**3GPP SA3LI#86-LI-b *S3i220429r3***

**Sophia-Antipolis, France, 30th Aug 2022 - 2nd Sep 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0176** | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** | architectures | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | SA3 LI (PIDS, NTAC, OTD, PCS, LKA Niedersachsen, Ministère Economie et Finances) | | | | | | | | | |
| ***Source to TSG:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | LI18 | | | | |  | ***Date:*** | | | 2022-09-02 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *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:*** | | LEAs have a requierment to get the UEs current network location. The CR adds the capability to acquire UE (network) location. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add location acquisition capability | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | CSP will be unable to meet the LI requierments for location acquisition capability | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 3.3, 5.3.5.1, 5.3.5.2, 5.4.3, 5.3.5.X (new), 5.3.X (new), 5.4.1, 5.4.3, 5.4.X (new), 5.4.Y (new), 5.4.Z (new), 5.4.W (new), 7.3.X (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | S3i220429 | | | | | | | | |

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.126: "Lawful interception requirements".

[4] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[5] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".

[6] OMA-TS-MLP-V3\_5-20181211-C: "Open Mobile Alliance; Mobile Location Protocol, Candidate Version 3.5", <https://www.openmobilealliance.org/release/MLS/V1_4-20181211-C/OMA-TS-MLP-V3_5-20181211-C.pdf>".

[7] ETSI TS 103 120: "Lawful Interception (LI); Interface for warrant information".

[8] ETSI TS 103 221-1: "Lawful Interception (LI); Internal Network Interfaces; Part 1: X1 ".

[9] 3GPP TS 33.501: "Security Architecture and Procedures for the 5G System".

[10] ETSI GR NFV-SEC 011: "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture".

[11] 3GPP TS 33.107: "3G Security; Lawful interception architecture and functions".

[12] 3GPP TS 23.214: "Architecture enhancements for control and user plane separation of EPC nodes; Stage 2".

[13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[14] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[15] 3GPP TS 33.128: "Protocol and Procedures for Lawful Interception; Stage 3".

[16] ETSI TS 103 221-2: " Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3".

[17] MMS Architecture OMA-AD-MMS-V1\_3-20110913-A.

[18] Multimedia Messaging Service Encapsulation Protocol OMA-TS-MMS\_ENC-V1\_3-20110913-A.

[19] 3GPP TS 22.140: "Multimedia Messaging Service (MMS); Stage 1".

[20] ETSI GS NFV-IFA 026: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification".

[21] 3GPP TS 33.108: "Handover Interface for Lawful Interception (LI)".

[22] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for   
Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[23] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[24] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

[25] OMA-AD-PoC-V2\_1-20110802-A: "Push to talk over Cellular (PoC) Architecture".

[26] GSMA IR.92: "IMS Profile for Voice and SMS".

[27] GSMA NG.114: "IMS Profile for Voice, Video and Messaging over 5GS".

[28] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[29] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[30] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[31] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage3".

[32] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[33] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[34] OMA-AD-CPM-V2\_2-20170926-C: "Open Mobile Alliance, OMA Converged IP Messaging System Description", <http://www.openmobilealliance.org/release/CPM/V2_2-20200907-C/OMA-AD-CPM-V2_2-20170926-C.pdf>.

[35] GSMA RCC.07: "Rich Communication Suite – Advanced Communications Services and Client Specification".

[36] IETF RFC 4975: "The Message Session Relay Protocol (MSRP)".

[37] IETF RFC 6714: "Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)".

[38] IETF RFC 3862: "Common Presence and Instant Messaging (CPIM): Message Format".

[39] 3GPP TS 24.229: "IP Multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[40] IETF RFC 8224: "Authenticated Identity Management in the Session Initiation Protocol (SIP)".

[41] IETF RFC 8946: "Personal Assertion Token (PASSporT) Extension for Diverted Calls".

[42] IETF draft-ietf-stir-passport-rcd-12, "PASSporT Extension for Rich Call Data".

NOTE: The above document cannot be formally referenced until it is published as an RFC.

[43] IETF RFC 7095: "jCard: The JSON Format for vCard".

[44] 3GPP TS 24.196: "Enhanced Calling Name (eCNAM)".

[45] IETF RFC 8816: "Secure Telephone Identity Revisited (STIR) Out-of-Band Architecture and Use Cases".

[46] IETF draft-ietf-stir-passport-messaging-00, "Messaging Use Cases and Extensions for STIR".

NOTE: The above document cannot be formally referenced until it is published as an RFC.

[47] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[48] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[49] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

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

[xx] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

\*\*\* Next 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

AAnF AKMA Anchor Function

ADMF LI Administration Function

AF Application Function

AF\_ID Application Function Identity

AKA Authentication and Key Agreement

A-KID AKMA Key IDentifier

AKMA Authentication and Key Management for Applications

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

CPIM Common Presence and Instant Messaging

CPS Call Placement Service

CSI Cell Supplemental Information

CSP Communication Service Provider

CUPS Control and User Plane Separation

DN Data Network

DNAI Data Network Access Identifier

DoNAS Data over NAS

EAP Extensible Authentication Protocol

eCNAM Enhanced Calling Name

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 Identity Caching Function

IEF Identity Event Function

IMS-AGW IMS Access Gateway

IM-MGW IM Media Gateway

IP Interception Product

IQF Identity Query Function

IRI Intercept Related Information

KAF AKMA Application Key

KAKMA AKMA Anchor Key

KID Key IDentifier

KLI Decryption key(s) for services encrypted by CSP-provided keys

KSF Key Server Function

LAF Location Acquisition Function

LALS Lawful Access Location Services

LARF Location Acquisition Requesting Function

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\_HILA Lawful Interception Handover Interface Location Acquisition

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\_X2\_LA Lawful Interception Internal Interface 2 Location Acquisition

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\_XLA Lawful Interception Internal Interface Location Acquisition

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

MSRP Message Session Relay Protocol

N3A Non-3GPP Access

N3IWF Non 3GPP Inter Working Function

N9HR N9 Home Routed

NAS Non-Access Stratum

NCGI NR Cell Global Identity

NEF Network Exposure Function

NFV Network Function Virtualisation

NFVI Network Function Virtualisation Infrastructure

NFVO Network Function Virtualisation Orchestrator

NIDD Non-IP Data Delivery

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-C PDN Gateway Control Plane

PGW-U PDN Gateway User Plane

POI Point Of Interception

PLMN Public Land Mobile Network

PTC Push to Talk over Cellular

RCD Rich Call Data

RCS Rich Communication Suite

S8HR S8 Home Routed

SCEF Service Capability Exposure Function

SCS Service Capability Server

SGW Serving Gateway

SGW-C Serving Gateway Control Plane

SGW-U Serving Gateway User Plane

SHAKEN Signature-based Handling of Asserted information using toKENs

SIRF System Information Retrieval Function

S-CSCF Serving - Call Session Control Function

SIP Session Initiation Protocol

SMF Session Management Function

SMSF SMS-Function

STF Security Terminating Function

STIR Secure Telephony Identity Revisited

SUCI Subscriber Concealed Identifier

SUPI Subscriber Permanent Identifier

TAI Tracking Area Identity

TF Triggering Function

TLS Transport Layer Security

TNGF Trusted Non-3GPP Gateway Function

TrGW Transit Gateway

TWIF Trusted WLAN Interworking Function

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

W-AFG Wireline Access Gateway Function

xCC LI\_X3 Content of Communication

xIRI LI\_X2 Intercept Related Information

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

### 5.3.5 Administration Function (ADMF)

#### 5.3.5.1 General

The Administration Function (ADMF) provides the CSP's administrative and management functions for the LI capability. This includes overall responsibility for the provisioning/activating, modifying, and de-activating/de-provisioning the Point(s) Of Interception (POI), Triggering Functions (TF), and the Mediation and Delivery Functions (MDF). The ADMF is also responsible for managing the Identifier Event Functions (IEF) and Identifier Caching Function (ICF). The ADMF is also responsible for controlling and managing the Location Acquisition Requesting Function (LARF).

The ADMF includes the following logical sub-functions:

- Lawful Interception Control Function (LICF).

- Lawful Interception Provisioning Function (LIPF).

- Identifier Query Function (IQF).

- Certificate Authority (CA).

- Location Acquisition Function (LAF).

Within one ADMF there is one LICF, one IQF, one LAF, and at least one, but possibly multiple LIPFs.

The LICF and LIPF communicate via the internal LI\_ADMF interface, the details of which are outside the scope of the present document.

The LICF and LAF communicate via the internal LI\_LAFC interface, the details of which are outside the scope of the present document.

The LIPF and LAF communicate via the internal LI\_LAFP interface, the details of which are outside the scope of the present document.

The ADMF contains the issuing Certificate Authority (CA) for all LI components (POIs, MDFs etc.). Further details are defined in clause 8.3.

The IQF is used for handling identifier association requests. Further details are defined in clause 5.7.

NOTE: It is assumed that the LICF and IQF are always implemented on dedicated LI infrastructure which is only accessible to CSP personnel explicitly authorised to handle LI. However, the LIPF is assumed in some scenarios (e.g. virtualisation) to be implemented within the main CSP network infrastructure environment, although still only accessible to LI authorised CSP personnel.

The LAF is used for handling location acquisition requests. Further details are defined in clause 7.3.X.

For further details on the roles and responsibilities of the ADMF refer to Annex B.

#### 5.3.5.2 LICF

The LICF controls the management of the end-to-end life cycle of a warrant. The LICF contains the master record of all sensitive information and LI configuration data. The LICF is ultimately responsible for all decisions within the overall LI system. The LICF, via the LIPF acting as its proxy is responsible for auditing other LI components (POIs, MDFs etc.). The LICF is responsible for communication with administrative LEA systems (LI\_HI1).

The LICF provides the intercept information derived from the warrant for provisioning at the POI, TF, MDF2, and MDF3. With the exception of the communication with the LEA, all other communication between the LICF and any other entities shall be proxied by the LIPF.

The LICF also maintains and authorises the master list of POIs, IEFs, ICF, TFs, MDFs, and LARFs. In dynamic networks the LIPF is responsible for providing the LICF with any necessary updates to the POI, TF, IEF, ICF, MDF, and LARF list.

The LICF is responsible for management and audit of the IEF(s) and ICF proxied by the LIPF.

The LICF shall support activating and deactivating of IEF identifier association reporting capabilities on a per IEF basis proxied by the LIPF.

The LICF shall provide the IQF with information relating to IEFs and ICF necessary for the IQF to handle queries from the LEA and obtain answers to such queries.

If the LICF deactivates event record reporting to an IEF, the LICF shall also instruct the ICF to immediately delete all cached identifier associations which the ICF had received from that IEF.

The LICF shall ensure that the ICF is always activated before IEFs and de-activated after IEFs to ensure that data loss does not occur due to an IEF sending events before an ICF is configured to receive them.

The LICF shall provide the LAF with information necessary for the LAF to handle location acquisition queries from the LEA and obtain answers to such queries.

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

#### 5.3.5.X LAF

The Location Acquisition Function (LAF) is responsible for processing the location requests received from the LEA during the location acquisition procedure. Further details of the LAF are defined in clause 7.3.X.

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

### 5.3.X LARF

The Location Acquisition Requesting Function (LARF) is a function associated with the AMF responsible for handling the location requests from the LAF during the location acquisition procedure. Further details of the LARF are defined in clause 7.3.X.

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

### 5.4.1 General

A high-level interception architecture diagram showing key point-to-point LI interfaces is shown in figure 5.4.1-1 below.



**Figure 5.4.1-1: High-level interception architecture diagram with key point-to-point LI interfaces**

A high-level acquisition architecture diagram showing key point-to-point LI interfaces is shown in figure 5.4.1-2 below.



**Figure 5.4.1-2: High-level acquisition architecture diagram with key point-to-point LI interfaces**

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

### 5.4.3 Interface LI\_HI1

LI\_HI1 is used to send warrant and other interception request information from the LEA to the CSP. This interface may be electronic or may be an offline manual process depending on national warranty processes.

The following are some of the information elements sent over this interface:

- Target identifier: used to identify the communications to be intercepted.

- Type of intercept: used to indicate whether IRI only, CC only, or both IRI and CC, is to be delivered to the LEMF.

- Location acquisition: used to indicate whether location acquisition is required (in addition to lawful interception for other services, only location acquisition, or no location acquisition) and the type of delivery (via LI\_HILA, via LI\_HI2, or both).- Service scoping: used to identify the service (e.g. voice, packet data, messaging, target positioning) to be intercepted.

- Filtering criteria: used to provide additional specificity for the interception (e.g. for bandwidth optimization).

- LEMF address: used to deliver the Interception Product.

- Lawful Interception Identifier (LIID) used to associate the issued warrant with the Interception Product.

LI\_HI1 interfaces shall support the use of ETSI TS 103 120 [7] for communication of warrant information between the LEA and CSP. However, default configurations, information element formats and other parameters as defined in the present document shall apply regardless of generic default options specified in ETSI TS 103 120 [7].

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

### 5.4.X Interface LI\_HILA

The LI\_HILA interface is used by the LEA to forward the location acquisition requests to the LAF and when requiered to forward the location acquisition responses from the LAF to the LEA.

The following are examples of some of the information that may be passed over the LI\_HILA interface:

- Target identifier (SUPI, GPSI).

- Authorisation identifier (LIID).

If the type of location acquisition delivery is via the LI\_HILA, the following are examples of some of the additional information that may be passed over the LI\_HILA interface from LAF to LEA:

- Timestamp of when the target’s location was acquired.

- Location information.

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

### 5.4.Y Interface LI\_XLA

The LI\_XLA interface is used by the LAF to forward the location acquisition requests to the LARF and when required to forward the location acquisition responses from the LARF to the LAF if the delivery type of location acquisition delivery is via the LI\_HILA.

The following are examples of some of the information that may be passed over the LI\_XLA interface from LAF to LARF:

- Internal interception identifier.

- Target identifier (SUPI, GPSI).

- Information relating to the type of delivery (via LI\_HILA, via LI\_HI2, or both).

- Address of MDF2.

If the type of location acquisition delivery is via the LI\_HILA, the following are examples of some of the information that may be passed over the LI\_XLA interface from LARF to LAF:

- Timestamp of when the target’s location was acquired.

- Location information.

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

### 5.4.Z Interface LI\_X2\_LA

LI\_X2\_LA interfaces are used to pass the xIRI containing location acquisition outcomes between the LARF to the MDF2. It is realised using TS 103 221-2 [16].

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

### 5.4.W Interface LI\_LAFP and LI\_LAFC

LI\_LAFP and LI\_LAFC are interfaces used to exchange relevant information between the LIPF, LICF and the LAF. Further details about this interface are outside the scope of the present document.

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

### 7.3.X Location Acquisition

#### 7.3.X.1 General

This clause defines the location acquisition procedure, which provides lawful access to the target’s network-provided location. The outcome of this procedure is the target’s TAI, NCGI and optionally the timestamp when the target’s location was acquired. It is emulating the AMF location services request and consumes the response as defined in TS 29.518 [xx] clause 5.5.2.4. The AMF shall override any user consent, privacy and paging restrictions concerned with location acquisition that may apply to the target UE.

The LEA shall be able to indicate in the request to the LAF whether the AMF location services shall be invoked or whether the current stored value of the location as known by the AMF is returned.

Prior to issuing of location acquisition requests, the LEA shall provide an authorization for these requests. This is done by issuing a warrant over the LI\_HI1 interface prior to issuing the location acquisition requests. Subsequently, the LIPF will provision the MDF2 if needed.

NOTE: The use of the location acquisition procedure may cause detectability issues due to the possibility of triggering a Network Triggered Service Request procedure for a UE. Detectibility issues may also include the visibility between different LEAs using location acquisition with warrants for the same target. It is up to the LEA to decide if location acquitison is to be used.

#### 7.3.X.2 Location acquisition architecture

This clause describes the architecture for location acquisition. The architecture is based on the use of a LAF, which communicates with the LARF associated with an AMF over the LI\_XLA interface.

To use the location acquisition procedure, the LAF needs to determine the serving AMF for the target UE.

NOTE: The method for determining the serving AMF is not defined in the present document.

The LAF is requested to perform location acquisition via the LI\_HILA interface between LEA and LAF. Upon receiving the request, the LAF initiates location acquisition to the LARF via the LI\_XLA interface.

The networks shall support the delivery of location information via the following methods:

- Location information is delivered back as a response to the location acquisition request via the LAF over the LI\_XLA and the LI\_HILA interfaces.

- Location information is delivered via the MDF2 over the LI\_X2\_LA and the LI\_HI2 interfaces.

The two delivery options may be used simultaneously.

The LARF and the IRI-POI will exchange the necessary information to ensure that IRI-POI will not generate the xIRI for location requests initiated by the LARF.

The ADMF shall be able to audit the LARF over the LI\_XLA interface.

##### 7.3.X.2.1 Location information delivery via the LI\_HILA

The architecture for delivering location information via the LI\_HILA is depicted in figure 7.3.X.2.1-1.



Figure 7.3.X.2.1-1: Delivery of the retrieved location information via the LI\_HILA

Upon determining the location, the LARF will forward the location information to the LAF via the LI\_XLA interface. The retrieved information is further provided in the response to the LEA over the interface LI\_HILA. The LARF and the IRI-POI will exchange the necessary information to ensure that IRI-POI will not generate the xIRI for location requests initiated by the LARF.

##### 7.3.X.2.2 Location information delivery via the LI\_HI2

The architecture for delivering location information via LI\_HI2 is depicted in figure 7.3.X.2.2-1.

##### 

Figure 7.3.X.2.2-1: Delivery of the retrieved location information via the LI\_HI2

Upon determining the location, the LARF shall forward the location information to the MDF2 over the LI\_X2\_LA interface using the information provided by the LAF in the LI\_XLA request (e.g., internal intercept identifier). The retrieved information is further provided by the MDF2 to the LEMF via the LI\_HI2 interface. The LARF and the IRI-POI will exchange the necessary information to ensure that IRI-POI will not generate the xIRI for location requests initiated by the LARF.\*\*\* End of all changes \*\*\*