**3GPP SA3LI#81-e-a *S3i210274***

**eMeeting, 12-16 April 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v11.4* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.127** | **CR** | **<CR#>** | **rev** | **<Rev#>** | **Current version:** | **16.7.0** |  |
|  | | | | | | | | |
| *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:*** | LI state information transfer in SMF sets | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | SA3 LI (PIDS) | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | <Related\_WIs> | | | | |  | ***Date:*** | | | 2021-04-07 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | ***C*** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | SMF sets share SM context information and together handle PDU sessions for a group of users. The same PDU session can be managed by different SMs, requiring the TF in the SMF sets to share LI state information, mainly the XID. The behaviour of LI functions in SMF sets is currently undefined and can violate LI requirements. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Defining LISSF function and LI\_ST interface. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Implementation of LI for SMF sets remains undefined and confusing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.3, 6.2.3.1, 6.2.3.X, 6.2.3.X+1, 6.2.7, 6.2.X | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS/TR 33.128 CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |

--------------------------FIRST CHANGE------------------------

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC 5G Core Network

5GS 5G System

ADMF LI Administration Function

AMF Access and Mobility Management Function

AS Application Server

AUSF Authentication Server Function

BBIFF Bearer Binding Intercept and Forward Function

BSS Business Support System

CAG Closed Access Group

CC Content of Communication

CP Control Plane

CSI Cell Supplemental Information

CSP Communication Service Provider

CUPS Control and User Plane Separation

DN Data Network

DNAI Data Network Access Identifier

E-CSCF Emergency – Call Session Control Function

GPSI Generic Public Subscription Identifier

HMEE Hardware Mediated Execution Enclave

HR Home Routed

IBCF Interconnection Border Control Functions

ICF Identifier Caching Function

IEF Identifier Event Function

IMS-AGW IMS Access Gateway

IM-MGW IM Media Gateway

IP Interception Product

IQF Identifier Query Function

IRI Intercept Related Information

LALS Lawful Access Location Services

LBO Local Break Out

LEA Law Enforcement Agency

LEMF Law Enforcement Monitoring Facility

LI Lawful Interception

LI CA Lawful Interception Certificate Authority

LICF Lawful Interception Control Function

LI\_HI1 Lawful Interception Handover Interface 1

LI\_HI2 Lawful Interception Handover Interface 2

LI\_HI3 Lawful Interception Handover Interface 3

LI\_HI4 Lawful Interception Handover Interface 4

LI\_HIQR Lawful Interception Handover Interface Query Response

LIID Lawful Interception Identifier

LIPF Lawful Interception Provisioning Function

LIR Location Immediate Request

LI\_SI Lawful Interception System Information Interface

LISSF Lawful Interception State Storage Function

LI\_ST Lawful Interception State Transfer Interface

LI\_T1 Lawful Interception Internal Triggering Interface 1

LI\_T2 Lawful Interception Internal Triggering Interface 2

LI\_T3 Lawful Interception Internal Triggering Interface 3

LI\_X0 Lawful Interception Internal Interface 0

LI\_X1 Lawful Interception Internal Interface 1

LI\_X2 Lawful Interception Internal Interface 2

LI\_X3 Lawful Interception Internal Interface 3

LI\_X3A Lawful Interception Internal Interface 3 Aggregator

LI\_XEM1 Lawful Interception Internal Interface Event Management Interface 1

LI\_XER Lawful Interception Internal Interface Event Record

LI\_XQR Lawful Interception Internal Interface Query Response

LMF Location Management Function

LMISF LI Mirror IMS State Function

LMISF-CC LMISF for the handling of CC

LMISF-IRI LMISF for the handling of IRI

LTF Location Triggering Function

MA Multi-Access

MANO Management and Orchestration

MDF Mediation and Delivery Function

MDF2 Mediation and Delivery Function 2

MDF3 Mediation and Delivery Function 3

MRFP Multimedia Resource Function Processor

N9HR N9 Home Routed

N3IWF Non 3GPP Inter Working Function

NFV Network Function Virtualisation

NFVI Network Function Virtualisation Infrastructure

NFVO Network Function Virtualisation Orchestrator

NPLI Network Provided Location Information

NR New Radio

NRF Network Repository Function

NSSF Network Slice Selection Function

OSS Operations Support System

PAG POI Aggregator

PCF Policy Control Function

P-CSCF Proxy - Call Session Control Function

PEI Permanent Equipment Identifier

PGW PDN Gateway

PGW-U PDN Gateway User Plane

POI Point Of Interception

PLMN Public Land Mobile Network

PTC Push to Talk over Cellular

S8HR S8 Home Routed

SIRF System Information Retrieval Function

S-CSCF Serving - Call Session Control Function

SMF Session Management Function

SMSF SMS-Function

SUCI Subscriber Concealed Identifier

SUPI Subscriber Permanent Identifier

TF Triggering Function

TrGW Transit Gateway

UDM Unified Data Management

UDR Unified Data Repository

UDSF Unstructured Data Storage Function

UPF User Plane Function

VNF Virtual Network Function

VNFC Virtual Network Function Component

xCC LI\_X3 Communications Content

xIRI LI\_X2 Intercept Related Information

------------------------SECOND 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 have 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 function to all the CC-TFs 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:

- In approach 1, the IRI-POI responsible for the generation of such xIRI resides in the UPF. Such an IRI-POI requires a trigger to enable it to detect the user plane packets. The corresponding Triggering Function (IRI-TF) resides in the same SMF that has the IRI-POI for the generation of other xIRI.

- The trigger sent by the IRI-TF (present in the SMF) to the IRI-POI (present in the UPF) includes the following:

- User plane packet detection rules.

- Target identity.

- Correlation information.

- MDF2 address.

- The IRI-POI present in the UPF generates the xIRI (that includes the correlation number and the target identity) from the user plane packets and sends it to the MDF2. The MDF2 generates the IRI messages and send them to the LEMF.

- In approach 2, xCC is generated by the CC-POI present in the UPF as if the warrant involves the interception of communication contents. To enable this, the CC-TF presumed to be present in the SMF even when the warrant does not require the interception of communication contents. As explained before, the CC-POI generates the xCC and sends it to the MDF3. The MDF3 (based on the provisioned intercept information) does not generate and deliver the CC to the LEMF. Instead, the MDF3 forwards the xCC to the MDF2 over LI\_MDF interface. The MDF2 then generates the IRI messages from xCC and delivers those IRI messages to the LEMF.

NOTE 3: The IRI-POI and IRI-TF present in the SMF may be handled by the same process in the SMF.

NOTE 4: When multiple warrants are active on a target with one requiring the interception of communication contents and the other not (in other words, this other one requiring xIRI from user plane packets), the first approach requires the UPF to have both CC-POI and IRI-POI and the SMF to have IRI-POI, IRI-TF and CC-TF. Alternatively, the interception of communication contents is required anyway for one warrant, and hence, the second approach will become simpler and therefore, may be preferable.

NOTE 5: Directly provisioned CC-POI is not considered in the present document.

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.

-------------------------THIRD CHANGE----------------------

### 6.2.3.X LI state transfers in SMF sets

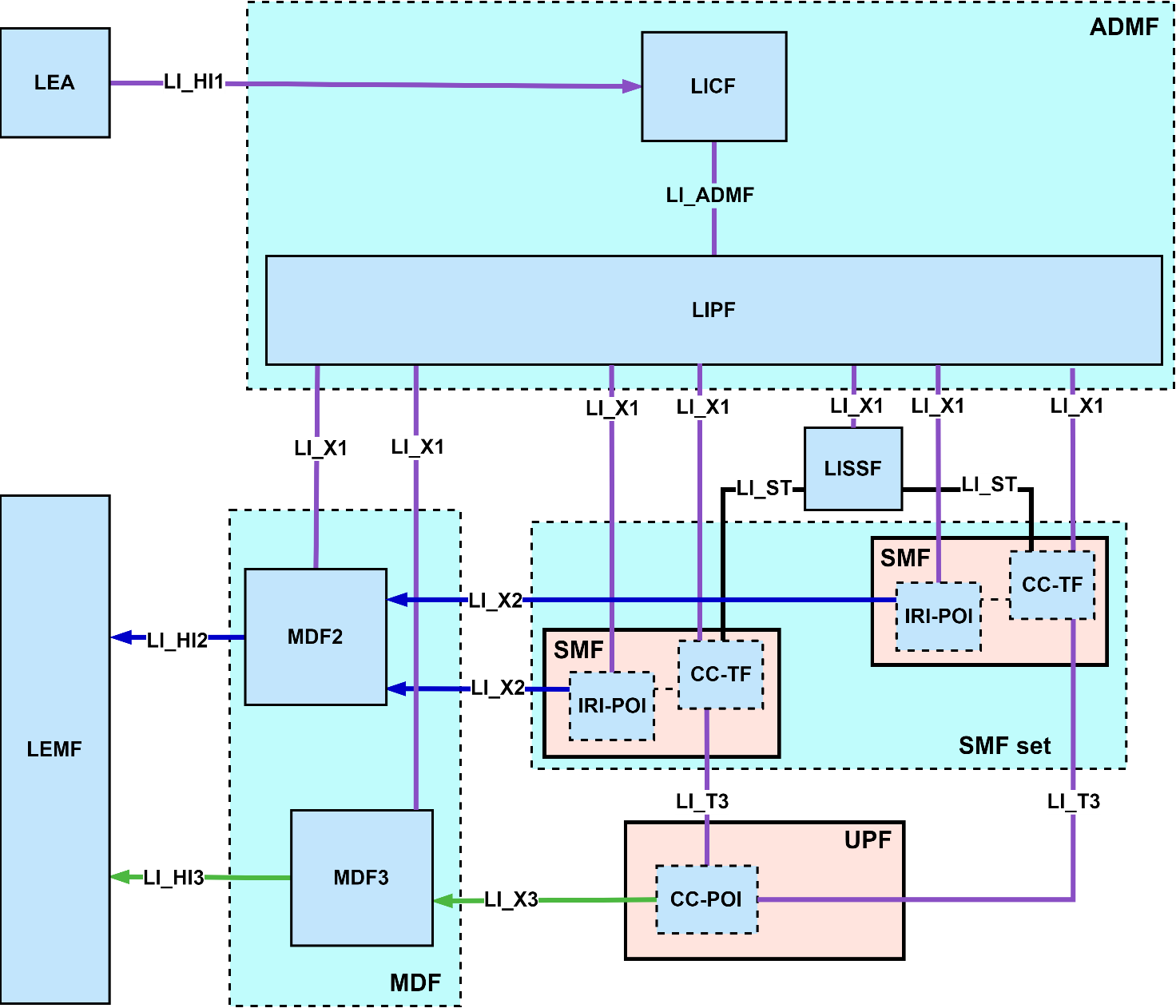


Figure 6.2-X: LI architecture diagram for SMF/UPF interception when using SMF sets

If the SMF belongs to a SMF set, it shall ensure that the relevant parts of the LI state in the CC-TF are not lost when the SMF is terminated. This can be achieved by keeping the relevant LI state up to date in a shared LISSF as shown in figure 6.2-X.

When a SMF in a SMF set receives context information related to a specific UE (either from a UDSF or from another SMF), the CC-TF within the SMF shall retrieve also the relevant LI state information from the shared LISSF.

------------------------FOURTH CHANGE-----------------------

### 6.2.3.X+1 Interface LI\_ST

LI\_ST is an interface between the LISSF and other LI functions such as the CC-TF or the LIPF. The LI functions may request, store or erase LI state information from the LISSF using this interface. LI functions other than the LIPF need to be authorized by the LIPF to have access to a specific instance of the LISSF before using the LI\_ST interface.

-------------------------FIFTH CHANGE------------------------

### 6.2.7 External data storage

The UDSF or UDR as defined in TS 23.501 [2] are used to externally store data relating to one or more NFs, separating the compute and storage elements of an NF. Where the NF contains a POI the following restrictions on the use of the UDSF/UDR shall apply:

- The UDSF/UDR shall be subject to the same location, geographic, security and other physical environment constraints as the NF POI for which it is storing data.

- No LI specific POI data (e.g. target list) shall be stored in the UDSF/UDR unless storage is directly under the control of the POI within the NF.

- LI data stored in a UDSF/UDR shall only be accessible by the specific individual POI for which the UDSF/UDR is storing data and that data shall not be shared between POIs unless specifically authorised by the LICF within the ADMF.

- By default, LI data shall not be stored in a UDSF/UDR which is shared by multiple NFs unless specifically authorised by the LICF.

- Any storage of LI data outside of the POI in the UDSF/UDR shall be auditable by the LICF.

- The interface between the POI/NF and the UDSF/UDR shall be protected such that an attacker cannot identify targeted users based on observation of this interface. (i.e. access to the UDSF/UDR shall be identical for both intercepted and non-intercepted user communications).

- The use and placement of a UDSF/UDR within an NF/POI design shall not introduce additional interception delay compared with non-separated compute and storage.

- Where the POI requires access to NF data that is stored in the UDSF/UDR, non-LI network functions and processes or non-LI authorised personnel shall not be able to detect POI access to that data in the UDSF/UDR.

- The POI and LICF/MDF shall be responsible for managing encryption of LI data stored for the POI in addition to any default encryption applied by the NF.

The above requirements shall apply when the UDSF/UDR provide data storage for TF/NF.

NOTE: For transfering LI state between different CC-TFs which belong to the same SMF set, see clause 6.2.X

-----------------------SIXTH CHANGE----------------------

### 6.2.X LI State Storage Function (LISSF)

The LI State Storage Function (LISSF) is the functional equivalent of a UDSF in the LI domain. There can be multiple instances of the LISSF in the network being handled by the same ADMF. The LISSF can be implemented as a separate function or within the ADMF. The LISSF may be used to transfer LI state information between LI functions, such as CC-TFs in the same NF set. The following restrictions on the use of the LISSF shall apply:

- The LISSF shall be subject to the same location, geographic, security and other physical environment constraints as the NF POIs or TFs for which it is storing data.

- The LISSF shall be directly under the control of the ADMF, and it shall be directly accessible and auditable by the ADMF.

- LI data stored in a LISSF shall only be accessible by the POIs and TFs authorised by the LIPF within the ADMF.

- Any storage of LI data outside of the POI or TF in the LISSF shall be auditable by the LIPF.

- The use and placement of a LISSF within an NF/POI/TF design shall not introduce additional interception delay compared with non-separated compute and storage.

- Where the POI/TF requires access to LI data that is stored in the LISSF, non-LI network functions and processes or non-LI authorised personnel shall not be able to detect POI/TF access to that data in the LISSF.

--------------------THE END OF CHANGES--------------------