**3GPP SA3LI#79e-a *S3i200624r3***

**eMeeting, 19-23 October 2020**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **2** | **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:***  | Identifier Association |
|  |  |
| ***Source to WG:*** | SA3-LI (BT Plc, Public Safety Canada, PIDS, OTD, Ministère de l'Economie et des Finances, BfV, LKA Niedersachen, Telefónica S.A., EVE Compliancy Solutions, NTAC, BAE Systems Applied Intelligence Limited, OFCOM(CH), Rogers Communications Canada, Nokia, Nokia Shanghai Bell, ZiTiS, BKA, AGD) |
| ***Source to TSG:*** | SA3 |
|  |  |
| ***Work item code:*** | LI16 |  | ***Date:*** | 2020/10/22 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Release 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 canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Features such as SUPI privacy cause challenges for LEAs in being able correctly identify and target individual UEs for LI purposes. It also presents challenges for CSPs to be able to meet LI requirements in terms of removing encryption or transcoding applied by the CSP.  |
|  |  |
| ***Summary of change:*** | This CR provides a set of real-time identifier assocation reporting and querying capabilities which allow LEAs to target individual UEs when SUPI privacy or other temporary identifier mechanisms are in use by the AMF. The CR allows privacy mechanism to remain enabled while allowing the CSP to meet LI related regulatory obligations. |
|  |  |
| ***Consequences if not approved:*** | LEAs are not able to obtain necessary permanent to temporary and temporary to permanent identifier assocations for LI purposes. |
|  |  |
| ***Clauses affected:*** | 3.3, 5.3.5.1, 5.3.5.2, New 5.3.5.4, 5.4.1, 5.4.3, New 5.4.13, New 5.4.14, New 5.4.15, New 5.4.16, New 5.4.17, 5.6.3.2, New 5.7, 6.2.2.4, 6.2.2.6, New 6.2.2A, 6.3.2.3, 6.3.2.5, 7.1, 7.3.1, New 7.4 |
|  |  |
|  | **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 should be implemented before CR 0094. |
|  |  |
| ***This CR’s revision history:*** | s3i200603, s3i200624 |

----------------------START OF CHANGES---------------------

## 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

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

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

----------------------NEXT CHANGES---------------------

### 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 managing the Identifier Event Functions (IEF) and Identifier Caching Function (ICF).

The ADMF includes four logical sub-functions:

- Lawful Interception Control Function (LICF).

- Lawful Interception Provisioning Function (LIPF).

- Identifier Query Function (IQF).

- Certificate Authority (CA).

Within one ADMF there is one LICF, one IQF 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 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.

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 and MDFs. In dynamic networks the LIPF is responsible for providing the LICF with any necessary updates to the POI, TF, IEF, ICF and MDF 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.

----------------------NEXT CHANGES---------------------

#### 5.3.5.4 IQF

The IQF is the function responsible for receiving and responding to dedicated LEA real-time queries for identifier associations. Further details of the IQF are defined in clause 5.7.2.1.

----------------------NEXT CHANGES---------------------

## 5.4 LI interfaces

### 5.4.1 General

A high-level LI architecture diagram showing key point-to-point LI interfaces is shown in figure 5.4-1 below.



**Figure 5.4-1: High-level architecture diagram with key point-to-point LI interfaces**

----------------------NEXT CHANGES---------------------

### 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.

- 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 CHANGES---------------------

### 5.4.13 Interface LI\_IQF

LI\_IQF is an interface between LICF and IQF and is used by the LICF to send management information related to IEFs and ICF, to the IQF. Further details about this interface is outside the scope of the present document.

### 5.4.14 Interface LI\_XQR

The LI\_XQR interface is used by the IQF to send identifier association queries to the ICF and from the ICF to return identities associations to the IQF in response.

The following are examples of some of the information that may be passed over LI\_XQR from the IQF to the ICF:

- Information relating to the type of query.

- Temporary or permanent identifier provided by the LEA.

- Other information associated with identifier required for localisation provided by the LEA.

 - Cell identity.

 - Tracking area identifier.

- Time that identifier provided by the LEA was observed by the LEA.

The following are examples of some of the information that may be passed over LI\_XQR from the ICF to the IQF:

- Information relating to the type of query being responded to.

- Temporary and permanent identifiers corresponding to identifier provided by LEA.

- Identifier association validity start and end times.

### 5.4.15 LI\_HIQR

The LI\_HIQR interface is used by the LEA to send identifier association queries to the IQF and from the IQF to return identities associations to the LEA in response.

The following are examples of some of the information that may be passed over LI\_HIQR from LEA to the IQF:

- Information relating to the type of query.

- Warrant/authorisation identifier.

- Temporary or permanent identifier provided by the LEA.

- Other information associated with identifier required for localisation provided by LEA.

 - Cell identity.

 - Tracking area identifier.- Time that identifier provided by LEA was observed by the LEA.

The following are examples of some of the information that may be passed over LI\_HIQR from IQF to the LEA:

- Information relating to the type of query being responded to.

- Warrant/authorisation identifier.

- Temporary and permanent identifiers corresponding to identifier provided by LEA.

- Identifier association validity start and end times.

### 5.4.16 LI\_XER

The LI\_XER interface is used by the IEF to send identifier association events to the ICF.

The following are examples of some of the information that may be passed over LI\_XER from the IEF to the ICF:

* Permanent identifier and temporary identifier association.
* Permanent identifier and temporary identifier excommunication / de-association.
* Time stamp of association observation.

### 5.4.17 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 TS 103 221-1 [8].

----------------------NEXT CHANGES---------------------

#### 5.6.3.2 LI\_X0 procedures

Only once an LI function has been instantiated and the LIPF in the ADMF informed of that NF's existence, can that NF be managed by the LIPF in the ADMF over LI\_X0. Such notification is achieved as described in clause 5.6.3.1 over LI\_NO and LI\_MANO and occurs prior to any SIRF/NRF (or equivalent) NF discovery processes.

The LI\_X0 interface is used to manage LI functions after instantiation such they are made ready for LI use and subsequent provisioning over LI\_X1.

After a VNF is instantiated (e.g. using the procedures in ETSI GR NFV-SEC 011 [10] and ETSI NFV-IFA 026 [20] or equivalent), it is necessary to automatically configure the LI functions (e.g. POI, TF, MDF) before use (i.e. to initialise it to a state where it can accept LI\_X1 messages). To achieve this the LI Function shall after instantiation and initial network configuration by NFV MANO (e.g. allocation of network IP address and FQDN) contact the LIPF over the LI\_X0 interface and LIPF will notify the LICF that a new potential LI function has contacted the LIPF. The LIPF shall only accept incoming connections from new LI functions that have previously been notified to the LIPF/LICF by the LI NFV controller over LI\_NO. The LI\_NO interface shall carry information to allow the LIPF to associate a VNF instance with the LI application instance running in it.

The LICF in the ADMF, through the LIPF, shall verify the authenticity of the LI function over LI\_X0 in order to verify that the new LI function has been instantiated from a valid software image. If the LI function software image has been partly encrypted as described in ETSI GR NFV-SEC 011 [10], then once the LICF has verified the integrity of the LI function it shall provide any necessary keys to the LIPF to decrypt the LI function to complete instantiation of that LI function.

Once a trust relationship has been established between the LICF and new LI function, the LIPF shall issue the LI function with an LI identity (e.g. POI CSCF number 42 or LI System FQDN) and provide the other necessary certificates and configuration information to allow the new LI function to be configured for LI use on LI\_X1. The LICF is responsible for providing necessary information and policy rules necessary for the LIPF to perform configuration of LI functions over LI\_X0. For the purposes of instantiation IEFs and ICF follow the same instantiation flow as POIs except that the LIPF has a more limited role in managing these functions after instantiation over LI\_XEM1 compared to POIs as neither of these types of LI functions are subject to LI provisioning.

In the case of triggered POIs which are not directly provisioned by the LIPF in the ADMF over LI\_X1, the LIPF is still responsible for LI\_X0 configuration of the POI including identity manage and all necessary identity / communication certificates in order to allow the POIs and TF to communicate over LI\_X1, LI\_T2 and LI\_T3. The same applies to virtualised MDFs or CC-PAG.

Once an LI function directly associated with or embedded in an NF has been made fully ready for provisioning over LI\_X1 using LI\_X0, the LICF in the ADMF via the LIPF shall notify the LI NFV Controller that the LI function is ready for service and NFV MANO may advise the OSS/BSS that the NF associated with the LI functions is ready for service and discovery by the NRF. For MDFs, CC-PAGs, or non-embedded POIs the LICF may still need to provide a ready for service indication to NFV MANO / OSS / BSS depending on the implementation scenario.

NOTE: The full procedure for notifying the OSS/BSS that LI is ready and that the NF can be notified to the NRF (in the case of 5G SBA) is out of scope of the present document and is left to operator deployment choice.

During normal system operation LI\_X0 shall be used by the LIPF in the ADMF to maintain the LI function throughout the LI function’s lifecycle, except as a result of scaling or other changes applied by NFV MANO (such changes are first managed by the NFV LI Controller through LI\_NO and LI\_MANO and any necessary LI\_X1/LI\_X2/LI\_X3 level re-configuration then applied over LI\_X0). In-life certificate updates, identity changes, LI\_X1/2/3 credential changes and other similar configuration changes shall be supported by both the LIPF in the ADMF and LI functions over LI\_X0.

Figure 5.6-2 shows an example of what the procedures described in this clause look like when instantiating a new NF and associated LI functions.



Figure 5.6-2: Example simplified flow-diagram for OSS / BSS originated LI instantiation procedures

----------------------NEXT CHANGES---------------------

## 5.7 Identifier association and reporting

### 5.7.1 General

3GPP networks use temporary identifiers in place of permanent identifiers to ensure that identities which are visible on exposed interfaces (e.g. RAN) cannot be used to track or degrade the privacy of a subscriber. For LI purposes, CSPs are required to be able to provide real-time association between temporary and permanent identifiers where the use of such identifier associations impact the ability of the LEA to uniquely identify the UE, subscriber or true permanent identifiers associated with a service.

The present document defines two sets of capabilities which allow CSPs to report such association to LEAs;

* Real-time reporting of associations as observed by POIs as part of network access, target communications and service usage.
* Dedicated real-time query, lookup and reporting of identifier associations.

For real-time reporting based on POI observation, associations are reported through a combination of dedicated event records sent from the POI to the MDF over LI\_X2 and through inclusion of specific parameters in other communications service records reported over LI\_X2.

For dedicated query, lookup and reporting, figure 5.7-1 shows the high-level architecture used to support identifier association query and response requirements. The Identifier Event Function (IEF) provides the Identifier Caching Function (ICF) with the events necessary to answer the identifier association queries from the IQF. LEAs are able to issue real-time queries to the Identifier Query Function (IQF), which in turn queries the ICF.

 

Figure 5.7-1 High-level identifier retrieval via Query and Response.

The IQF and ICF shall support the following query types;

* Single query and response.
* Single query and response followed by triggered real-time reporting of any subsequent changes reported to the ICF. (See NOTE 2).

Within the present document, only a single ICF for all IEFs is supported.

Within the present document, interfaces and generic functionality for dedicated identifier query and response are defined in this clause, while specific instances of the IEFs are defined within clause 6 and the ICF in clause 7.

For each request over LI\_HIQR, the LEA shall provide a legal warrant/authorisation unique identifier. In addition, depending on the scenario, the LEA needs to provide, the observed identity (temporary or permanent), along with the serving cell identity, tracking area identifier, and time of observation by LEA.

The IQF shall obtain in real-time the identifier associations which match the LEA query from the ICF and provide a response to the LEA over LI\_HIQR.

In some cases, it may not be possible to establish a single unique identifier association given the information provided by the LEA. IQF handling in such a scenario is subject to the authorisation in the warrant and is outside the scope of the present document.

NOTE 1: If the LEA is unable to provide the tracking area associated with an observed temporary identifier this may prevent the CSP from uniquely associating the identifier to the correct UE.

NOTE 2: Single query and response followed by triggered real-time reporting of any subsequent changes detected by the IEF is only applicable to queries based on a permanent identifier where the changes reported are new temporary identifiers to which that permanent identifier has been associated.

### 5.7.2 Functional entities

#### 5.7.2.1 Identity Query Function (IQF)

The IQF is the function responsible for received and responding to dedicated LEA real-time queries for identifier associations. The IQF is a sub-function of the ADMF.

On receiving a valid query, the IQF shall query the ICF in order to obtain the required mapped identities. The IQF shall be able to support both association from permanent identifierss to temporary identifiers and from temporary identifiers to permanent identifiers.

NOTE 1: Only queries based on applicable subscription permanent identifiers or associated temporary identifiers are supported by the present document. Queries based on ME hardware identifiers or communications services identifiers (e.g. E.164 numbers) are not supported by the IQF.

NOTE 2: A specific query response to the LEA may require both permanent and temporary identifiers to be returned in a single response for a given query. For example, if an LEA queries using a temporary identifier, then it may be necessary to respond with a permanent identifier, plus other associated temporary identifiers in order to fulfil the query.

The IQF shall only support queries that are received from the LEA within the caching duration and shall reject any queries from the LEA which fall outside those time limits.

NOTE 3: It may not always be possible for the CSP to provide an answer due to association information no longer being available in the network. The IQF shall provide support for multiple LEA scenarios. The IQF shall be able to support different query constraints for different LEAs.

NOTE 4: Since IEF event generation and ICF temporary caching applies to all UEs served by the parent NF, any multiple LEA scenarios or differences in requirements are handled by the IQF only and no specific support is provided by IEF or ICF.

The IQF shall support both query and response types as defined in clause 5.7.1.

#### 5.7.2.2 Identity Event Function (IEF)

The IEF is the function responsible for observing and detecting identifier association changes within its parent NF and providing those changes in the form of event records to the ICF over LI\_XER.

IEFs may be co-located with POIs but may also be placed in other NFs where the NFs handling identifier association do not otherwise support POI functionality.

The IEF shall be able to provide event records to the ICF when associations are updated. Association events include both allocation or deallocation events for temporary identifiers managed by the IEF’s parent NF and for identifier association which are registered or deregistered in the IEF’s parent NF but the identifier allocation is not controlled by that NF.

The IEF shall support activation and deactivation of IEF association reporting capabilities, as controlled by the LICF (proxied by the LIPF) over the LI\_XEM1 interface.

When IEF reporting capabilities are activated, the IEF shall obtain the current allocation and registration state of all UEs known to the parent NF, (where that information has been retained in the NF as part of normal network operations) and send this as a series of allocation/registration events to the ICF.

NOTE: The IEF can only report on associations that occurred before activation of the IEF if those associations remain valid for UEs which are still served by the parent NF (some allocations may not be retained by the parent NF). Therefore, not all UE identifier associations may be available at IEF activation (e.g. due to NF or UE mobility) and therefore ICF caching may be incomplete until network reauthentication timers or similar reallocation timers have refreshed all served UE as part of normal network operation. Such incomplete data will result in no matching identifier responses from the ICF.

When IEF reporting capabilities are deactivated, the IEF shall immediately stop sending event records to the ICF.

#### 5.7.2.3 Identity Caching Function (ICF)

The ICF is the LI function responsible for caching of identifier associations provided by the IEF in event records received over the LI\_XER and answering queries from the IQF received over LI\_XQR. The ICF shall support association queries from both temporary identities to permanent identities and from permanent identities to temporary identities.

Identifier associations shall be held while the identities remain actively associated with a UE served by the IEF’s parent NF.

The ICF shall be able to update and mark identifier associations for expiry as necessary to maintain the required caching period.

Upon receiving a disassociation event from the IEF, the ICF shall match any corresponding identifier associations and mark them for deletion once the short-term caching time limit is reached. Both the allocation and deallocation event shall be deleted and purged irrecoverably from the ICF once the limit is reached.

If a network supports service handover between NFs, or UEs do not cleanly deregister from the network (e.g. UE battery removal), then the IEF may not be able to generate de-allocation event records. Therefore, the ICF shall delete identifier associations from the cache after a CSP defined age has been reached, regardless of whether a matching deallocation/registration event has been received for a given identity association.

NOTE 1: The time period after which automatic deletion should occur is outside the scope of the present document. However, this CSP determined value should typically be matched to the network re-authentication timers and maximum temporary identity validity period after which the network would update temporary identity allocations. In all cases this value needs to be as short as possible.

The ICF shall support both query and response types as defined in clause 5.7.1. For the on-going triggered response query type, after sending the initial response, the ICF shall send a further response each time the permanent identifier provided in the initial query is associated or de-associated with a temporary identifier until the IQF deprovisions the query in the ICF.

The ICF shall support immediate deletion of identifier associations received in events for one or more IEF(s) when requested to do so by the LICF (proxied by the LIPF) over LI\_XEM1.

----------------------NEXT CHANGES---------------------

#### 6.2.2.4 IRI events

The IRI-POI present in the AMF shall generate xIRI, when it detects the following specific events or information:

- Registration.

- Deregistration.

- Location update.

- Identifier association.

- Start of interception with already registered UE.

- Unsuccessful communication related attempt.

NOTE: AMF reporting of UE state changes other than registration or deregistration is not supported in the present document.

The registration xIRI is generated when the IRI-POI present in an AMF detects that a target UE has successfully registered to the 5GS via 3GPP NG-RAN or non-3GPP access. The registration xIRI describes the type of registration performed (e.g. initial registration, periodic registration, registration mobility update) and the access type (e.g. 3GPP, non-3GPP). Unsuccessful registration shall be reported only if the target UE has been successfully authenticated.

The deregistration xIRI is generated when the IRI-POI present in an AMF detects that a target UE has deregistered from the 5GS. The deregistration xIRI shall indicate whether it was a UE-initiated or a network-initiated deregistration.

The location update xIRI is generated each time the IRI-POI present in an AMF detects that the target's UE location is updated due to target's UE mobility (e.g. in case of Xn based inter NG-RAN handover) or when the AMF observes target UE location information during some service operation (e.g., LCS, Location Reporting, or emergency services). The generation of such xIRI may be omitted if the updated UE location information is already included in other xIRIs (e.g. mobility registration) provided by the IRI-POI present in the same AMF. If the information in the AMF received over N2 (TS 38.413 [14]) includes one or more cell IDs, then all cell IDs shall be reported to the LEMF whenever location reporting is triggered at the AMF.

The identifier association xIRI is generated each time the IRI-POI in the AMF detects a SUCI or 5G-GUTI allocation change for a SUPI which is served by the AMF.

The start of interception with already registered UE xIRI is generated when the IRI-POI present in an AMF detects that interception is activated on the target UE that has already been registered in the 5GS.

When additional warrants are activated on a target UE, MDF2 shall be able to generate and deliver the start of interception with already registered UE related IRI messages to the LEMF associated with the warrants without receiving the corresponding start of interception with already registered UE xIRI.

The unsuccessful communication related attempt xIRI is generated when the IRI-POI present in an AMF detects that a target UE initiated communication procedure (e.g. session establishment, SMS) is rejected or not accepted by the AMF before the proper NF handling the communication attempt itself is involved. The unsuccessful communications related attempt xIRI is also generated when the IRI-POI present in the AMF detects that a PDU session modification request to convert a single access PDU session to a Multi-Access PDU (MA PDU) session is not accepted by the AMF and therefore not forwarded to the SMF.

The IRI-POI in the AMF shall support per target selective activation or deactivation of reporting of only identifier association xIRI independently of activation of LI for all other events. The IRI-POI in the AMF shall support activating location update xIRI in combination with identifier association xIRI only reporting.

----------------------NEXT CHANGES---------------------

#### 6.2.2.6 Specific IRI parameters

The list of parameters in each xIRI are defined in TS 33.128 [15]. The following give a summary.

The registration xIRI shall include the following:

- Registration type information.

- Access type information.

- Requested slice information.

The deregistration xIRI shall include the following:

- UE initiated de-registration.

- Access type information.

- Network initiated de-registration.

The location update xIRI shall include the following:

- Location of the target UE (see clause 7.3).

The identifier association xIRI shall include the following:

* Subscription permanent identifier.
* Temporary identifier association (i.e. SUCI or 5G-GUTI).
* Association change type indication.

The start of interception with already registered UE xIRI shall include the following:

- Access type information.

- Requested slice information.

The unsuccessful communication attempt xIRI shall include the following:

- Rejected type of communication attempt.

- Access type information.

- Failure reason.

When the access type is non-3GPP, the IP address used by the UE to reach the N3IWF shall be reported. The port shall also be reported if available.

----------------------NEXT CHANGES---------------------

### 6.2.2A Identifier Reporting for AMF

#### 6.2.2.1A General

The AMF shall provide IEF capabilities. The IEF present in the AMF shall support LI\_XEM1 interface and upon activation shall provide identity events to the ICF over LI\_XER interface.

The IEF shall not generate events prior to UEs being successfully registered by the AMF onto the network. For SUCIs seen during registration, they shall only be reported if UE registration is successfully completed.

#### 6.2.2.2A IEF Events

The IEF present in the AMF shall generate report records, when it detects the following specific events or information for any UE:

- An 5G-GUTI is allocated to a SUPI.

 - An 5G-GUTI is deallocated from a SUPI.

- A SUCI is successfully authenticated, re-registered or observed.

- A SUPI is deregistered from the network by the AMF or UDM informs AMF of de-registration.

- A SUPI is deregistered from the AMF due to AMF handover.

- A SUPI is registered on the AMF following AMF handover.

#### 6.2.2.3A IEF Event parameters

The list of event parameters is specified in TS 33.128 [15]. Each event shall include at the minimum the following information:

* Subscription permanent identifier.
* Observed temporary identifier(s).
* Cell identity (See clause 7.3).
* Time stamp of event.
* AMF identifier (including Region and Set Identifiers).
* Tracking area identifier
* Registration area (including tracking area identifier list).

The following additional information shall be included if it is available in the AMF when the event is reported to the ICF:

* Permanent equipment identifier.

#### 6.2.2.4A Network topologies

Since the IEF generates events independently of network topology for individual service usage UEs, no specific network topology handling is provided by the IEF. The IQF shall be responsible for handling any network topology requirements that may be applied by the LEA in an individual warrant.

----------------------NEXT CHANGES---------------------

#### 6.3.2.3 IRI events

The IRI-POI present in the MME shall generate xIRI, when it detects the applicable events specified in TS 33.107 [11].

In addition to the events specified in TS 33.107 [11] the MME shall generate xIRI, when it detects the following additional event;

* Identifier association.

The identifier association xIRI is generated each time the IRI-POI in the MME detects a GUTI allocation change for an IMSI which is served by the MME.

The IRI-POI in the MME shall support per target selective activation or deactivation of reporting of only identifier association xIRI independently of activation of LI for all other events. The IRI-POI in the MME shall support activating Tracking Area/EPS Location Update xIRI (as defined in TS 33.107 [11] clause 12.2.1.2) in combination with identifier association xIRI only reporting.

----------------------NEXT CHANGES---------------------

#### 6.3.2.5 Specific IRI parameters

The list of parameters in each xIRI are defined in TS 33.128 [15], for events which are imported from TS 33.107 [11] clause 12.2.1.2.

The identifier association xIRI shall include the following:

- IMSI.

- IMEI.

- Temporary identifier association (i.e. GUTI).

- Association change type indication.

----------------------NEXT CHANGES---------------------

## 7.1 General

Clause 7 provides details for the configuration of the high-level LI architecture for service layer based interception and for network function which are not specific to a single access type or network service (e.g. subscription management functions). It defines aspects of the LI configuration specific to each service under consideration, while aspects concerning network over which the service is delivered (e.g. 5G) are considered in clause 6.

----------------------NEXT CHANGES---------------------

### 7.3.1 General

This clause provides location reporting functionality for both UE location obtained as part of normal network access or user service usage and location actively triggered through location based services or other LALS reporting.

In addition, clause 7.3.4 describes Cell Supplemental Information (CSI) (e.g., civic address, geographical coordinates, or operator specific information) derived from CSP databases.

For all UE locations obtained, generated or reported to the MDF2, the POI shall report the time at which the location was established by the location source (e.g. AMF, MME or HSS/UDM) and provide this to the MDF along with the location information.

For all UE locations obtained, generated or reported to the ICF, the IEF shall report the time at which the location was established by the location source (e.g. AMF) and provide this to the ICF along with the location information.

----------------------NEXT CHANGES---------------------

## 7.4 Identity Caching Function

### 7.4.1 General

The ICF is responsible for receiving identity caching events from all IEFs in the network over the LI\_XER interface and handling queries from the IQF over the LI\_XQR interface to the IQF as defined in clause 5.7.

The temporary cache duration shall be configurable by the LICF on a per CSP network basis.

### 7.4.2 ICF Query Identities

The IQF present in the ADMF shall be able to query the records held by the ICF using one of the following target identifiers:

- SUPI.

- SUCI.

- 5G-S-TMSI.

- 5G-GUTI.

NOTE: Targeting based on GPSI, PEI, IMS identifiers or other legacy identifiers (e.g. MSISDN) is not supported by the present document as this information is not available in the ICF.

The list of event parameters is specified in TS 33.128 [15]. Each event shall include at the minimum the following information:

* Query target identifier.
* Time of target identifier observation.

For queries based on temporary identifiers the following additional information shall be included:

* Tracking area identifier.
* Cell identity.

### 7.4.3 ICF Response parameters

The list of event parameters is specified in TS 33.128 [15]. Each event shall include at the minimum the following information:

* Subscription permanent identifier.
* Related temporary identifier(s).
* Start of validity timestamp(s).
* End of validity timestamp(s).

The following additional information shall be included if it was available in the IEF records provided to the ICF:

* Permanent equipment identifier.

### 7.4.4 Network topologies

Since the ICF caches events independently of network topology for individual service usage UEs, no specific network topology handling is provided by the ICF. The IQF shall be responsible for handling any network topology requirements that may be applied by the LEA in an individual warrant.

----------THE END OF CHANGES, NO MORE, ONLY THE GREAT UNKNOWN BEYOND THIS POINT. THERE MIGHT BE DRAGONS----------