRI and xCC for the target's communication traffic, as described in more detail below. Figure 7.15.2-1 shows the case where STF is assumed to provide services based on 5G-native identifier, e.g. SUPI, enabling the STF to be provisioned over LI\_X1.



NOTE: If the STF is located outside the PLMN (not shown), the LI\_X2 from IRI-POI in KSF can be used to provide IRI with key management information such as decryption keys via MDF2.

Figure 7.15.2-1: General architecture, STF using 5G native identifiers.

If the STF instead provides services based on some other user identifier space, the STF POIs are assumed to be triggered by IRI-TF and CC-TF in the KSF, as shown in figure 7.15.2-2. The triggering is based on the KSF detecting requests from the STF for cryptographic keys associated with a target UE.When the key management service of the KSF is based on target specific key identifiers (KID) known both at KSF and STF, such KID can serve as basis for mapping STF-identifiers to 5G-native identifiers at the KSF. The IRI-TF or CC-TF present in the KSF send the triggers to the IRI-POI or CC-POI present in the STF to indicate that the communication traffic is that of a target. The IRI-POI and CC-POI are then enabled for delivery of xIRI and the xCC with communication traffic of the target in a decrypted form as laid out above.

Figure 7.15.2-2: General architecture, STF not relying on 5G native identifiers.

The IRI-POI present in the KSF is provisioned by the LIPF over LI\_X1 and is responsible for providing key management related information in the form of xIRI. The key management related information can comprise information about requesting, creating, changing, or deleting encryption keys, and most importantly, can comprise decryption keys. Such decryption keys are generically denoted KLI and may comprise one or more cryptographic keys.

The IRI-POI in the STF is responsible for providing xIRI with auxiliary security parameters necessary to decrypt xCC which has been encrypted using the keys provided by the KSF. In addition, application specific (not encryption related) xIRI for the target's communication traffic. In more detail, the auxiliary security parameters can typically include:

- Additional cryptographic keys.

- Selected protocols / cipher-suites / cryptographic algorithms for UE-STF traffic encryption.

- Parameters for key derivation (e.g. nonces).

- Other cryptographic state information (e.g. counters).

Similarly, the CC-POI in the STF is responsible for providing the xCC for the target's communicaiton traffic in a decrypted form.

The remainder of the present clause provides details of IRI-intercept and, as applicable, CC-intercept of specific services encrypted by CSP-provided keys.

### \*\* Next Change \*\*

##### 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.

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 |

### \*\* End of all Changes \*\*