**3GPP SA3LI#84e-b *S3i220122r1***

**eMeeting, 02-04 March 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.127** | **CR** | **0163** | **rev** | **1** | **Current version:** | **17.3.0** |  |
|  | | | | | | | | |
| *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:*** | TS 33.127 - Corrections and Editorial changes | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | SA3\_LI (UtimacoTS GmbH) | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | LI17 | | | | |  | ***Date:*** | | | 2022-02-23 |
|  |  | | | |  | |  | | |  |
| ***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 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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Mistakes and editorial errors were found. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Corrected mistakes and fixed editorial errors. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Specification will lack quality. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 5.4.17, 6.2.2.3, 6.2.3.1, 6.2.3.8, 6.3.1, 6.3.3.7, 7.2.1, 7.2.3.1, 7.2.3.6, 7.3.3.1, 7.3.3.2.1, 7.4.4.3, 7.4.6.2, 7.4.7.2.3, 7.4.7.3.1, 7.4.7.3.3, 7.4.7.4.8, 7.6.1, 7.8.1.1, 7.8.1.3.2, 7.8.2.1.2, 7.9.4.1, 7.10.1.1, 7.14.3, 7.15.1.2, 7.15.2, 7.15.3.1.7, 8.5, A.1.2, A.3.1, E.3.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | S3i220122 | | | | | | | | |

FIRST CHANGE

# 2 References

…

[50] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

NEXT CHANGE

### 5.4.17 Interface LI\_XEM1

The LI\_XEM1 interface is used by the LICF (proxied by the LIPF) to manage and control the activation state of the IEF(s) and ICF.

LI\_XEM1 interfaces shall support the use of ETSI TS 103 221-1 [8] for transport of XEM1 messages / information. However, the requirements specified in the present document shall apply regardless of generic default options specified in ETSI TS 103 221-1 [8].

NEXT CHANGE

#### 6.2.2.3 Identity privacy

TS 33.501 [9] defines the ability to prevent the SUPI being exposed over the 5G RAN through the use of SUCI. Where SUPI privacy is implemented by both the UDM and UE, the SUPI is not sent in the clear over the RAN. Therefore, AMF has to rely on the UDM to provide the SUPI as part of the registration procedure as defined in TS 33.501 [9].

If the AMF receives a SUCI from the UE then the AMF shall ensure for every registration (including re-registration) that SUPI has been provided by the UDM to the AMF and that the SUCI to SUPI mapping has been verified as defined in TS 33.501 [9]. This shall be performed regardless of whether the SUPI is a target of interception.

The AMF IRI-POI shall provide both the SUPI and the current SUCI in all applicable events defined in clause 6.2.2.4.

NEXT CHANGE

#### 6.2.3.1 Architecture

In the 5GC network, user plane functions are separated from the control plane functions. The SMF that handles control plane actions (e.g. establishing, modifying, deleting) for the PDU sessions shall include an IRI-POI that has the LI capability to generate the related xIRI. The UPF that handles the user plane data shall include a CC-POI that has the capability to duplicate the user plane packets from the PDU sessions based on the interception rules received from the SMF. Figure 6.2-4 shows the LI architecture for SMF/UPF based interception.



Figure 6.2-4: LI architecture showing LI at SMF/UPF

The LICF present in the ADMF receives the warrant from an LEA, derives the intercept information from the warrant and provides it to the LIPF.

The LIPF present in the ADMF provisions IRI-POI (present in the SMF), MDF2 and MDF3 over the LI\_X1 interfaces. To enable the interception of the target's user plane packets (e.g. when the warrant requires the interception of communication contents), the CC-TF present in the SMF is also provisioned with the intercept data.

NOTE 1: The IRI-POI and CC-TF represented in figure 6.2-4 are logical functions and require correlation information be shared between them; they may be handled by the same process within the SMF.

The LIPF may interact with the SIRF (over LI\_SI) present in the NRF to discover the SMFs and UPFs in the network. The IRI-POI present in the SMF detects the PDU session establishment, modification, and deletion related events, generates and delivers the related xIRI to the MDF2 over LI\_X2. The MDF2 delivers the IRI messages to the LEMF over LI\_HI2.

When interception of communication contents is required, the CC-TF present in the SMF sends a trigger to the CC-POI present in the UPF over the LI\_T3 interface. The CC-POI in the UPF shall present itself as the same CC-POI to all the CC-TFs in the same SMF set, such that a CC-TF is capable of modifying or deactivating a task activated/modified in the CC-POI by a different CC-TF in the same SMF set.

The trigger sent from the CC-TF to CC-POI includes the following information:

- User plane packet detection rules.

- Target identity.

- Correlation information.

- MDF3 address.

NOTE 2: When LI\_T3 is used, the LI\_X1 between LIPF and CC-POI present in the UPF is used to monitor the user plane data.

The CC-POI present in the UPF generates the xCC from the user plane packets and delivers the xCC (that includes the correlation number and the target identity) to the MDF3. The MDF3 delivers the CC to the LEMF over LI\_HI3.

A warrant that does not require the interception of communication contents, may require IRI messages that have to be derived from the user plane packets. To support the generation of related xIRI (i.e. that requires access to the user plane packets), the present document supports two implementation approaches as described in clause 7.12.2. When approach 1 from clause 7.12.2 is used, the IRI-POI in the UPF shall present itself as the same IRI-POI to all the IRI-TFs in the same SMF set, such that an IRI-TF is capable of modifying or deactivating a task activated/modified in the IRI-POI by a different IRI-TF in the same SMF set.

Clause 8.6.2 defines a CC-PAG (CC-POI Aggregator) as an architectural extension option that is located between the MDF3 and CC-POI and performs the function of aggregating the xCC from different CC-POIs towards the MDF3.

NEXT CHANGE

#### 6.2.3.8 LI state transfers in SMF sets

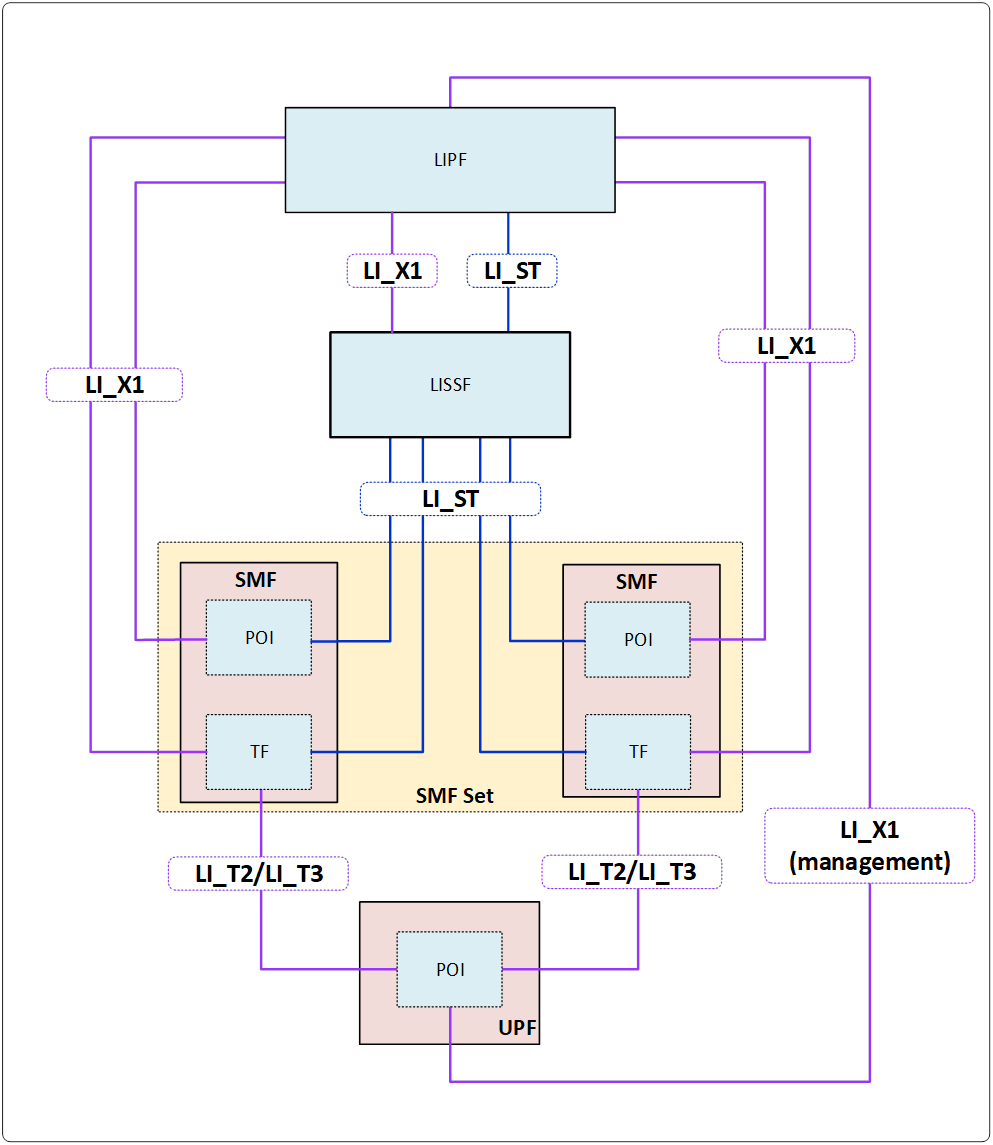


Figure 6.2-4A: LI architecture diagram for SMF/UPF interception when using SMF sets and LISSF

If an SMF belongs to an SMF set, then the TF present in the SMF shall have the ability to modify or stop the interceptions in the POIs present in the UPF irrespective of which TF present in an SMF from that SMF set had previously initiated the interception. A TF in one SMF of an SMF set may initiate the interception at a POI present in the UPF, the TF present in another SMF of the SMF set may make changes to the interception in that POI, and a TF in a different SMF of the SMF set may stop the interception in that POI.

In order to allow the TFs present in different SMFs of an SMF set to manage the interceptions at the POI present in an UPF, a new LI function referred to as LI State Storage Function (LISSF) is introduced. The TF that initiates the interception at a POI present in the UPF stores the related necessary information (e.g. correlation information) in case a different TF has to manage the interception at that POI. This necessary related information is referred to as LI state information (see TS 33.128 [15] for the details).

If an SMF belongs to an SMF set, then the POI present in the SMF shall have the ability to continue the interception using the same correlation information or stop the interception even when the SMF that manages the PDU session changes.

In order to allow the POIs present in different SMFs of an SMF set to continue the interception by maintaining a continuity, the LISSF mentioned above is used by storing the LI state information. When required, the POI present in the SMF of an SMF set stores the LI state information in the LISSF. The POI present in another SMF of the same SMF can retrieve the LI state information from that LISSF to provide a continued interception.

When an SMF in an SMF set requests SM context information related to a target from a UDSF or receives SM context information from another SMF, the TF and POI within the SMF shall retrieve also the relevant LI state information from the shared LISSF.

If the implementation of the SMF set does not ensure that active SM contexts are always present in some SMF of the SMF set, the TF shall also retrieve the relevant LI state information when an existing task is deactivated by the LIPF.

NOTE: The race conditions between the LI\_X1, LI\_ST operations, and network events are possible and need to be accounted for in the implementation.

NEXT CHANGE

### 6.3.1 General

The present document specifies three options for EPC interception capabilities:

- Option A. Perform LI on the events specified in the current document in clauses 6.3.2.3.1, 6.3.3.3 and 6.3.4.3 using the capabilities specified below for stage 2 and in TS 33.128 [15] for stage 3.

- Option B. Perform LI on the events specified in TS 33.107 [11] clause 12 and clause 18.2.4 using the capabilities specified below in the present document for stage 2 and in TS 33.128 [15] for stage 3.

- Option C. Use TS 33.107 [11] and TS 33.108 [21] natively as defined in those documents.

For implementations that include EPS/5GS interworking, Option A shall be used.

NEXT CHANGE

#### 6.3.3.7 EPC-5GC Interworking via SMF+PGW-C and UPF+PGW-U

In the case of interworking between EPC and 5GC via combined nodes (e.g. SMF+PGW-C, UPF+PGW-U) as defined in TS 23.501 [2] clause 5.17, all of the requirements found in clause 6.2.3 (LI for SMF/UPF) and clause 6.3.3 (LI at the SGW/PGW) of the present document apply with the following modifications:

- PDN Connection context information present in the combined SMF+PGW-C shall be reported via the mechanisms defined in TS 33.128 [15] clause 6.2.3.

- User identifiers that are EPC specific but known in the combined SMF+PGW-C are reported as supplemental user IDs per TS 33.128 [15] clause 6.2.3.

NEXT CHANGE

## 6.4 3G/4G

For virtualised 4G implemenations from Release 15 onwards (including combined 4G / 5G scenarios), 4G shall be virtualised based on the architecture in clause 5.6. For such implementations the LI architecture for 4G / LTE shall be implemented using an ADMF as defined in the present document (including LIPF and LICF split). However, equivalent reference points as specified in TS 33.107 [11] shall be used where appropriate (e.g. X2 is equivalent to LI\_X2 in the present document and MDF is equivalent to MF/DF). Security and audit requirements as defined in clause 8 of the present document shall be applied to such 4G scenarios.

The present document does not specify further LI functionality for 3G / UMTS. LI capabilities for 3G / UMTS for this release are specified in TS 33.107 [11].

NEXT CHANGE

### 7.2.1 General

Clause 7.2 provides LI architecture and requirements for the CSP 3GPP subscriber database LI reporting. Central subscriber databases are common for all CSP network services, including both the network layer and the service layer. This clause 7.2 provides requirements for both user session related interception events and requirements for reporting of changes to the subscriber information held within the 3GPP subscriber databases, which may or may not be directly related to service usage.

NEXT CHANGE

#### 7.2.2.3 Identity privacy

TS 33.501 [9] defines the ability to prevent the SUPI being exposed over the 5G RAN through the use of SUCI. Where SUPI privacy is implemented by both the UDM and UE, the SUPI is not sent in the clear over the RAN. Therefore, the UDM shall ensure that the SUPI is provided to the serving AMF in both initial registration and re-registration procedures as defined in TS 33.501 [9].

NEXT CHANGE

#### 7.2.3.1 Architecture

The [HSS](https://en.wikipedia.org/wiki/Home_Subscriber_Server) contains the subscription-related information for all users served by the CSP. The HSS provides the support functions in the mobility management, session setup, user authentication and access authorization.

The HSS shall have LI capabilities to generate the xIRIs as described in clause 7.2.3.3. The present document specifies two options for HSS LI capabilities:

1. Use TS 33.107 [11] and TS 33.108 [21] natively as defined in those documents.

2. Use the capabilities specified below in the present document for stage 2 and in TS 33.128 [15] for stage 3.

Extending the generic LI architecture presented in clause 5, figure 7.2-2 below gives a reference point representation the LI architecture with HSS as a CP NF providing the IRI-POI functions.



Figure 7.2-2: LI architecture for LI at HSS

The LICF present in the ADMF receives the warrant from an LEA, derives the intercept information from the warrant and provides it to the LIPF.

The LIPF present in the ADMF provisions IRI-POI (over LI\_X1) present in the HSS and MDF2.

The IRI-POI present in the HSS detects the target UE's service area registration and subscription related functions, generates and delivers the xIRI to the MDF2 over LI\_X2. The MDF2 generates and delivers the IRI messages based on received xIRI to the LEMF over LI\_H2.

The HSS shall provide the IRI-POI functions independent of the services on which the interception is active.

When multiple intercepts are active, IRI-POI functions in the HSS may send one xIRI which can then be distributed to the LEMFs associated with those multiple intercepts from the MDF2.

NEXT CHANGE

#### 7.2.3.6 Network topologies

The HSS shall provide the IRI-POI functions in the following network topology cases:

- Non-roaming case.

-

NEXT CHANGE

#### 7.3.3.1 General

LALS provides lawful access to the target's location. LALS is based on the Location Services (LCS) capabilities defined in TS 23.271 [5], TS 23.273 [30] and inOMA MLP [6]. The 5G Core Network support of LCS is described in TS 23.501 [2] clause 4.4.4 and TS 23.502 [4] clause 4.13.5.

LALS shall adhere to the requirements in TS 33.126 [3] clauses 6.6 (Security) and 6.3 (Detect and Capture). The LCS supporting LALS shall be able to provide priority to LALS requests. The subscriber location privacy settings shall be overridden for LALS by setting the privacy override indicator to "override" in the LI LCS client profile in the GMLC (see TS 23.273 [30] clause 5.4.4).

For inbound roaming targets, the VPLMN LCS functional entities fulfilling LALS requests, by default, shall not communicate with the target's HPLMN, as it may cause detectability issues, but rather the GMLC shall be able to determine the serving AMF/MME from which it can acquire the inbound roaming target's location. Detectability issues may also exist when LALS is invoked for outbound roaming targets. This means by default, the GMLC shall refrain from performing the positioning of an outbound roaming target.

Depending on national requirements and LCS capabilities of the CSP, the location information provided by LALS may vary in location information types (mobile network cell ID, location shape and geo-coordinates, civic address, or a combination of those), in the set of additional location parameters (map data, motion state, speed, etc.), as well as in the accuracy of provided location information.

NOTE 1: The accuracy of positioning is, usually, a trade-off for the location acquisition delay. It also depends on other positioning technology specific factors.

The parameters controlling the LALS output are either delivered per warrant over the LI\_X1 interface from the ADMF to the LI-LCS Client, or to the Location Triggering Function (LTF, see clause 7.3.3.3), or are pre-configured in the LI-LCS Client. The LI-LCS Client is a special type of IRI-POI in the CSP network fulfilling the role of the LCS client for LALS purposes. As such, the LI-LCS client shall support all the requirements and interfaces in accordance with 3GPP TS 23.273 [30] for an LCS client.

NOTE 2: The LI-LCS Client profile at GMLC is to be provisioned and accessed by authorized personnel only. The mechanism of this functionality is outside the scope of the present document.

There are two types of the location interception defined in the present document: target positioning and triggered location.

Target positioning determines the target's location independently of the services used by the target.

Triggered location determines the LALS based location of the target when specific network or service events related to the target occur.

The warrant for target positioning and for triggered location of the same target may be independent of each other and may be overlapping in time or combined in a single intercept warrant by the LEA.

There may be multiple active LALS warrants from different LEAs at any given time.

NEXT CHANGE

##### 7.3.3.2.1 General

As required by TS 33.126 [3] R6.3 – 370, the location provision variants supported in the current document are immediate location and periodic location.

The LI-LCS client shall include an IRI-POI that has the LI capabilities to generate the target UE’s location related xIRI.

Figure 7.3-1 shows the architecture for LALS where the LI-LCS client provides the target's location and associated information towards the MDF2 over the LI\_X2 interface as per the ADMF request for target positioning delivered over LI\_X1 interface.



Figure 7.3-1: LALS model for target positioning

NOTE: The Le interface is specified in OMA MLP [6].

NEXT CHANGE

#### 7.3.3.3 Triggered location

The Triggered location is the capability of providing LALS based location information when specific network or service events related to the target occur. While IRI generated by the event that also triggers the LALS may have the location information included (in the form of cell ID), LALS may provide additional location parameters, such as the target geo-location, velocity, etc. (see TS 33.126 [3] R6.3 – 270). The triggered location reporting utilizes the immediate location variant.

The LALS triggered location architecture in figures 7.3-2 and 7.3-3 depicts the Location Triggering Function (LTF). The LTF is an IRI-TF and resides in the same NF (e.g. AMF) that has the IRI-POI or in an MDF2. The LTF is responsible for triggering the IRI-POI in the LI-LCS Client when a specific event related to the target is observed at the co-located IRI-POI or received at the MDF2 in which the LTF is residing.

Figure 7.3-2 depicts the architecture of Triggered Location for IRI acquisition and delivery for the case when the LTF is residing in the same NF that has the IRI-POI reporting IRI events for the target.



Figure 7.3-2: LALS model for triggered location (POI/LTF option)

NOTE 1: The IRI-POI and LTF represented in figure 7.3-2 are logical functions and require correlation information be shared between them; they may be handled by the same process within the NF.

Figure 7.3-3 depicts the architecture of triggered location acquisition and delivery for the case when the LTF is embedded into an MDF2.



Figure 7.3-3: LALS Model for triggered location (MDF/LTF option)

In case of triggered location, the LTF (present in either an NF hosting an IRI-POI or in a MDF2) is provisioned by the ADMF over LI\_X1 interface.

As part of this request, the ADMF provides the address for the LTF to reach the LI-LCS client for use on the LI\_T2 interface. The IRI-POI (s) or the MDF2 then arm the LTF(s).

The LTF triggers the LI-LCS client over the LI\_T2 interface.

The LALS result is delivered to MDF2 from the LI-LCS Client as xIRI over the LI\_X2 interface asynchronously with the associated IRI events delivered by the IRI-POI. To enable correlation between the LALS reports and the associated IRI events, the LTF shall include the correlation information of the IRI event, if provided by the IRI-POI, into the LI\_T2 trigger.

NOTE 2: The IRI events may contain the location information obtained by other means, e.g. NPLI. The LALS reports are augmenting that information with extra details and accuracy.

NEXT CHANGE

#### 7.4.4.3 Common CC parameters

For the delivery of intercepted media packets, the following information shall be passed from the CC-POI to the MDF3 in addition to the intercepted media packets:

- Target identity.

- Correlation identifier

- Time stamp.

- Direction (indicates media is from or to the target).

NEXT CHANGE

#### 7.4.6.2 IMS Network Functions providing the IRI-POI

The IMS Network Functions that handle the target side of the session provide the IRI-POI functions except when the alternate option is used for the non-local ID target. When the alternate option is used for the non-local ID target, the IMS network function that handles the session-leg of the local served user connected directly to the non-local ID target.

Table 7.4.6.2-1 below identifies the IMS Network Functions in providing the IRI-POI functions in a non-roaming case for various session scenarios.

Table 7.4.6.2-1: IMS Network Functions providing the IRI-POI functions (non-roaming case)

|  |  |  |
| --- | --- | --- |
| Session type/target type | Default | Alternative option |
| Normal sessions | S-CSCF | P-CSCF |
| SMS over IMS | S-CSCF | P-CSCF |
| Emergency sessions | E-CSCF | P-CSCF (NOTE 1) |
| SMS over IMS to emergency services | E-CSCF | P-CSCF (NOTE1) |
| Redirected sessions: intra-PLMN | S-CSCF | P-CSCF |
| Redirected sessions: inter-PLMN (CS domain) | S-CSCF | MGCF |
| Redirected sessions: inter-PLMN (IMS domain) | S-CSCF | IBCF |
| Conference (NOTE 2) | Conf-AS/MRFC | - |
| PTC | PTC-Server | - |
| Non-local ID in CS domain (NOTE 3, NOTE 3A) | MGCF | S-CSCF |
| Non-local ID in IMS domain (NOTE 3, NOTE 3A) | IBCF | S-CSCF |
| Non-local ID for SMS over IMS (NOTE 3) | S-CSCF | P-CSCF (NOTE 3A) |

NOTE 1: For originated emergency sessions (or SMS over IMS to emergency services centre) handled in the fixed networks, where S-CSCF is also part of an emergency session, the S-CSCF based IRI-POI as a deployment option may also be considered.

NOTE 2: A conference ID can also be a target. Conf-AS stands for conference AS (see NOTE 2 in clause 7.4.4.1). When a normal session is extended to a conference session, the IMS signalling functions that provide the IRI-POI functions prior to the conference may continue to provide the IRI-POI functions in addition to the conference AS/MRFC.

NOTE 3: Non-roaming means that the local served user is non-roaming.

NOTE 3A: The default/alternate option used when the target is non-local ID is mutually independent of default/alternate option used when the target is local served user.

Table 7.4.6.2-2 below identifies the IMS Network Functions in providing the IRI-POI functions in a roaming case for various session scenarios.

Table 7.4.6.2-2: IMS Network Functions providing the IRI-POI functions (roaming case)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Session type/target type | Local Breakout (LBO) | | | | Home Routed (HR) | | | |
| HPLMN | | VPLMN | | HPLMN | | VPLMN | |
| Default | Alternate Option | Default | Alternate  Option | Default | Alternate Option | Default | Alternate Option |
| Normal sessions | S-CSCF | IBCF | P-CSCF | - | S-CSCF | P-CSCF | N9HR/S8HR | - |
| SMS over IMS | S-CSCF | IBCF | P-CSCF | - | S-CSCF | P-CSCF | N9HR/S8HR | - |
| Emergency sessions/SMS over IMS | - | - | E-CSCF | P-CSCF | - | - | E-CSCF | P-CSCF |
| SMS over IMS to emergency services | - | - | E-CSCF | P-CSCF | - | - | E-CSCF | P-CSCF |
| Redirected sessions | S-CSCF | See table 7.4.6.2-3 | - | - | S-CSCF | See table 7.4.6.2-3 | - | - |
| Conference (NOTE 2) | Conf-AS/MRFC | - | - | - | Conf-AS/MRFC | - | - | - |
| PTC | PTC-Server | - | - | - | PTC-Server | - | - | - |
| Non-local ID (E.164) in CS domain (NOTE 3A, NOTE 4, NOTE 4A) | MGCF | S-CSCF | P-CSCF | IBCF (NOTE 4B) | MGCF | S-CSCF (NOTE 3A) | N9HR/S8HR | - |
| Non-local ID in SIP/IMS domain (NOTE 3A, NOTE 4, NOTE 4A) | IBCF | S-CSCF | P-CSCF | IBCF (NOTE 4B) | IBCF | S-CSCF (NOTE 3A) | N9HR/S8HR | - |
| Non-local ID for SMS over IMS (NOTE 4) | S-CSCF | IBCF | P-CSCF | - | S-CSCF | P-CSCF | N9HR/S8HR | - |

NOTE 4: For roaming, this means the local served user is roaming. Also, see NOTE 3.

NOTE 4A: The default/alternate options used in the HPLMN and default/alternate options used in the VPLMN are mutually independent.

NOTE 4B: This alternate option may be used only in the VPLMN for IMS sessions with home-routed media.

The interception capabilities for normal sessions as defined in tables 7.4.6.2-1 (non-roaming) and 7.4.6.2-2 (roaming) shall be used for the cases where the Conf-AS and the PTSC-Server are not under the control of CSP serving the warrant.

Table 7.4.6.2-3: Extension of table 7.4.6.2-2

|  |  |  |  |
| --- | --- | --- | --- |
| Session type/target type | | Local Breakout (LBO) | Home Routed (HR) |
| Redirected sessions: Intra-PLMN | Redirected-to party non-roaming | P-CSCF | P-CSCF |
| Redirected-to party is roaming | IBCF | P-CSCF |
| Redirected sessions Inter-PLMN | Redirected-to party in CS domain | MGCF | MGCF |
| Redirected-to party in IMS domain | IBCF | IBCF |

Table 7.4.6.2-3 shows the IMS Network Functions that provide the IRI-POI functions in the HPLMN for redirected sessions in a roaming case when the alternate option is used to provide the IRI-POI functions for the normal case.

NOTE 5: For the redirected do not answer related sessions, the IMS Network Functions that provide the IRI-POI functions prior to the redirection are as illustrated in table 7.4.6.2-2 (normal case) and after the redirection are as illustrated in table 7.4.6.2-3.

The IMS Network Functions that provide the IRI-POI for STIR/SHAKEN and RCD/eCNAM are listed in clause 7.14.2.

NEXT CHANGE

##### 7.4.7.2.3 S8HR LI Process

For the describing the S8HR LI process, the following terms apply:

- The packet data connection representing the IMS signalling channel referenced in clause 7.4.7.4.11 is referred to as IMS signalling bearer. This is also referred to as the default bearer and uses the QCI value of 5 GSMA IR.92 [26].

- The packet data connection representing the IMS media channel referenced in clause 7.4.7.4.11 is referred to as IMS media bearer. This is a dedicated bearer and uses the QCI value of 1 for voice media GSMA IR.92 [26].

- The IMS signalling bearer and IMS media bearers are on separate GTP tunnels but are linked.

The S8HR LI process follows the steps described in clause 7.4.7.4.11 with the following specific aspects that apply to S8HR:

- The LIPF configures the BBIFF-C present in the SGW-C to notify the LMISF-IRI whenever an IMS signalling bearer or an IMS media bearer is created, modified, or deleted for S8HR inbound roaming UEs (i.e. the UEs that use S8HR APN).

- The BBIFF-C present in the SGW-C notifies the LMISF-IRI whenever it detects that such an IMS signalling bearer or an IMS media bearer is created, modified, or deleted.

- When the LMISF-IRI detects that IMS voice media interception is required, the LMISF-IRI instructs the BBIFF-C present in the SGW-C to deliver the user plane packets from the related IMS voice media bearer to the LMISF-CC.

NOTE 1: The LMISF-IRI includes the target UE location (when required) in the xIRI based on the UE location that it receives within the messages that denote the creation, modification, or deletion of IMS signalling or media bearers.

NOTE 2: When a target UE is involved in more than one IMS session, the release of an IMS session will not result in the BBIFF-U stopping the delivery of the user plane packets from the IMS media bearer since the IMS media bearer may still be active for that target UE.

NEXT CHANGE

##### 7.4.7.3.1 Background

The term N9HR is used to denote the home-routed roaming architecture for Vo5GS UEs. Within the VPLMN with N9HR, the IMS signalling messages and media packets are carried over the GTP tunnel that corresponds to the PDU session established for the UE for IMS based services.

The IMS signalling packets and the media packets are on separate Quality of Service (QoS) Flows with specific 5QI values (5QI = 5 for IMS signalling and 5QI = 1 for voice GSMA NG.114 [27]). The H-SMF in the HPLMN assigns a separate QoS Flow Index (QFI) for IMS signalling related packets and IMS voice related packets. The UPF in the VPLMN can isolate the IMS signalling and media related packets from user plane packets based on the QFI value.

NEXT CHANGE

##### 7.4.7.3.3 N9HR LI Process

For the purposes of describing the N9HR LI process, the following terms apply:

- The packet data connection representing the IMS signalling channel referenced in clause 7.4.7.4.11 is referred to as PDU session with IMS signalling related QoS flow.

- The packet data connection representing the IMS media channel referenced in clause 7.4.7.4.11 is referred to as PDU session with IMS media related QoS flow.

The IMS signalling and the IMS voice media are on the same PDU session.

NOTE 1: The QoS flow associated with the IMS signalling related user plane packets have the 5QI value 5 GSMA NG.114 [27] and such user plane packets can be identified at the BBIFF-U in UPF with the assigned QFI value.

NOTE 2: The QoS flow associated with the IMS voice media related user plane packets have the 5QI value 1 GSMA NG.114 [27] and such user plane packets can be identified at the BBIFF-U in UPF with the assigned QFI value.

The N9HR LI process follows the steps described in clause 7.4.7.4.11 with the following specific aspects that apply to N9HR:

- The LIPF configures the BBIFF-C present in the SMF to notify the LMISF-IRI whenever a PDU session is created, modified, or deleted for inbounding roaming UEs with an N9HR DNN.

- The BBIFF-C present in the SMF notifies the LMISF-IRI whenever it detects that a PDU session is created, modified, or deleted for inbound roaming UEs with N9HR DNN. The UE location information and the PDU session ID is included in such notifications.

- When the LMISF-IRI determines that IMS voice media interception is required, the LMISF-IRI instructs the BBIFF-C present in the SMF with the PDU session information that the IMS voice media related user plane packets from that PDU session are to be delivered to LMISF-CC.

NOTE 3: The LMISF-IRI includes the target UE location (when required) in the xIRI based on the UE location that it receives within the messages that denote the creation, modification, or deletion of the PDU session.

NOTE 4: When a target UE is involved in more than one IMS session, the release of an IMS session will not result in the BBIFF-U stopping delivery of IMS media related user plane packets since the IMS media related QoS Flow may still be active within the PDU session.

NEXT CHANGE

##### 7.4.7.4.8 CC parameters

The CC parameters are the same as those defined for IMS sessions in the VPLMN with LBO as the roaming architecture. See clause 7.4.4.3 for details.

NEXT CHANGE

### 7.6.1 General

In the present clause, "PTC" will be used to reference events or services that occur in either of two different architectures unless specified otherwise, e.g., Mission Critical Push To Talk (MCPTT) or Push to talk over Cellular (PoC).

The following servers support PTC architecture:

- MCPTT servers (Including Common services core as defined in TS 23.280 [24]).

- PoC servers (Including Shared XDMS as defined in OMA-AD-PoC-V2\_1-20110802-A [25]).

The PTC server will be used to represent the MCPTT server or PoC server for group communication services.

If two or more different parties involved in a PTC communication are each a target of interception, each interception shall operate independently of the others and the results of each intercept shall be delivered to the respective LEMF in accordance with the applicable warrant.

NEXT CHANGE

#### 7.8.1.1 General

Functions for NIDD (Non-IP Data Delivery) may be used to handle Mobile Originated (MO) and Mobile Terminated (MT) communication for unstructured data (also referred to as Non-IP). Such delivery to an AF is accomplished by one of the following two mechanisms (See TS 23.501 [2] clause 5.31.5):

- Delivery using NEF.

- Delivery using UPF via a Point-to-Point (PtP) N6 tunnel.

If the subscription includes a "NEF Identity for NIDD" corresponding to the DNN and S-NSSAI information, then the SMF selects that NEF as the anchor of this PDU session, otherwise, the SMF selects a UPF as the anchor of this PDU session. If NEF is used, the NIDD traffic is forwarded by NEF to the AF. If UPF is used, the NIDD traffic is forwarded by UPF to the AF.

NIDD applies to non-roaming and roaming with home-routed roaming architecture.

NEXT CHANGE

##### 7.8.1.3.2 Delivery using UPF via a PtP N6 tunnel

In roaming scenario, the user traffic is exchanged with DoNAS between UE and AMF, over N11 interface between AMF and V-SMF, over N4 interface between V-SMF and V-UPF, over N9 between V-UPF and H-UPF and finally over PtP N6 tunnel between H-UPF and AF (figure 7.8-4).

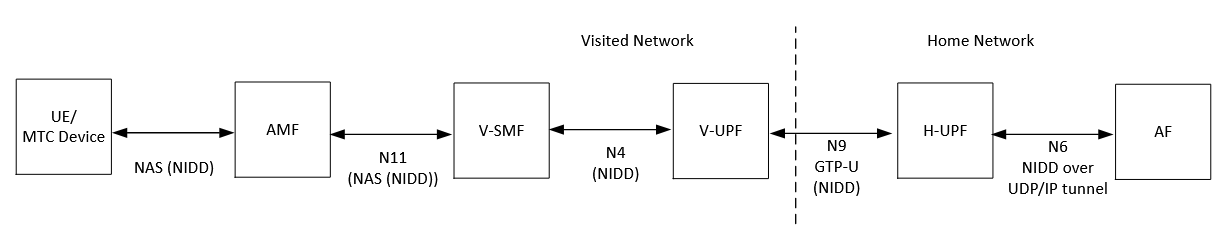


Figure 7.8-4: 5GS Architecture of NIDD using a PtP N6 tunnel in roaming situation

NEXT CHANGE

##### 7.8.2.1.2 Architecture for NIDD using NEF in the VPLMN

This clause describes the LI for NIDD using NEF in the VPLMN. The access method for the delivery of xCC related to NIDD using NEF is based on duplication of packets without modification of the packets at the V-SMF (in case of roaming) and NEF in the home network. The duplicated packets with additional information in a header are sent to MDF3 via LI\_X3 for further delivery to the LEMF via LI\_HI3. Figure 7.8-5 gives a reference point representation of the LI architecture with V-SMF as a CP NF and UP NF providing the IRI-POI and CC-POI functions for NIDD using NEF in the visited network.



Figure 7.8-5: LI architecture for NIDD using NEF showing LI at V-SMF

NEXT CHANGE

#### 7.9.4.1 Background

An MSISDN-less MO SMS is sent by a UE without MSISDN as originator and received by a third party application as destination (i.e. AF) via SMS-SC and NEF as presented in figure 7.9-3. MSISDN-less means that the GPSI of the UE is not an MSISDN but an External Identifier which form is username@realm. MSISDN-less MO-SMS service allows MSISDN-less UE to send small data to an AF using SMS-MO. The SMS-MO received by the SMS-SC through MO submission procedure as defined in TS 23.040 [50], is directly forwarded to the NEF for further transfer to the recipient AF (see TS 23.502 [4] clause 4.13.7 and TS 29.522 [31] clause 4.4.10).

The NEF queries the UDM with the SUPI of the UE, obtains the corresponding GPSI of the UE sending the SMS, and forwards it to the AF including the GPSI (i.e. external identifier) of the originating UE.



Figure 7.9-3: 5GS architecture for MSISDN-less MO SMS

NEXT CHANGE

#### 7.10.1.1 General

Functions for NIDD (Non-IP Data Delivery) may be used to handle Mobile Originated (MO) and Mobile Terminated (MT) communication for unstructured data (also referred to as Non-IP). Such delivery to the SCS/AS (Service Capability Server/ Application Server) is accomplished by one of the following two mechanisms as defined in TS 23.682 [33] clause 4.5.14:

- Delivery using SCEF.

- Delivery using a Point-to-Point (PtP) SGi tunnel.

If the subscription includes a "SCEF Identity for NIDD" corresponding with the APN information, then the MME selects that SCEF and uses the T6a interface to that SCEF, otherwise, the MME selects a SGW and PGW which handle this PDN connection. The PDN GW shares a SGi tunnel with the SCS/AS for the NIDD traffic exchange. If SCEF is used, the NIDD traffic is forwarded by SCEF to the SCS/AS.NIDD applies to non-roaming and roaming with home-routed roaming architecture.

NEXT CHANGE

#### 7.11.4.1 Background

An MSISDN-less MO SMS is sent by a UE without MSISDN as originator and received by a third party application as destination (i.e. SCS/AS) via SMS-SC and SCEF. MSISDN-less means that the UE has a subscription without MSISDN but an External Identifier which form is username@realm. MSISDN-less MO-SMS service allows MSISDN-less UE to send small data to an SCS/AS using SMS-MO. The SMS-MO received by the SMS-SC through MO submission procedure as defined in TS 23.040 [50], is directly forwarded to the SCEF for further transfer to the recipient SCS/AS (see TS 23.682 [33] clause 5.15).

The SCEF queries the HSS with the IMSI of the UE, obtains the corresponding External Identifier of the UE sending the SMS, and forwards the SMS to the SCS/AS including the External Identifier of the originating UE.



Figure 7.11-3: EPS architecture for MSISDN-less MO SMS

NEXT CHANGE

### 7.14.3 IRI events

The IRI-POI present in the IMS network functions listed in table 7.14.2-1 and 7.14.2-2 shall generate xIRI when it detects the following specific events or information:

- Signature generation.

- Signature validation.

The Signature generation xIRI is generated when the IRI-POI present in the Telephony AS for non-roaming UE or outbound roaming UE (HR) or in the egress IBCF detects that the Telephony AS or egress IBCF has sent a signing request (HTTP POST request) to the AS for signing and received a signing response (HTTP 200 OK) containing the Identity header. This interaction occurs when the Telephony AS or egress IBCF has received a SIP INVITE request or SIP MESSAGE request from a UE. The xIRI shall contain the identity token which also includes the signed RCD information if RCD is supported, and the initial caller number if changes occur on that number.

The Signature validation xIRI is generated when:

- The IRI-POI present in the Telephony AS or ingress IBCF has sent a verification request (HTTP POST request) containing the Identity token to the AS for verification and received a verification response (200 OK) containing the verification outcome (validation passed / validation failed / no validation). The xIRI shall contain the calling party identity, the identity token, the verification outcome, and the RCD or eCNAM related information if RCD or eCNAM is supported.

- The IRI-POI present in the P-CSCF for inbound roaming UE (LBO) or LMSIF-IRI for inbound roaming UE (HR) receives a SIP INVITE or a SIP MESSAGE request including appropriate SIP headers containing the verification outcome and RCS or eCNAM related information if RCS or eCNAM is supported.

These xIRIs should be correlated by MDF2 with the xIRIs related toIMS session establishment or SMS over IP delivery. The correlation identifier found in the STIR/SHAKEN xIRIs and IMS xIRIs should help the MDF2 performing the correlation procedure and generated IRIs with both sets of data for delivery to LEMF.

NEXT CHANGE

#### 7.15.1.2 LI requirements - overview

This clause specifies a common LI architecture for a general CSP-provided key management solution in support of encryption, implemented by generic KSF and STF functionality as defined in clause 7.15.1.1.

When encryption keys are provided by a CSP, lawful interception for a target's communication may be done in one of the two ways: (i) decrypt intercepted communication traffic before delivering IRIs and CCs to the LEA, or, (ii) provide to the LEA the decryption keys and other information necessary to enable the decryption of communication traffic. To fully enable decryption of communicaiton traffic, LI functions are in general required both at the KSF and at the STF as illustrated by the following examples.

EXAMPLE: In most situations, after STF has obtained encryption key from KSF, the STF has all the necessary information to decrypt the communication traffic without the additional help of KSF. In this situation, an LI function within the STF can decrypt the target's communication and does not need to provide, explicit encryption-related xIRI. However, the STF can also have access to xIRI which is not related to encryption, but which is still application specific, and which also can be of relevance to include as part of IRI.

EXAMPLE 2: In some situations, STF may not know whether communication traffic is that of a target since it could use a user identfier space which is independent from the 5G identifiers used for LI provisiong. In this situation, the LI function in KSF will have to provide intercept triggers to the LI function in the STF in order to identify the target communication traffic. Moreover, even if decrypted xCC is provided by the STF, the KSF can still typically report xIRI relating to key management (e.g. request for keys from other STFs, expiry of keys etc) which are of relevance for LI. For a third example of applicabity of LI at the KSF, refer to NOTE 3 below.

As mentioned, the physical/jurisdictional location of KSF and STF can differ depending on the scenario which can have bearing on LI requirements.

NOTE 1: When a warrant is served to a PLMN that has neither the STF nor the KSF, handling of LI aspects specifically related to the encrypted communication traffic of a target is outside the scope of the present document.

NOTE 2: For roaming situations, where LI providing unencrypted communication in the VPLMN is required, the STF would need to be located in the VPLMN and the STF would also need to use 5G native user identifiers which enable LI provisioning in the VPLMN (since LI can not rely on triggering from HPLMN in this case). However, such roaming scenarios are outside the scope of the present document.

NOTE 3: When a warrant is issued to a HPLMN that has the KSF, but not the STF, then the LI function in that KSF can still provide encryption related keys and related events to the LEMF. LI at the STF is however then outside the scope of the present document.

To summarize, with respect to the LI at KSF and STF, three specific type of xIRIs are identified:

1. xIRI from KSF consting of key managment information such as decryption keys and thereto related information.

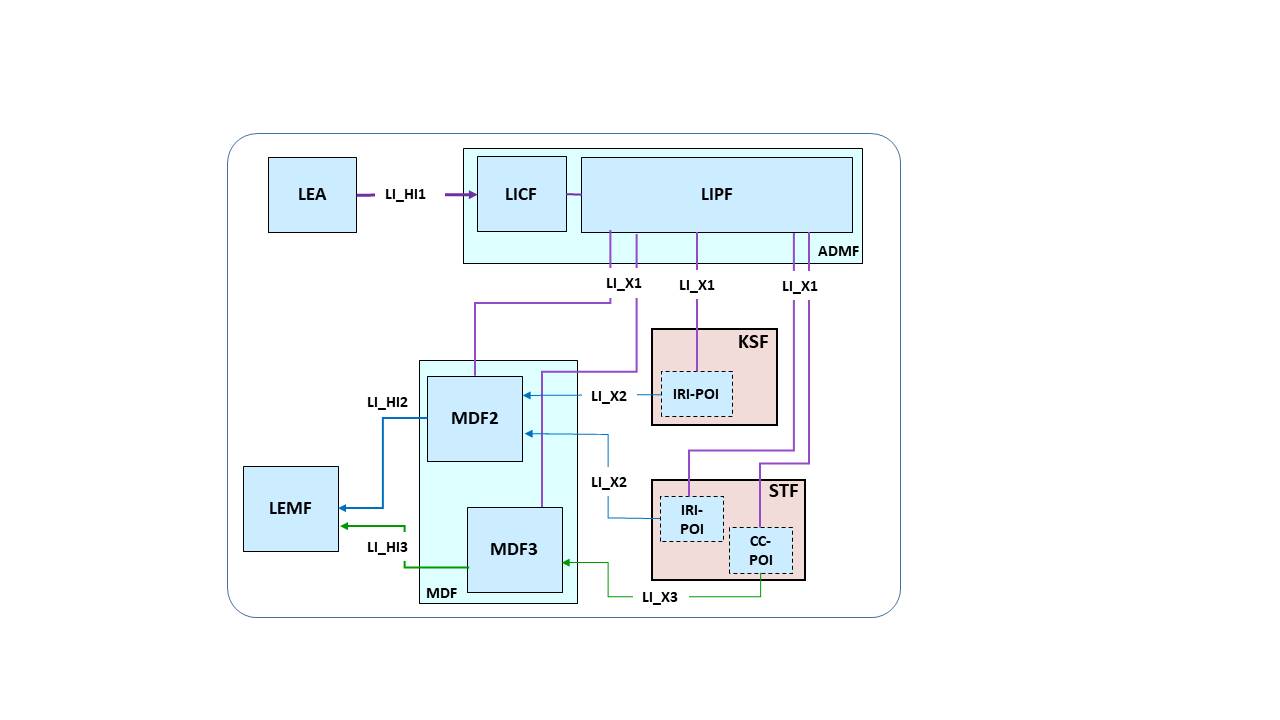
2. xIRI from STF consisting of other encryption related parameters, refered to as auxiliary security parameters.

3. xIRI from STF which are application specific but not pertaining to encryption.

NEXT 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.

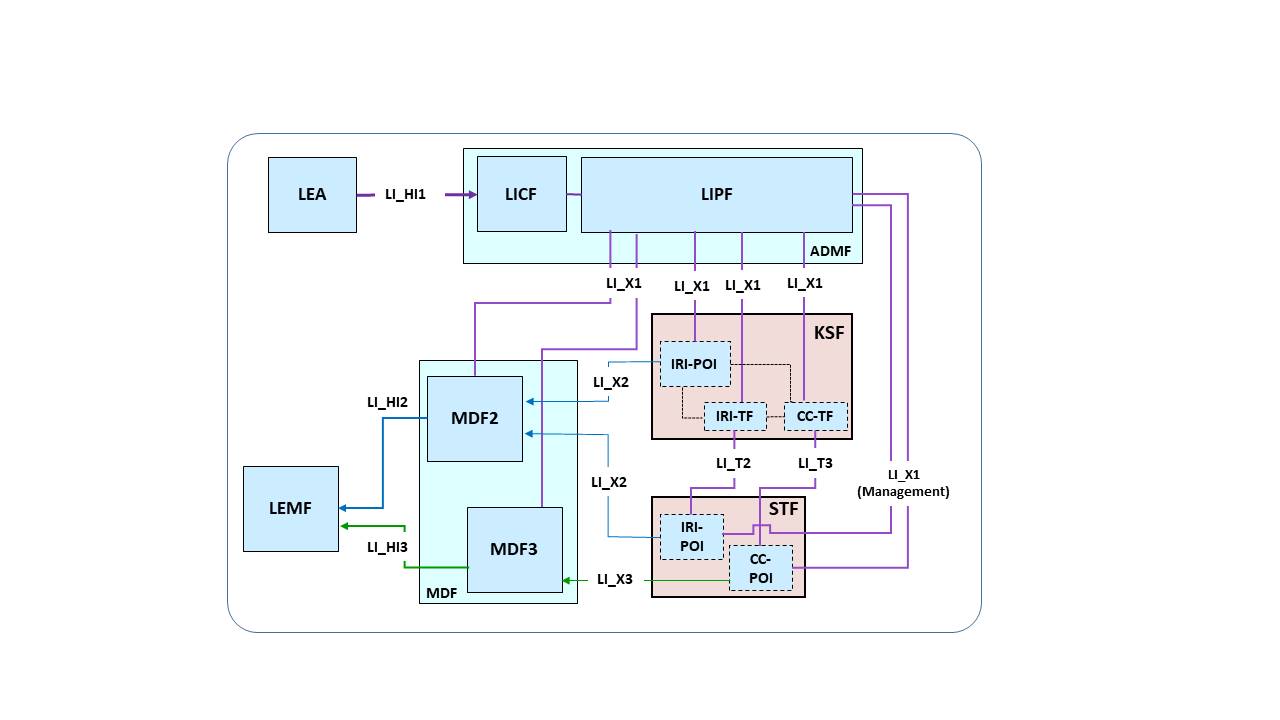


Figure 7.15.2-2: General architecture, STF not relying on 5G native identifiers.

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

7.15.3.1.7 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].

NEXT CHANGE

## 8.5 Points of Interception

CSPs use a wide range of 3GPP NFs to provide services to users. In order to intercept a service, POIs are associated with specific NFs, as depicted in Figure 8.5-1. The manner the POI obtains the required information from the NF depends on the service and can range from something as simple as a copy-and-forward mechanism, to sophisticated isolation and filtering. The POI may be embedded in the NF or external to the NF, connected to its interfaces. The choice of one, the other, or both approaches is service specific.



Figure 8.5-1: Embedded vs. external POIs

In figures 8.5-2 and 8.5-3 the POI will be depicted straddling the edge of the NF to simultaneously indicate both approaches.

Figure 8.5-2 shows the basic job of a POI: to obtain the state, or communicated user data, of the intercepted service. As the NF changes state, or as additional user data is generated or forwarded, in the course of providing the service, the appropriate interceptable events or real-time content are transferred into the POI.



Figure 8.5-2: POI state capture

Although the POI has access to service state in the NF and information flows in and out of the NF, the NF shall not be able to access data in the POI, for obvious security reasons, as depicted in figure 8.5-3. If the POI is embedded, LI data leakage from the POI back into the non-secure area of the NF shall be prohibited. If the POI is not embedded, the implementation shall prohibit LI data leakage back into the NF.

The same requirements apply to TFs.

  
Figure 8.5-3: POI state capture security

Generally, embedded POIs have full access to the state machine of the service they intercept, while external POIs have to infer the state of the intercepted service from the events detected on the interfaces or externally applied traffic filtering criteria.

NEXT CHANGE

## A.1.2 Service-based representation with point-to-point LI system

The overall network configuration for 5G in a non-roaming scenario with the LI aspects is shown in figure A.1-1 using the service-based representation (as shown in TS 23.501 [2]) with the use of point-to-point LI system.



Figure A.1-1: Network topology showing LI for 5G (service-based representation) with point-to-point LI system

Figure A.1-1 shows the network topology of 5G system in a service-based representation; however, all the LI-related interfaces remain to be point-to-point.

The IRI-POIs present in the AMF, UDM SMF and SMSF deliver the xIRI to the MDF2 and CC-POI present in the UPF delivers the xCC to the MDF3. The MDF3 address to CC-POI present in UPF is provided by the CC-TF present in the SMF over LI\_T3 reference point.

The LIPF present in the ADMF provisions the IRI-POIs and the CC-TF present in the NFs with the intercept related data. The LI\_X1 interfaces between the LIPF and the UPF is to monitor the user plane data.

NOTE: The CC-POI present in the NEF is not shown in figure A.1-1 but will be present if intercept of those services is supported.

NEXT CHANGE

## A.3.1 General

According to TS 23.501 [2], a PDU session can involve multiple UPFs, but regardless of how many UPFs are involved in the session, the session only connects to a single DN through one or more DN connections (i.e. connections to the same DN).

When a PDU session involves multiple UPFs, the interception of user plane packets can be done in two ways:

- At one UPF (branching UPF) through which all the user plane packets pass through.

- At anchor UPFs.

When the second approach is chosen with branching UPF being one of the anchor UPFs, redundant delivery of CC should be avoided.

In a non-roaming scenario, the IRI-POI present in UDM also provide the LI functions.

NEXT CHANGE

## E.3.3 eCNAM

The Enhanced Calling Name (eCNAM) service defined in TS 24.196 [44] provides the terminating user with a name that identifies the originating user, and metadata about that originating user (e.g. address, language, etc.), like with RCD. eCNAM data is managed by the originating network and stored in an authoritative database. To enable the terminating network to retrieve eCNAM data, the terminating service provider queries the database using the calling telephone number as the key, to obtain calling display name and other metadata.

In both RCD and eCNAM the terminating network shall populate the received name and received metadata elements in appropriate SIP headers in the INVITE request being forwarded to the terminating UE.

END OF CHANGES