ETSI TR 133 928 V18.3.0 (2024-05)

5G;
ADMF logic for provisioning Lawful Interception (LI)
(3GPP TR 33.928 version 18.3.0 Release 18)

Reference
DTR/TSGS-0333928vi30

Keywords
5G,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

Introduction

The LI technical specifications (TS 33.126 [2], TS 33.127 [3], TS 33.128 [4]) contain the normative part of the LI requirements and the technical report TR 33.929 [5] contains additional information as an implementation guidance for LI. The ADMF that receives the warrant information from the Law Enforcement Agencies has the task of provisioning the LI functions present in various Network Functions (NFs) of the serving CSP network. Upon provisioning, the LI is activated in those NFs, and accordingly, the LI functions within those NFs monitor the target's communications and provide the LI as required by the warrant.

The scope of the NFs that provide the LI functions within the CSP network is determined based on various factors such as LI service type, CSP deployment choice, scope of LI as authorized in the warrant. The present document provides the logic used within the ADMF in provisioning the LI functions considering those points.

1 Scope

The present document provides ADMF provisioning logic for LI in association with the LI functions defined in TS 33.126 [2], TS 33.127 [3] and TS 33.128 [4].

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 33.126: "Lawful Interception Requirements".

[3] 3GPP TS 33.127: "Lawful Interception (LI) Architecture and Functions".

[4] 3GPP TS 33.128: "Lawful Interception (LI) Protocol and Procedures".

[5] 3GPP TR 33.929: "Lawful Interception (LI) Implementation Guidance".

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

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.2 Symbols

For the purposes of the present document, the following symbols apply:

None.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

4 ADMF and provisioning

4.1 Overview

According to the LI model defined in ETSI TS 103 221-1 [6], the ADMF as an administration function establishes and manages the Lawful Interception (LI). In doing so, the ADMF performs the target provisioning at various Network Elements (NEs) using the X1 protocol as defined in ETSI TS 103 221-1 [6].

Within the LI architecture model defined in TS 33.127 [3] and TS 33.128 [4], the ADMF has two sub-functions referred to as Lawful Interception Control Function (LICF) and Lawful Interception Provisioning Function (LIPF). The LICF receives the warrant information from the LEA over LI_HI1 interface. The LIPF performs the provisioning of all LI functions within various NFs of CSP network including the MDF2 and MDF3. See figure 4.1-1 below for an overview.

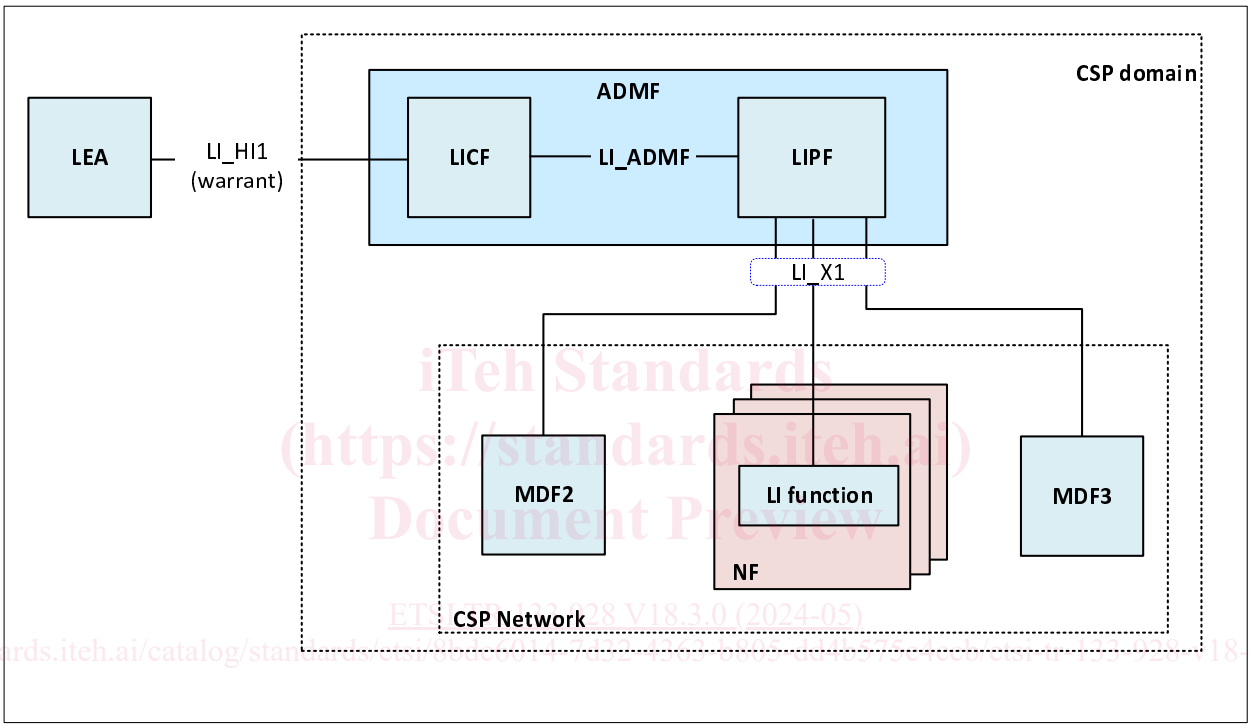

Figure 4.1-1: LIPF in ADMF provisioning of NEs

With respect to the LI model of ETSI 103 221-1 [6], the LIPF plays the role of ADMF (as defined in ETSI 103 221-1 [6], and the LI functions (within the NFs) MDF2, and MDF3 play the role of NE (as defined in ETSI 103 221-1 [6]).

The present document focuses on LIPF provisioning logic of LI functions, MDF2, MDF3 over the LI_X1. Henceforth, the term LIPF logic is used in the present document. See clause 5 for details of LIPF logic.

4.2 General

A separate box is used to represent each of the NF in which an LI function is provisioned by the LIPF. In the illustration shown below in figure 4.2-1, P-CSCF and MGCF are two NFs and are represented by two separate boxes.

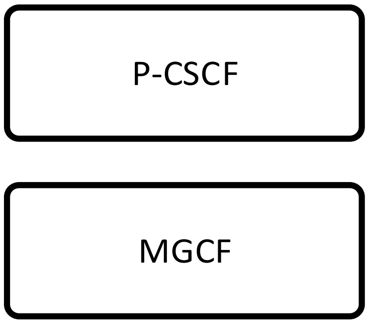

Figure 4.2-1: Separate box for each NF that has the LI function

The LI function present within a NF and provisioned by the LIPF is represented within the parenthesis. In the illustration shown in figure 4.2-2, the IRI-POI in P-CSCF and IRI-POI in MGCF are provisioned by the LIPF.

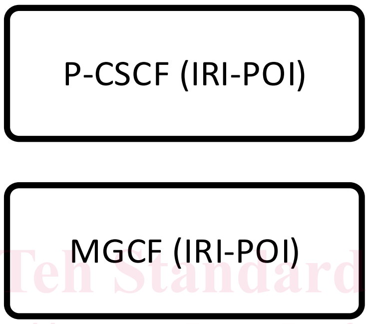

Figure 4.2-2: LI function as applicable to the NF

The possible target identities that are applicable to the LI function present in a NF are represented within another parenthesis that begin with "Target Id:". In the illustration shown in figure 4.2-3, the possible target identities for an IRI-POI in P-CSCF and IRI-POI in MGCF are PEI (IMEI only), IMEI, IMPU and IMPI.

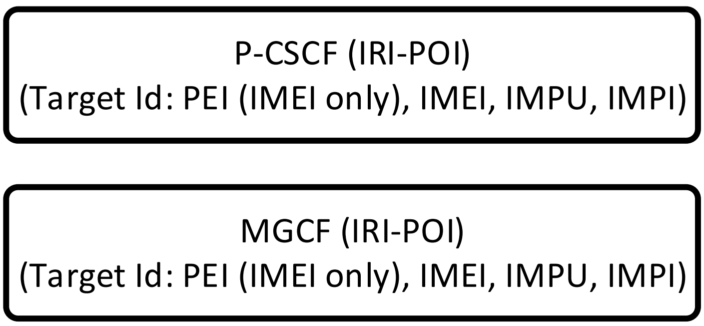

Figure 4.2-3: Possible target identifiers are in parentheses

Some of the flow-charts have a callout description shown next to the provisioned box. The text within the callout description provides a hint on the conditions that would enable the LI function to provide the interception. When such a condition for the interception is obvious, no such call-out description is provided. In the illustration shown in figure 4.2-4, no callout description is given for the IRI-POI of P-CSCF implying no further clarity is needed. The callout description for the IRI-POI in MGCF is to hint that the IRI-POI in an MGCF is used only when an IMS session is redirected to a CS domain (see TR 33.929 [5]).

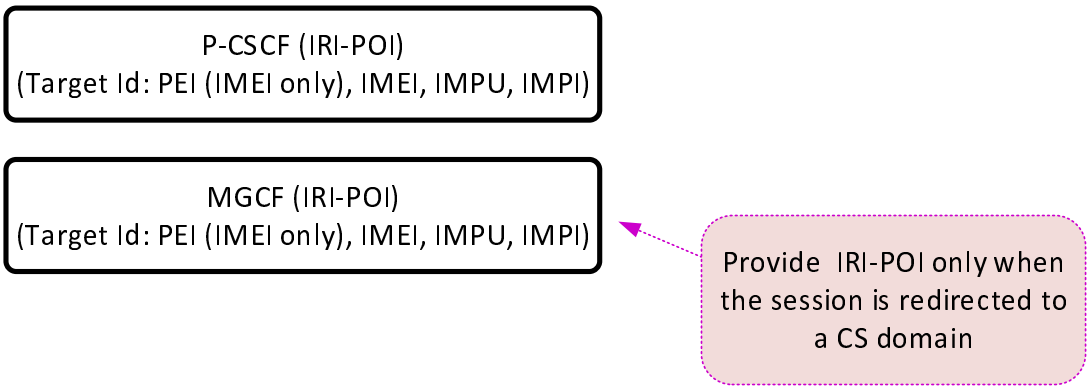

Figure 4.2-4: Call out next to the NF describe the conditionality of interception

The conditions given inside the call-out description are outside the scope of LIPF logic. However, the LIPF logic is aware of the condition in an overall scheme of things.

Most of the flow-charts have follow up tables that identify the scope of NF domain in providing the LI functions.

In the illustration shown in table 4.2-1:

- P-CSCF has CC-TF in a non-roaming case, has IRI-POI (for non-emergency services only) and CC-TF in VPLMN with LBO and CC-TF (for emergency services only) in VPLMN with HR (home-routed).
- MGCF has CC-TF in a non-roaming case, CC-TF in HPLMN with roaming (both LBO and HR) when an incoming session is redirected over a CS domain.
- IMS-AGW has CC-POI when P-CSCF has the CC-TF and IM-MGW has the CC-POI whenever the MGCF has the CC-TF.

Note that for each clause the relevant table is to be used as an aid to understand the LIPF logic and it is outside the scope of LIPF logic. However, the LIPF logic is aware of the condition in an overall scheme of things.

Table 4.2-1: Scope of NF domain that provide the LI functions

NFs with LI function	Non-roaming	Roaming with LBO		Roaming with HR	
		VPLMN	HPLMN	VPLMN	HPLMN
P-CSCF	n/a	IRI-POI (NOTE 1)	n/a	n/a	n/a
P-CSCF	CC-TF	CC-TF	n/a	CC-TF (NOTE 2)	n/a
IMS-AGW	CC-POI	CC-POI	n/a	CC-POI (NOTE 2)	n/a
MGCF (NOTE 3)	CC-TF	n/a	CC-TF	n/a	CC-TF
IM-MGW (NOTE 3)	CC-POI	n/a	CC-POI	n/a	CC-POI

NOTE 1: For non-emergency sessions only.

NOTE 2: For emergency sessions only.

NOTE 3: Only when an incoming session to a target is redirected over a CS domain.

4.3 Destination end points

As a part of the LI provisioning task, the LIPF first provisions the LI functions with the destination end points for the delivery of the appropriate intercepted data on the LI interfaces that those LI functions support.

Table 4.3-1 provides the destination end points for each of the LI interfaces defined in TS 33.127 [3] and TS 33.128 [4].

Table 4.3-1: Destination end points

LI interface	Destination end point	Source LI function
LI_HI2	LEMF	MDF2
LI_HI3	LEMF	MDF3
LI_HI4	LEMF	MDF2, MDF3
LI_X2	MDF2	IRI-POI, LI_LCS Client, LMISF-IRI
LI_X2_LA	MDF2	LARF
LI_X3	MDF3	CC-POI, CC-PAG
LI_X2_LITE	LMISF-IRI	BBIFF-C, BBIFF
LI_X3_LITE_S	LMISF-IRI	BBIFF-U, BBIFF
LI_X3A	CC-PAG	CC-POI

NOTE: The present document is on the provisioning of various LI functions (i.e. on LI_X1 interface) and as such delivery end point is not applicable to LI_X1 or the triggering interfaces (i.e. LI_T2, LI_T3).

If the same destination end point is used for one or more intercepts, then the provisioning of that destination end point at an LI function is done only once. If the same destination end point is used on multiple interfaces at an LI function, then the provisioning of that destination end point at that LI function is done only once (e.g. the same LEMF as the destination end from MDF2 for LI_HI2 and LI_HI4).

The present document assumes that the required provisioning is done as per the above table prior to any provisioning and these aspects are not shown in the illustrative LIPF logic diagrams.

5 LIPF logic

5.1 Background

According to TS 33.126 [2] clause 6.4, the CSP is expected to only deliver Interception Product relating to specific CSP services. In other words, the CSP is expected to perform the interception only for the services required by the warrant. The interception may be performed for more than one service when required by the warrant.

NOTE: The term "interception" used in the present document refers to the step that involves actual capturing and then delivery of the Intercept Product to the LEMF.

This clause considers the following possibilities in the analysis:

- The intended target may have subscribed to only a specific service and in this case, by default, the interception would apply only to such service when specified in the warrant. The CSP network would provide the interception as and when the service is accessed by the target.

- The intended target may have subscribed to multiple services and in this case, the interception would have to be done based on the service type(s) specified in the warrant as and when CSP network detects that such services are accessed by the target.

- A NF may be involved in providing only a particular service and in this case, by default, the interception performed by the POI present in that NF would apply to such service when specified in the warrant.

- A NF may be involved in providing multiple services and in this case, the interception performed by the POI present in that NF would have to be based on the service type applicable to the warrant.

- There may be multiple warrants with differing service types active on a target, in this case, all applicable services would have to be intercepted at the POIs, and the MDFs would have to then deliver Interception Product based on the service type (s) applicable to the warrant.

In supporting the above scenarios, as per clause 4.4 of TS 33.128 [4], the LIPF will have to provision the POIs, TFs and the MDF2/MDF3 according to the CSP service type(s) applicable to a warrant.

To cover all the scenarios mentioned above, the service type may have to be part of LI provisioning data sent to the MDFs. Whether a service type will have to be provisioned to the POIs and TFs as an indication will depend on the services provided by the NFs that have such POIs and TFs.

In addition to the CSP service type, a few other factors present in the warrant may influence the LIPF logic in provisioning the POIs, TFs and MDF2/MDF3. Few examples are:

- Delivery type.
- LALS triggering.
- CSP deployment options.
- The target type (local Vs non-local ID).

For the target non-local ID, Voice, RCS and Messaging type of services are supported in the present document. In this case, the other party communicating with the target non-local ID happens to access the service provided by the CSP.

This clause illustrates the LIPF logic through a series of flow-charts in provisioning the POIs and the TFs. The provisioning aspect of MDF2/MDF3 are not shown unless such details provide additional clarity. For a given warrant, the provisioning of MDF2 and MDF3 are done before the provisioning of LI functions (e.g. POIs).

5.2 Governing scenarios

With respect to the interception performed within the CSP network, there are five scenarios:

1. The target (or party communicating with a target non-local ID) is non-roaming.
2. The target (or party communicating with a target non-local ID) is outbound roaming with HR.
3. The target (or party communicating with a target non-local ID) is outbound roaming with LBO.
4. The target (or party communicating with a target non-local ID) is inbound roaming with HR.
5. The target (or party communicating with a target non-local ID) is inbound roaming with LBO.

Scenario 4 is also referred to as N9HR or S8HR, depending on whether the packet core is 5GC or EPC. As indicated clause 5.1, a target can be a non-local ID only when the service type is Voice or Messaging.

The same NF that provides an LI function may be present in one or more of the above scenarios. The LIPF logic, even though may not be aware of the roaming nature of a target, will have to accommodate the above five scenarios while provisioning the LI functions.

5.3 Top-level LIPF provisioning logic

5.3.1 LIPF logic for initial configuration

The provisioning for Identity Association Caching is considered as a part of initial configuration. Likewise, part of the S8HR/N9HR LI also requires some initial configuration (see clause 5.5.2).

The details of initial configuration for N9HR/S8HR are illustrated in figure 5.5.2-1 (clause 5.5.2). The initial configuration of Identity Association Caching is required if and only if the CSP has deployed the Identity Association Caching service. Likewise, the initial configuration for N9HR/S8HR is required if and only if the interception of voice calls for inbound roaming targets is required in a home-routed roaming scenario.

5.3.2 LI provisioning logic in LIPF

When Location Acquisition service is deployed in the CSP network, a warrant may be received to authorize Location Acquisition service for the targeted user. This may be a standalone warrant of its own or may be tagged along with the warrant issued to perform the service-based interception.

The details of LI provisioning logic for Location Acquisition are illustrated in clause 5.9. The details of service-based LI provisioning logic in LIPF are illustrated in clause 5.3.3.

5.3.3 Service-based LI provisioning logic in LIPF

The flow-chart in figure 5.3-1 shows a top-level logic within the LIPF to branch off into separate processes according to the service type defined in the present document.

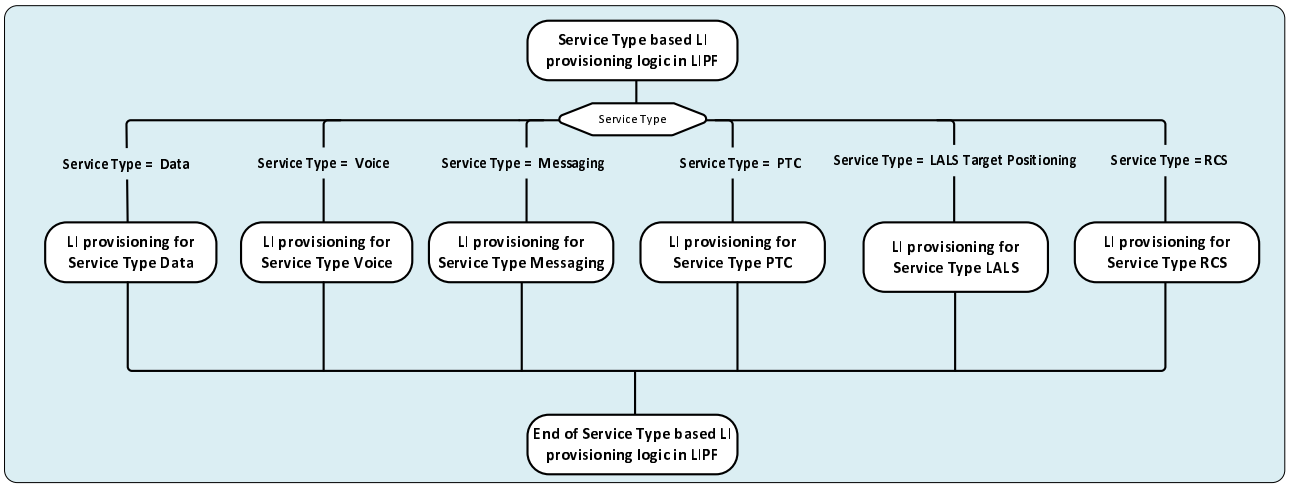

Figure 5.3.3-1: Top-level view of LIPF logic in handling the service type

Based on the LI functionality defined in the present document:

- For the service type of Data, it is assumed that the NFs in the packet core network are involved and hence, provide the IRI and CC interception.
- For the service type of Voice, it is assumed that the NFs in the IMS domain are involved and hence, provide the IRI and CC interception.
- For the service type of Messaging (that includes SMS and MMS), the NFs in the packet core network, IMS or MMS Proxy Relay are involved and hence, provide the IRI and CC interception. The interception of SMS has only the IRIs. For, the service type of Messaging, the LI provisioning for the service type RCS is also done (see below) if supported and applicable to the target.
- For the service type of PTC, the PTC Server is involved and hence, provides the IRI and CC interception.
- For the service type of LALS, the LI-LCS Client provides the IRI interception, and the CC interception does not apply to LALS.

  For the service type RCS, the RCS Server, the HTTP Content Server, the File Transfer Localization Function are involved and hence, provide the IRI and CC interception.

When the service type "Messaging" is explicitly specified in a warrant, the provisioning for the service type RCS is also performed by the LIPF, if the latter is supported and applicable to the target. If the warrant explicitly includes both "Messaging" and "RCS" as the service types, the LI provisioning for the service type RCS is done only once.

The UDM and HSS are also the NFs that have the IRI-POI and the provisioning of IRI-POI in UDM and HSS is independent of the service type indicated in the warrant as long as the target is not indicated as a non-local ID. The provisioning of IRI-POI in the UDM and HSS for a target identifier is done only once.

When multiple service types are applicable for a target identifier, the LIPF may provision the LI function in a NF only once including all the applicable service types. Alternatively, the LIPF may determine the services that need to be intercepted at the LI function present in a NF and then provision that LI function for all services together.

5.3.4 Location Acquisition

Figure 5.3.4-1 shows the LIPF logic in provisioning the LI functions for Location Acquisition.

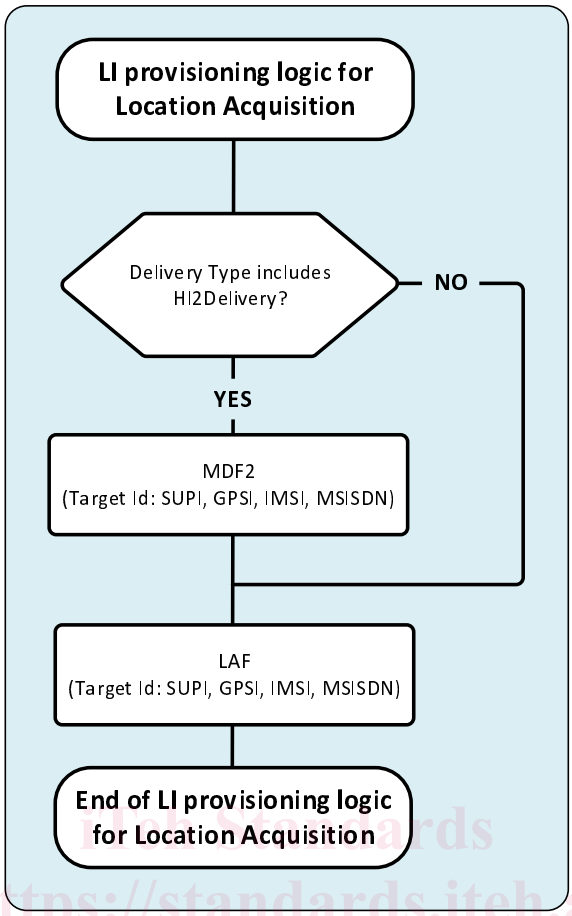

Figure 5.3.4-1: LIPF logic for Location Acquisition

The LAF is a Location Acquisition specific LI function present in the ADMF. Therefore, the provisioning of LAF is treated as internal to the ADMF. The provisioning of MDF2 is required if and only if the delivery method for Location Acquisition includes IRI-based reporting which is indicated with the Delivery Type of HI2Delivery.

The target identity SUPI collectively represents the SUPIIMSI and SUPINAI. The target identity GPSI collectively represents the GPSIMSISDN and GPSINAI.

5.4 Data

5.4.1 Scope of interception

For the service type of Data, the NFs present in the packet core network provide the LI functions. This clause illustrates the LIPF logic for 5GC and EPC as the two packet core networks.

The interception of service type of Data includes:

- Delivery of IRI, or CC based on the delivery type indicated in the warrant.
- When required, the delivery of packet data header reporting.
- When required, the delivery of LALS reports based on the LALS triggering.

The CSP may have differing implementation options for the packet data header reporting and LALS triggering.

In the case of EPC, the CSP may also have differing deployment options in choosing the NFs (SGW-based Vs PGW-based) that provide the interception.