ETSI TS 133 127 V16.7.0 (2021-04)

LTE;
5G;
Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
Lawful Interception (LI) architecture and functions
(3GPP TS 33.127 version 16.7.0 Release 16)

Reference
RTS/TSGS-0333127vg70

Keywords
5G,GSM,LTE,SECURITY,UMTS

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 Specification (TS) 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 http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 8
Introduction 8
1 Scope 9
2 References 9
3 Definitions, symbols and abbreviations 10
3.1 Definitions 10
3.2 Symbols 11
3.3 Abbreviations 11
4 Requirements realisation 13
5 Functional architecture 13
5.1 General 13
5.2 High-level generic LI architecture 13
5.3 Functional entities 14
5.3.1 Law Enforcement Agency (LEA) 14
5.3.2 Point of Interception (POI) 15
5.3.2.1 General 15
5.3.2.2 Directly provisioned and triggered POIs 15
5.3.2.3 IRI-POIs and CC-POIs 15
5.3.2.4 Failure handling 15
5.3.3 Triggering Function 15
5.3.4 Mediation and Delivery Function (MDF) 16
5.3.5 Administration Function (ADMF) 16
5.3.5.1 General 16
5.3.5.2 LICF 17
5.3.5.3 LIPF 17
5.3.5.4 IQF 18
5.3.5.5 LI Function Selection 18
5.3.6 System Information Retrieval Function (SIRF) 18
5.3.7 LEMF – Law Enforcement Monitoring Facility 19
5.4 LI interfaces 19
5.4.1 General 19
5.4.2 Interface LI_SI 20
5.4.3 Interface LI_HI1 20
5.4.4 Interface LI_X1 20
5.4.4.1 General 20
5.4.4.2 LIPF and POI 20
5.4.4.3 LIPF and TF 21
5.4.4.4 LIPF and MDF2/MDF3 21
5.4.5 Interface LI_X2 21
5.4.6 Interface LI_X3 21
5.4.7 Interface LI_T 22
5.4.7.1 General 22
5.4.7.2 Interface LI_T2 22
5.4.7.3 Interface LI_T3 22
5.4.8 Interface LI_HI2 22
5.4.9 Interface LI_HI3 22
5.4.10 Interface LI_HI4 23
5.4.10.1 General 23
5.4.10.2 LI operation notification 23

5.4.10.3 Contents of the notification 23
5.4.11 Interface LI_ADMF 23
5.4.12 Interface LI_MDF 23
5.4.13 Interface LI_IQF 23
5.4.14 Interface LI_XQR 23
5.4.15 Interface LI_HIQR 24
5.4.16 Interface LI_XER 24
5.4.17 Interface LI_XEM1 24
5.5 LI service discovery 25
5.6 LI in a virtualised environment 25
5.6.1 General 25
5.6.2 Virtualised deployment architecture 25
5.6.3 LI function instantiation and lifecycle management procedures 27
5.6.3.1 Controller virtualisation layer and MANO procedures 27
5.6.3.1.1 Responsibilities 27
5.6.3.1.2 General procedures 27
5.6.3.1.3 Instantiation 27
5.6.3.1.4 Modification 28
5.6.3.1.5 Termination 28
5.6.3.1.6 Direct instantiation of LI Functions by ADMF 28
5.6.3.2 LI_X0 procedures 28
5.6.3.3 Exception Procedures 30
5.7 Identifier association and reporting 31
5.7.1 General 31
5.7.2 Functional entities 32
5.7.2.1 Identity Query Function (IQF) 32
5.7.2.2 Identity Event Function (IEF) 32
5.7.2.3 Identity Caching Function (ICF) 33

6 Network layer based interception 34
6.1 General 34
6.2 5G 34
6.2.1 General 34
6.2.2 LI at AMF 35
6.2.2.1 Architecture 35
6.2.2.2 Target identities 36
6.2.2.3 Identity privacy 37
6.2.2.4 IRI events 37
6.2.2.5 Common IRI parameters 38
6.2.2.6 Specific IRI parameters 38
6.2.2.7 Network topologies 39
6.2.2A Identifier Reporting for AMF 39
6.2.2A.1 General 39
6.2.2A.2 IEF Events 39
6.2.2A.3 IEF Event parameters 39
6.2.2A.4 Network topologies 40
6.2.3 LI for SMF/UPF 40
6.2.3.1 Architecture 40
6.2.3.2 Target identities 42
6.2.3.3 IRI events 42
6.2.3.4 Common IRI parameters 42
6.2.3.5 Specific IRI parameters 43
6.2.3.6 Network topologies 43
6.2.3.7 Multi-Access PDU (MA PDU) Session Specific 43
6.2.4 LI at UDM for 5G 44
6.2.5 LI at SMSF 44
6.2.5.1 Architecture 44
6.2.5.2 Target identities 45
6.2.5.3 IRI events 45
6.2.5.4 Common IRI parameters 45
6.2.5.5 Specific IRI parameters 45
6.2.5.6 Network topologies 45

6.2.6 LI support at NRF 46
6.2.6.1 Architecture 46
6.2.6.2 LI_SI notifications 46
6.2.6.3 LI_SI parameters 47
6.2.7 External data storage 47
6.3 EPC 47
6.3.1 General 47
6.3.2 LI at the MME 48
6.3.2.1 Architecture 48
6.3.2.2 Target identities 48
6.3.2.3 IRI events 49
6.3.2.4 Common IRI parameters 49
6.3.2.5 Specific IRI parameters 49
6.3.2.6 Network topologies 49
6.3.3 LI at SGW/PGW 49
6.3.3.1 Architecture 49
6.3.3.2 Target identities 51
6.3.3.3 IRI events 51
6.3.3.4 Common IRI parameters 51
6.3.3.5 Specific IRI parameters 52
6.3.3.6 Network topologies 52
6.3.4 LI at ePDG 52
6.3.4.1 Architecture 52
6.3.4.2 Target identities 53
6.3.4.3 IRI events 53
6.3.4.4 Common IRI parameters 54
6.3.4.5 Specific IRI parameters 54
6.3.4.6 Network topologies 54
6.4 3G 54
6.5 VoNR 54
6.6 4G/5G Interworking 55

7 Service layer based interception 55
7.1 General 55
7.2 Central subscriber management 55
7.2.1 General 55
7.2.2 LI at UDM 56
7.2.2.1 Architecture 56
7.2.2.2 Target identities 57
7.2.2.3 Identity privacy 57
7.2.2.4 IRI events 57
7.2.2.5 Common IRI parameters 57
7.2.2.6 Specific IRI parameters 58
7.2.2.7 Network topologies 58
7.2.3 LI at HSS 58
7.2.3.1 Architecture 58
7.2.3.2 Target identities 59
7.2.3.3 IRI events 60
7.2.3.4 Common IRI parameters 60
7.2.3.5 Specific IRI parameters 60
7.2.3.6 Network topologies 60
7.3 Location 60
7.3.1 General 60
7.3.2 Service usage location reporting 60
7.3.2.1 General 60
7.3.2.2 Embedded location reporting 60
7.3.2.3 Separated location reporting 61
7.3.3 Lawful Access Location Services (LALS) 61
7.3.3.1 General 61
7.3.3.2 Target positioning 62
7.3.3.2.1 General 62
7.3.3.2.2 Immediate location provision 62

7.3.3.2.3 Periodic location provision 62
7.3.3.3 Triggered location 63
7.3.3.4 LI_X2 interface for target positioning and triggered location 64
7.3.4 Cell database information reporting 64
7.4 IMS 65
7.4.1 General 65
7.4.2 Architecture 66
7.4.2.1 Overview 66
7.4.2.2 Target identities 67
7.4.2.3 Target identification 68
7.4.3 IRI-POI 68
7.4.3.1 General 68
7.4.3.2 IRI events 68
7.4.3.3 Common IRI parameters 69
7.4.3.4 Specific IRI parameters 69
7.4.4 CC-TF and CC-POI 69
7.4.4.1 General 69
7.4.4.2 CC intercept trigger 69
7.4.4.3 Common CC parameters 70
7.4.5 Correlation of xCC and xIRI 70
7.4.6 Network topologies 70
7.4.6.1 General 70
7.4.6.2 IMS Network Functions providing the IRI-POI 70
7.4.6.3 IMS Network Functions providing the CC-TF and CC-POI functions 72
7.4.7 Roaming cases 73
7.4.7.1 Media unavailable in a roaming case 73
7.4.7.2 S8HR 73
7.4.7.2.1 Background 73
7.4.7.2.2 LI architecture 74
7.4.7.2.3 S8HR LI Process 74
7.4.7.2.4 CC intercept trigger 74
7.4.7.2.5 S8HR LI and Target UE Mobility 75
7.4.7.3 N9HR 75
7.4.7.3.1 Background 75
7.4.7.3.2 LI architecture 75
7.4.7.3.3 N9HR LI Process 75
7.4.7.3.4 CC intercept trigger 76
7.4.7.3.5 N9HR LI and Target UE Mobility 76
7.4.7.4 LI in VPLMN with home-routed roaming architecture 76
7.4.7.4.1 Background 76
7.4.7.4.2 LI architecture 77
7.4.7.4.3 Target identifiers 77
7.4.7.4.4 Target identification 77
7.4.7.4.5 IRI events 77
7.4.7.4.6 IRI parameters 77
7.4.7.4.7 CC intercept trigger 78
7.4.7.4.8 CC parameters 78
7.4.7.4.9 Correlation of xCC and xIRI 78
7.4.7.4.10 LI specific functions and interfaces 78
7.4.7.4.11 LI Process 79
7.4.7.4.12 Target UE Mobility 80
7.5 MMS 80
7.5.1 Overview 80
7.5.2 LI at MMS Proxy-Relay 80
7.5.2.1 Architecture 80
7.5.2.2 Target Identities 80
7.5.2.3 IRI Events 81
7.5.2.4 Common IRI parameters 81
7.5.2.5 Specific IRI parameters 81
7.5.2.6 CC 81
7.5.2.7 Network Topologies 81
7.6 PTC service 81

7.6.1 General....81
7.6.2 Target identities....82
7.6.3 IRI events....82
7.6.4 Common IRI parameters....83
7.6.5 Specific IRI parameters....83
7.6.6 Common CC parameters....83
7.6.7 Specific CC parameters....83
7.6.8 Network topologies....83
7.7 Identity Caching Function....83
7.7.1 General....83
7.7.2 ICF Query Identities....84
7.7.3 ICF Response parameters....84
7.7.4 Network topologies....84

8 LI security and deployment considerations....84
8.1 Introduction....84
8.2 Architectural alternatives....85
8.2.1 Full target list at every POI node....85
8.2.2 Full target list only in LICF....85
8.2.3 Provisioning for registered users....85
8.3 LI key management at ADMF....85
8.3.1 General....85
8.3.2 Key management....85
8.4 Virtualised LI security....86
8.4.1 General....86
8.4.2 NFVI and host requirements....86
8.4.3 Virtualised LI function implementation....86
8.4.4 Container based deployments....86
8.5 Points of Interception....86
8.6 Deployment considerations....87
8.6.1 General....87
8.6.2 CC-PAG....87

Annex A (informative): 5G LI network topology views....89

A.1 Non-roaming scenario....89
A.1.1 General....89
A.1.2 Service-based representation with point-to-point LI system....89

A.2 Interworking with EPC/E-UTRAN....90
A.2.1 General....90
A.2.2 Topology view for a non-roaming scenario....91

A.3 Multiple DN connections in a PDU session....93
A.3.1 General....93
A.3.2 Topology view for a non-roaming scenario....93

A.4 Non-3GPP access in a non-roaming scenario....95
A.4.1 General....95
A.4.2 Topology view....95

Annex B (normative): ADMF functionality....97

Annex C (informative): LEA initiated suspend and resume....98

Annex Z (informative): Change history....99

History....100

Foreword

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

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document has been produced by the 3GPP TSG SA to standardise Lawful Interception of telecommunications. The present document specifies the architecture and functions required to support Lawful Interception in 3GPP networks. Lawful Interception shall always be done in accordance with the applicable national or regional laws and technical regulations. Such national laws and regulations define the extent to which functional capabilities in the present document are applicable in specific jurisdictions.

1 Scope

The present document specifies both the architectural and functional system requirements for Lawful Interception (LI) in 3GPP networks. The present document provides an LI architecture supporting both network layer based and service layer based Interception.

National regulations determine the specific set of LI functional capabilities that are applicable to a specific 3GPP operator deployment.

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".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP 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 3GPP TR 21.905 [1].

Content of Communication (CC): The content of communication as forwarded from the Mediation and Delivery Function 3 (over the LI_HI3 interface) to the Law Enforcement Monitoring Facility.

CUPS: As defined in 3GPP TS 23.214 [12], represents PLMN with architecture enhancements for control and user plane separation of EPC nodes.

Intercept Related Information (IRI): The intercept related information as forwarded from the Mediation and Delivery Function 2 (over the LI_HI2 interface) to the Law Enforcement Monitoring Facility.

IRI event: The network procedure or event that created an xIRI in the Point Of Interception.

LI component: The function and equipment involved in handling the Lawful Interception functionality in the CSP's network.

Lawful Interception Identifier (LIID): Unique identifier that associates a warrant to Lawful Interception Product delivered by the CSP to the LEA.

LI system: The collection of all LI components involved in handling the Lawful Interception functionality in the CSP's network.

Non-local ID: An identity assigned and managed at a different CSP than the CSP performing LI.

Provisioning: The action taken by the CSP to provide its Lawful Interception functions information that identifies the target and the specific communication services of interest to the LEA, sourced from the LEA provided warrant.

Triggering: The action taken by a dedicated function (Triggering Function) to provide another dedicated function (Triggered POI), that Provisioning could not directly be applied to, with information that identifies the specific target communication to be intercepted.

Warrant: The formal mechanism to require Lawful Interception from a LEA served to the CSP on a single target identifier. Depending on jurisdiction also known as: intercept request, intercept order, lawful order, court order, lawful order or judicial order (in association with supporting legislation).

xCC: The content of communication as forwarded from the Point Of Interception (over the LI_X3) interface to the Mediation and Delivery Function 3.

xIRI: The intercept related information as forwarded from the Point Of Interception (over the LI_X2) interface to the Mediation and Delivery Function 2.

3.2 Symbols

3.3 Abbreviations

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

5GC	5G Core Network
5GS	5G System
ADMF	LI Administration Function
AMF	Access and Mobility Management Function
AS	Application Server
AUSF	Authentication Server Function
BBIFF	Bearer Binding Intercept and Forward Function
BSS	Business Support System
CAG	Closed Access Group
CC	Content of Communication
CP	Control Plane
CSI	Cell Supplemental Information
CSP	Communication Service Provider
CUPS	Control and User Plane Separation
DN	Data Network
DNAI	Data Network Access Identifier
E-CSCF	Emergency – Call Session Control Function
GPSI	Generic Public Subscription Identifier
HMEE	Hardware Mediated Execution Enclave
HR	Home Routed
IBCF	Interconnection Border Control Functions
ICF	Identifier Caching Function
IEF	Identifier Event Function
IMS-AGW	IMS Access Gateway
IM-MGW	IM Media Gateway
IP	Interception Product
IQF	Identifier Query Function
IRI	Intercept Related Information
LALS	Lawful Access Location Services
LBO	Local Break Out
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LI CA	Lawful Interception Certificate Authority
LICF	Lawful Interception Control Function
LI_HI1	Lawful Interception Handover Interface 1
LI_HI2	Lawful Interception Handover Interface 2
LI_HI3	Lawful Interception Handover Interface 3
LI_HI4	Lawful Interception Handover Interface 4
LI_HIQR	Lawful Interception Handover Interface Query Response
LIID	Lawful Interception Identifier
LIPF	Lawful Interception Provisioning Function

LIR	Location Immediate Request
LI_SI	Lawful Interception System Information Interface
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

4 Requirements realisation

The LI architecture set out in the present document is designed to allow CSP deployments to meet the set of LI requirements described in TS 33.126 [3] that are determined to be applicable by the relevant national regulation for that deployment. For more details on the relationship between LI requirements and national legislation, see TS 33.126 [3] clause 4.

A CSP may deploy different network technologies or services considered in the present document. A CSP should consider each of these network technologies or services separately with respect to the present document, bearing in mind that a different subset of LI requirements may apply according to relevant national legislation, and that a warrant may require the CSP to intercept multiple network technologies or services.

5 Functional architecture

5.1 General

The following clauses describe the high-level functional architecture for LI for 3GPP-defined services and network technologies. It describes the architectural elements necessary for LI, their roles and responsibilities, and the interfaces and interactions between them.

Clauses 6 and 7 of the present document describe how the LI for various 3GPP-defined network technologies and services are realised within the generic LI architecture, including associations of LI architectural elements with the network functions involved.

Not all LI architectural elements and interfaces are used in all network technologies and services.

5.2 High-level generic LI architecture

The overall conceptual view of LI architecture is shown in figure 5.2-1 below.

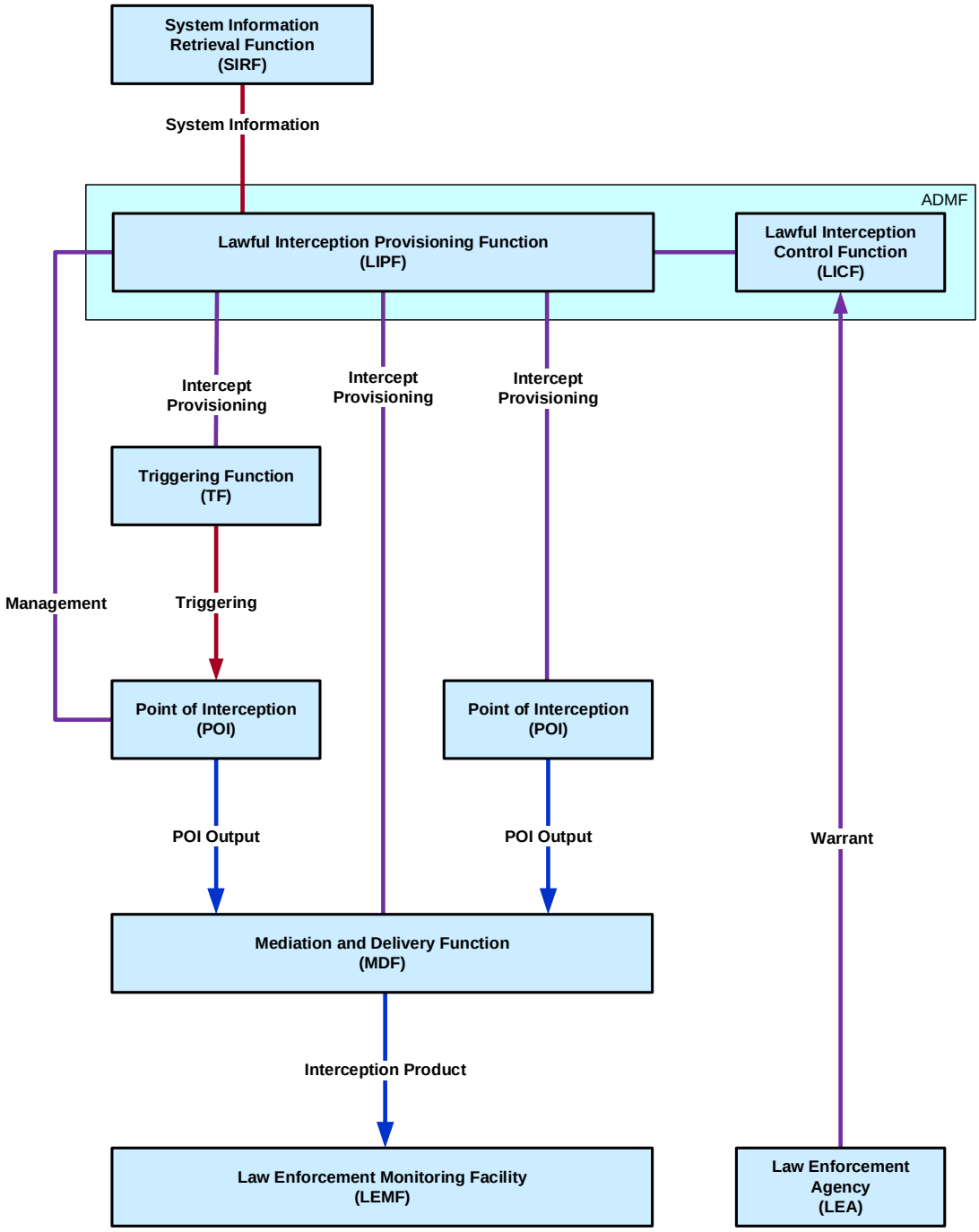

Figure 5.2-1: A high-level generic view of LI architecture

The functional entities of the architecture are described in more detail in clause 5.3 below. Details of the specific interfaces between these entities are described in clause 5.4.

5.3 Functional entities

5.3.1 Law Enforcement Agency (LEA)

In general the LEA is responsible for submitting the warrant to the CSPs, although in some countries the warrant may be provided by a different legal entity (e.g. judiciary).

5.3.2 Point of Interception (POI)

5.3.2.1 General

The **Point of Interception (POI)** detects the target communication, derives the intercept related information or communications content from the target communications and delivers the POI output as xIRI to the MDF2 or as xCC to the MDF3. The output of a POI is determined by the type of the NF associated with the POI. A POI may be embedded within a Network Function (NF) or separate from a NF with which it is associated.

Multiple POIs may have to be involved in executing a warrant.

5.3.2.2 Directly provisioned and triggered POIs

POIs are divided into two categories:

- Directly provisioned POIs are provisioned by the LIPF.
- Triggered POIs are triggered by a Triggering Function (TF) (see clause 5.3.3).

The directly provisioned POIs detect the target's communications that need to be intercepted, and then derive the intercept related information or communication contents from that target communications depending on the POI type (see clause 5.3.2.3). The triggered POIs detect the target communications based on the trigger received from an associated Triggering Function and then derives the intercept related information or communication contents of target communications depending on the POI type (see clause 5.3.2.3).

5.3.2.3 IRI-POIs and CC-POIs

POIs are divided into two types for each category based on the type of data they send to the MDF (see clause 5.3.4):

- IRI-POI delivers xIRI to the MDF2.
- CC-POI delivers xCC to the MDF3.

Both IRI-POIs and CC-POIs are either directly provisioned or triggered (see clause 5.3.2.2).

In the present document, an xIRI is identified with the event that has caused its generation within the IRI-POI.

5.3.2.4 Failure handling

In case a network procedure involving the target UE and requiring the generation of an xIRI fails, the IRI-POI shall be able to report the failure reason available from the involved network protocol.

5.3.3 Triggering Function

The **Triggering Function (TF)** is provisioned by the LIPF and is responsible for triggering triggered POIs in response to network and service events matching the criteria provisioned by the LIPF. The Triggering Function detects the target communications and sends a trigger to the associated triggered POI.

As a part of this triggering, the Triggering Function shall send all necessary interception rules (i.e. rules that allow the POIs to detect the target communications), forwarding rules (i.e. MDF2, MDF3 address), target identity, and the correlation information.

A Triggering Function may interact with other POIs to obtain correlation information. Details of this interface are not specified by the present document.

The Triggering Function that triggers CC-POI is referred to as a CC-TF and the Triggering Function that triggers an IRI-POI is referred to as IRI-TF.

5.3.4 Mediation and Delivery Function (MDF)

The **Mediation and Delivery Function (MDF)** delivers the Interception Product to the Law Enforcement Monitoring Facility (LEMF).

Two variations of MDF are defined: MDF2 and MDF3.

MDF2 generates the IRI messages from the xIRI and sends them to one or more LEMFs. The MDF3 generates the CC from the xCC and delivers it to one or more intercepting LEMFs. An overview of this is shown in figure 5.3-2 below.

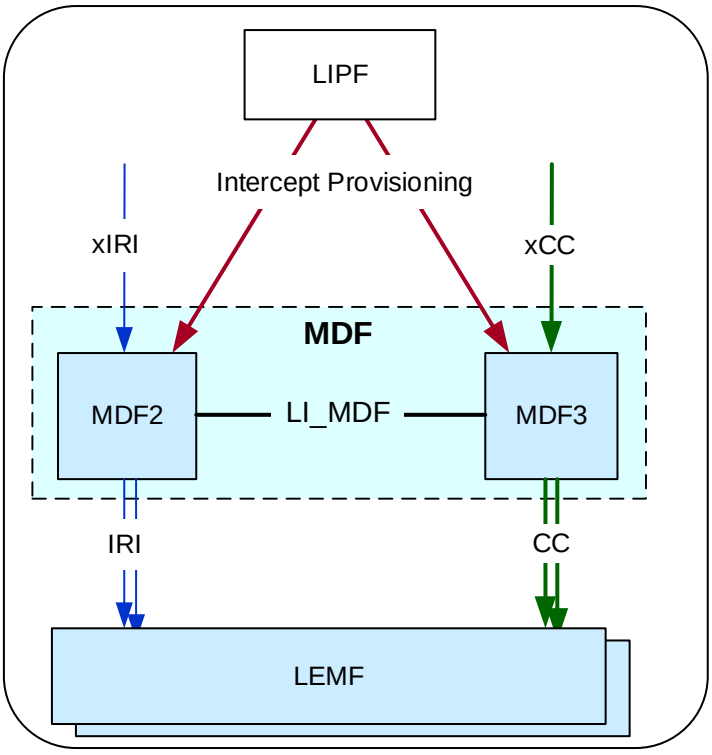

Figure 5.3-2: MDF2 and MDF3

The MDF2 and MDF3 are provisioned by the LIPF with the intercept information necessary to deliver the IRI and/or CC to one or more LEMFs.

The LI_MDF interface between MDF2 and MDF3 (shown in figure 5.3-2) allows the MDF3 and MDF2 to exchange information between the two.

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.

5.3.5.3 LIPF

The LIPF provisions all the applicable POIs, TFs and MDFs.

The role of the LIPF varies depending on implementation of network functions and of the ADMF itself (e.g. virtual or non-virtual).

In its simplest form, the LIPF is the secure proxy used by the LICF to communicate with POIs, TFs, MDFs or other infrastructure required to operate LI within the CSP network. In this scenario the LIPF does not store target information and simply routes LI_X1 messages from and to the LICF.

In scenarios where the ADMF is required to take an active role in POI triggering, the LIPF is responsible for receiving triggering information (e.g. from an IRI-TF) and forwarding the trigger to the appropriate POI.

For directly provisioned POIs, TFs and MDFs, the LIPF will forward all LI administration instructions from the LICF to the intended destination POI, TF or MDF.

In SBA as defined in TS 23.501 [2] or virtualised deployments, the LIPF is responsible for identifying changes to NFs, POIs, and TFs and MDFs through interaction with the SIRF or underlying virtualisation infrastructure. The LIPF shall notify the LICF of changes affecting the number of active NFs/POIs and TFs or other information which the LICF requires to maintain the master POI/TF and MDF list.

While the LIPF is assumed to be stateful with respect to dynamic interceptions it is managing, it shall not hold the full static target or other historic LI data. If the LIPF is deployed in a virtualised environment, the LIPF shall not store LI information in persistent storage and shall rely on the LICF to manage re-synchronisation in the case of LIPF restart.

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.

5.3.5.5 LI Function Selection

The LICF and LIPF shall support selective management and provisioning of groups of POIs, TFs and IEFs, based on the warrant parameters (e.g., service scope, target identities), the target UE type and profile (e.g. a smartphone, a CIoT device) and the CSP's network deployment architecture and services implementation (e.g. Slicing, MEC and URLLC enablers, etc.), with the purpose of optimizing the LI system operation and avoiding its over-provisioning. This selective management and provisioning shall apply independently of architectural alternatives in clause 8.2.

The selective management and provisioning of LI functions may be supported by ADMF's GUI configuration capabilities, as well as by ADMF's ability to obtain and use the CSP network data to drive its provisioning decisions.

The following are examples of the ADMF's configuration capabilities:

- Single or multiple POIs or TFs or IEFs.
- Groups of one or more POIs, TFs, and IEFs of a specific parent NF type.
- POIs, TFs, and IEFs associated with NFs in a specific slice.
- POIs, TFs, and IEFs independently where they are contained in the same parent NF.
- Enabling only specific services or features of POIs (individually and in groups).

Selective provisioning shall be supported on a per warrant basis.

NOTE: The criteria by which the CSP decides which POIs, IEFs and TFs to select is outside the scope of the present document except where the ADMF is able to make selections using information provided by the SIRF (e.g. all POIs and TFs in a slice).

5.3.6 System Information Retrieval Function (SIRF)

The **System Information Retrieval Function (SIRF)** is responsible for providing the LIPF with the system related information for NFs that are known by the SIRF (e.g. service topology). The information provided shall allow the LIPF/LICF to perform the necessary operations to establish and maintain interception of the target service (e.g. provisioning POIs, TFs and MDFs over LI_X1). LIPF/LICF knowledge of POI, TF and MDF existence is provided directly by interactions between the LIPF/LICF and the underlying CSP management systems that instantiate NFs (as defined in clause 5.5). The NRF/SIRF are not involved in this step of NF/POI or MDF instantiation.

While the LIPF is responsible for interactions with the SIRF, the LIPF will forward applicable information to the LICF. Details of LIPF vs LICF responsibilities in managing and maintaining interception are defined in clause 5.3.2.

As described in clause 5.6 of the present document, the OSS/BSS is responsible for managing the number of NFs within the network including the NF within which the SIRF is implemented. Therefore, the SIRF is not responsible for notifying the LIPF that a new NF, POI, TF or MDF has been instantiated (in virtualised networks) or connected to the network using manual processes (legacy networks). The LIPF is notified of these events directly by the relevant CSP management system as described in clause 5.6, prior to any interaction with the SIRF. When the SIRF subsequently notifies the LIPF that, for example an NF associated with a POI has now been registered with the SIRF, the LIPF knows that an NF and POI which it has already configured for LI usage is ready for live user traffic service.

NOTE: The SIRF will only become aware of the existence of NFs after they are commissioned for use within the network and are ready for service usage (NFs are authorised, instantiated and configured for network connectivity before the SIRF will become aware of them). By this stage the NF may be only several milli-seconds away from live user traffic handling. This is too late to check whether the LI components are functional and therefore the SIRF is not involved in NF instantiation reporting to the LIPF.

In virtualised networks where selective per POI provisioning of target identifiers is not required, or only limited network static network slicing is in use, implementation of the SIRF is not required to allow the LIPF and LICF to meet LI requirements.

5.3.7 LEMF – Law Enforcement Monitoring Facility

The **Law Enforcement Monitoring Facility (LEMF)** receives the Interception Product. The **LEMF** is out of scope of the present document.

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.

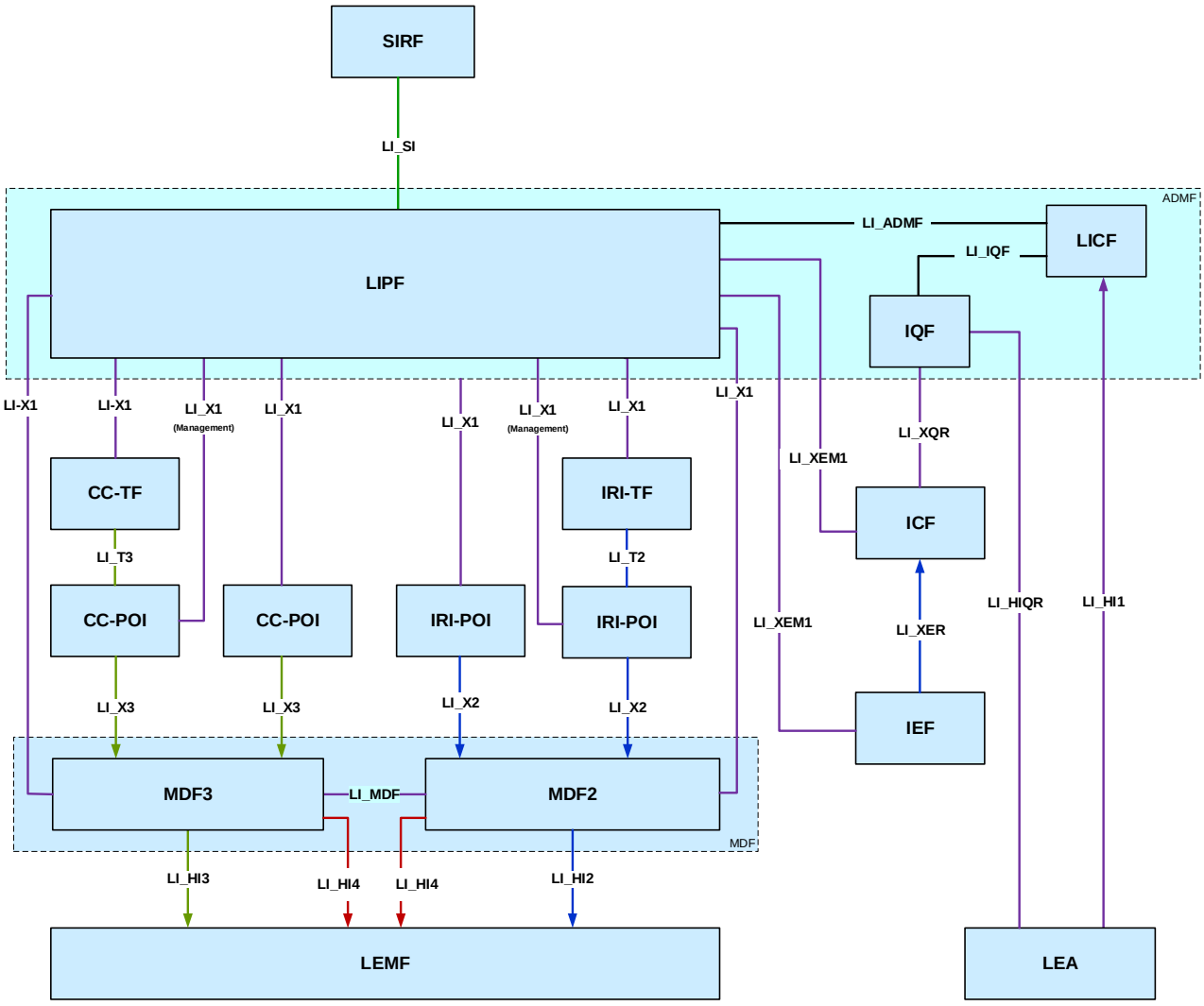

Figure 5.4-1: High-level architecture diagram with key point-to-point LI interfaces

5.4.2 Interface LI_SI

LI_SI is an interface between the SIRF and LIPF. SIRF uses this interface to provide the system information to the LIPF. The LIPF may request the SIRF for such information before sending the intercept provisioning information to the POIs. The SIRF may also notify the LIPF whenever the status of a system function changes (e.g. removed from service, migrating to another location, etc.).

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].

5.4.4 Interface LI_X1

5.4.4.1 General

LI_X1 interfaces are used to manage the POIs and TFs and to provision LI target information on the POIs and TFs in order to intercept target communications. LI_X1 interfaces are also used to manage and provision MDFs with the necessary information to deliver those communications in the correct format to LEMFs.

LI_X1 interfaces shall support the use of ETSI TS 103 221-1 [8] for transport of X1 messages / information. However, the requirements specified in the present document shall apply regardless of generic default options specified in TS 103 221-1 [8].

5.4.4.2 LIPF and POI

The following are examples of some of the information that may be passed over LI_X1 to the POI as a part of intercept provisioning:

- Information necessary to associate multiple xIRI/xCC at MDF2/MDF3.
- Target identifier.
- Type of intercept (IRI only; CC only; or IRI and CC).
- Service scoping.
- Further filtering criteria.
- Address of MDF2 or MDF3.

The exact nature of the information passed depends on the role of the POI.

The LI_X1 interface between the LIPF (in the ADMF) and a Triggered POI shall be used only for audit and management purposes, and not for provisioning purposes.

5.4.4.3 LIPF and TF

The following are examples of some of the information that may be passed over LI_X1 to the TF as a part of intercept provisioning:

- Information necessary to associate multiple xIRI/xCC at MDF2/MDF3.
- Target identifier.
- Type of intercept (IRI only; CC only; or IRI and CC).
- Service scoping.
- Further filtering criteria.
- Address of MDF2 or MDF3.

The exact nature of the information passed depends on the role of the TF.

5.4.4.4 LIPF and MDF2/MDF3

The following are examples of some of the information that may be passed over LI_X1 to the MDF2/MDF3 as a part of intercept provisioning:

Information necessary used to associate multiple xIRI/xCC at MDF2/MDF3.

- Target identifier.
- Lawful Interception identifier.
- Type of intercept (IRI only; CC only; or IRI and CC).
- Service scoping.
- Further filtering criteria.
- LEMF address.

The exact nature of the information passed depends on the role of the MDF. -

5.4.5 Interface LI_X2

The LI_X2 interfaces are used to pass xIRI from IRI-POIs to the MDF2.

The following are some of the information passed over this interface to the MDF2 as a part of xIRI:

- Target identifier.
- Time stamp.
- Correlation information.
- IRI event resulting in xIRI.

5.4.6 Interface LI_X3

LI_X3 interfaces are used to pass real-time content of communications (i.e. xCC) and associated metadata from CC-POIs to MDF3.

The following are some of the information passed over this interface to the MDF3 as a part of xCC:

- Target identifier.

- Time stamp.
- Correlation information.
- User plane packets.

5.4.7 Interface LI_T

5.4.7.1 General

The LI_T interface is used to pass the triggering information from the Triggering Function to the POI. Depending on the POI type, two types of LI_T are defined:

- LI_T2.
- LI_T3.

LI_T2 is used when POI output is sent over LI_X2 and LI_T3 is used when POI output is sent over LI_X3.

5.4.7.2 Interface LI_T2

The LI_T2 interface is from IRI-TF to IRI-POI.

The following are some of the information passed over this interface to the IRI-POI:

- Target identifier.
- IRI interception rules.
- MDF2 address.
- Correlation information.

The IRI interception rules allow the IRI-POI to detect the target communication information to be intercepted.

5.4.7.3 Interface LI_T3

LI_T3 interface is from CC-TF to CC-POI.

The following are some of the information passed over this interface to CC-POI:

- Target identifier.
- CC interception rules.
- MDF3 address.
- Correlation information.

The CC interception rules allow the CC-POI to detect the target communication information to be intercepted.

5.4.8 Interface LI_HI2

LI_HI2 is used to send IRI from the MDF2 to the LEMF. This interface is defined in TS 33.128 [15].

5.4.9 Interface LI_HI3

LI_HI3 is used to send CC from the MDF3 to the LEMF. This interface is defined in TS 33.128 [15].

5.4.10 Interface LI_HI4

5.4.10.1 General

LI_HI4 is used by the MDF2 and MDF3 to report to the LEMF that the MDF2/3 have been provisioned as expected. This capability is mandatory to support but optional to use (subject to relevant national agreement) at both MDF2 and MDF3.

NOTE: It is FFS if/how LI_HI4 interface could be used to report network topology information.

5.4.10.2 LI operation notification

The MDF2 and MDF3 shall support reporting to the LEMF changes to provisioning, including:

- Activation of LI.
- Modification of active LI.
- Deactivation of LI.

NOTE: A mechanism may be needed at the CSP to prevent duplicate notifications being raised in the case of LI being provisioned across multiple MDFs. Such a mechanism is for FFS.

5.4.10.3 Contents of the notification

Each notification shall include at least the following:

- The type of notification (e.g. activation, deactivation).
- Relevant related information (LIID, time of change).

5.4.11 Interface LI_ADMF

LI_ADMF is an interface between LICF and LIPF and is used by the LICF to send the intercept provisioning information to the LIPF. Further details about this interface is outside the scope of the present document.

5.4.12 Interface LI_MDF

LI_MDF is an interface between MDF2 and MDF3 and is used for MDF2 and MDF3 to interact with each other in the generation of IRI and CC. Further details about this interface is outside the scope of the present document.

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 Interface 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 Interface 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 Interface LI_XEM1

The LI_XEM1 interface is used by the LICF (proxied by the LIPF) to manage and control the activation state of the IEF(s) and ICF.

LI_XEM1 interfaces shall support the use of ETSI TS 103 221-1 [8] for transport of XEM1 messages / information. However, the requirements specified in the present document shall apply regardless of generic default options specified in [8].

5.5 LI service discovery

In SBA as defined in TS 23.501 [2] the NRF is a central repository of discoverable NFs. For NFs to be discoverable, they need to have been previously instantiated and undergone a degree of configuration (function identity allocated, IP addresses, certificates, network connectivity to NRF, etc.).

LI functions (e.g. ADMF, POIs and MDFs) exist within a separate security domain to the main network NF to which they are embedded. Furthermore, as with legacy networks, LI functions associated with NFs shall be configured and tested before the associated NF is allowed to enter active network user service (i.e. LI shall be configured and tested before an NF can handle live user traffic).

In the present document, all LI functions have dedicated LI_X interfaces and discovery of LI functions by the LIPF shall happen as part of the NF / LI function instantiation phase. POIs, TFs and MDFs shall not be subject to or within the scope of NRF service discovery as defined in TS 23.501 [2]. The SIRF is used to provide the LIPF with NF discovery information which shall be used to identify which NFs are applicable to intercept specific user sessions, as described in clause 5.3.6. However, the SIRF is not involved directly in LI service discovery.

The SIRF may be used to inform the LIPF that an NF has been registered / deregistered with the NRF and is now ready for use in a network user service. The LIPF is assumed to already have knowledge of which POIs and TFs are associated with which NFs.

POIs, TFs and MDFs may be discovered in virtualised deployments using the approach described in clause 5.6. The exact mechanisms for achieving this are out of scope of the present document.

5.6 LI in a virtualised environment

5.6.1 General

Virtualisation is one of the 3GPP network deployment options for NFs containing LI functions as described in the present document. In virtualised deployments, many of the initial deployment and configuration actions performed manually in non-virtualised deployments need to be automated and occur in near real-time. This clause outlines the basic architecture enhancements to support virtualised LI in 3GPP networks. Security aspects relating to virtualisation are described in clause 8.

The architecture enhancements in this clause are intended to apply to any virtualised 2G, 3G, 4G, 5G scenario including IMS that needs to support LI. Where legacy network functions defined in TS 33.107 [11] are virtualised, the architecture in figure 5.6-1 shall be applied, with legacy TS 33.107 [11] reference points and functional elements substituted for their equivalent in the present document (e.g. POI is equivalent to ICE and LI_X2 is equivalent to X2 in TS 33.107 [11]).

5.6.2 Virtualised deployment architecture

Figure 5.6-1 shows the necessary extensions to the basic LI architecture described in clause 5.2 required to support real-time deployment of virtualised LI functions. Figure 5.6-1 is a simplified version of the virtual LI function deployment procedures.

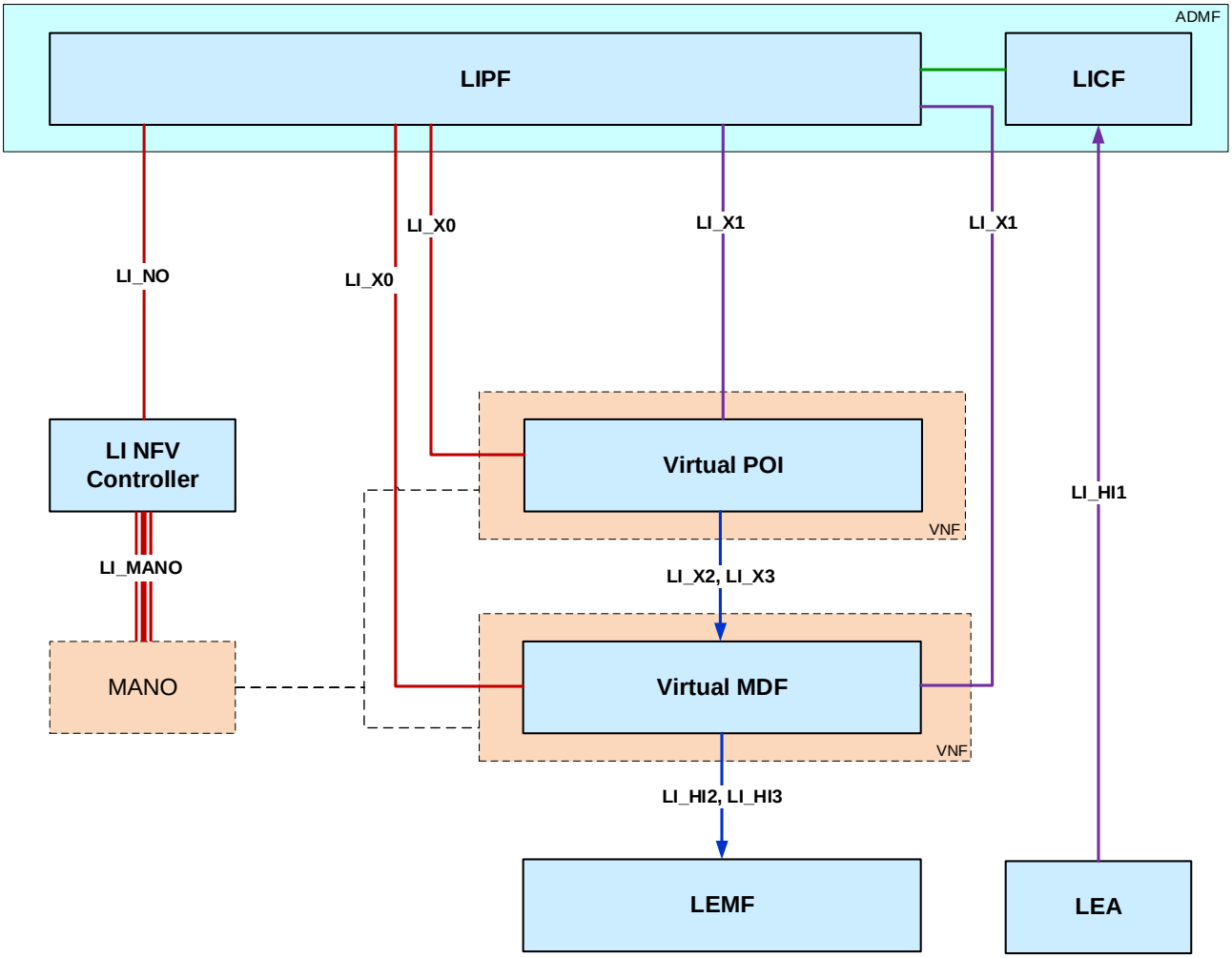

Figure 5.6-1: Simplified virtualised LI system with provisioning infrastructure for a direct provisioned POI

Figure 5.6-1 shows the LI NFV controller and NFV Management and Orchestration functions (MANO), together with two logical interfaces:

- LI_NO: This interface allows to exchange correlation and notification information between the LI application/service and NFV layer about related VNF and VNFC lifecycle management; it also allows to configure optional virtual deployment parameters. In addition, in case of LI functions not instantiated by OSS/BSS (see clause 5.6.3.1.6 of the present document) this interface shall support LI function instantiation requests from the ADMF.

- LI_MANO: This interface allows to notify the LI NFV controller about VNF/VNFC lifecycle management and enforce virtual deployment LI security policy.

These two interfaces are assumed to be already setup between the involved functional entities via a mutual authenticated and encrypted dedicated connection.

The procedures in clause 5.6.3 assume that the LIPF, LICF and NFV LI Controller already exist before creation of any other LI functions.

The OSS/BSS is responsible for controlling the number of 3GPP VNFs and service chains within the network. The OSS/BSS instructs NFV MANO to instantiate, scale or terminate one or more VNFs. NFV MANO is also able to instantiate and terminate VNF sub-components (VNFCs) dynamically without input from the OSS/BSS in order to maintain performance and resilience requirements. This is especially likely in container-based implementations.

To ensure that all LI related aspects, if applicable, are considered within that VNF, NFV MANO notifies the LI NFV Controller about the VNF and VNFC instantiation, scaling and termination. In case where a VNF, about to be instantiated, is expected to have LI specific functionalities such as POI, TF or MDF, the LI NFV controller notifies the LIPF about those LI specific functionalities within the VNF. The LIPF would forward that notification to the LICF,

which in turn, validate/verify/authorize (via LIPF, of course) that POI/TF/MDF for LI over LI_X0. If the VNF does not contain an LI function then the LI NFV Controller may still notify the LIPF/LICF.

LI NFV Controller shall be configurable to apply default LI policy and configuration to LI VNFCs without explicit authorisation from the LIPF/LICF, depending on network performance and LI security requirements. The LI NFV Controller shall be able to apply policy on a per instantiation basis or apply a static configuration policy to NFV MANO, which NFV MANO is able to use to automatically instantiate LI components using this default configuration.

In most deployments some default LI configuration information will need to be provided as part of the VNF image packages and package descriptor files. Such LI information needs to be adequately protected within NFV MANO and software catalogues.

Where explicit authorisation of LI components is required, the LIPF would notifies the LI NFV Controller that the LI specific functions are authorized/verified and the LI NFV Controller notifies NFV MANO.

NOTE: In figure 5.6.1, LI_MANO is shown as a combined representation of the up to three separate NFV MANO interfaces provided by ETSI GS NFV IFA 026 [20]. Since the exact number of interfaces required depends on the vendor implementation of the NFVI / NFV MANO and whether a combined single NFVO interface is supported by NFV MANO, the present document treats this a single logical interface labelled as LI_MANO for 3GPP LI purposes.

5.6.3 LI function instantiation and lifecycle management procedures

5.6.3.1 Controller virtualisation layer and MANO procedures

5.6.3.1.1 Responsibilities

The 5G NRF is not involved in the discovery of LI functions, as described in clause 5.3.6. NFs containing LI functions shall only be discoverable by the NRF / SIRF once all LI initialisation steps in this clause have been completed and the OSS/BSS/ MANO informed that LI operation is ready. The process by which the NRF / SIRF is notified by the OSS/BSS/MANO is out of scope of the present document.

5.6.3.1.2 General procedures

When the 3GPP network OSS/BSS makes a request to NFV MANO to instantiate, modify or terminate a 3GPP NF, NFV MANO shall notify the LI NFV Controller of the request over LI_MANO using procedures as described in ETSI GS NFV-IFA 026 [20] or equivalent. The NFV LI Controller shall be able to send all applicable NF changes to the LIPF over LI_NO, so that the LICF is able to maintain an understanding of network topology. In 5G, the LICF in the ADMF (via the LIPF) also maintains understanding of active use of NF via the NRF / SIRF.

In addition, NFV MANO is required to send notifications of non-OSS/BSS triggered (e.g. NFV MANO automated VNF relocation, or software image update) as described in ETSI GS NFV IFA 026 [20]. The LI NFV Controller shall also be able to provide applicable notifications to the LICF in the ADMF (via the LIPF) of such changes.

NOTE: The precise list of information required for the ADMF to maintain understanding of network topology is implementation specific and therefore outside the scope of the present document.

In deployments where the implementation supports data centre / location verification for NFs being instantiated or modified, subject to operator policy the LI NFV Controller shall not allow instantiation or modification of LI functions or associated NFs which do not comply with LI location constraints set by the LICF in the ADMF (via the LIPF).

5.6.3.1.3 Instantiation

Where an NF being instantiated contains one or more LI functions (e.g. POI, TF, MDF) the LI NFV Controller shall handle any necessary steps to allow the LI functions to be instantiated by NFV MANO and the LI functions to be added to the LI environment, so that initial contact between the LI functions and the LIPF in the ADMF can be established. The LI NFV Controller shall provide details of the new LI functions to the LICF in the ADMF (via the LIPF), including the identity of the new LI functions, so that the LICF is aware of the existence of the LI functions.

In deployments where ADMF (LICF) signing of LI function software images has been implemented, the LI NFV Controller shall provide the signatures to the LICF in the ADMF (via the LIPF) for verification and shall only authorise NFV MANO to continue instantiation of the LI function if the LICF has successfully verified the signatures.

NOTE: Once this instantiation step is completed an LI function is considered ready for configuration by the ADMF (LIPF) but is not ready to become a live LI function.

5.6.3.1.4 Modification

When an NF containing LI functions is being modified (e.g. scaled or relocated) the LI NFV Controller shall manage the necessary interactions with NFV MANO (using the procedures in ETSI GS NFV-IFA 026 [20] or equivalent) to allow the LI functions to also be modified in alignment with changes to their parent NF. The LI NFV Controller shall notify the LICF in the ADMF via the LIPF over LI_NO, of the subsequent modifications. Where the modifications result in a new LI function being instantiated (e.g. where a scale up exceeds the existing capabilities of the existing LI functions and a new VNFC is instantiated), the LI NFV Controller shall notify the LICF about the existence of the new LI function and indicate to which existing NF the new LI function is associated.

5.6.3.1.5 Termination

When an NF containing LI functions is terminated, the LI NFV Controller shall manage the necessary interactions with NFV MANO (using the procedures in ETSI GS NFV IFA 026 [20] or equivalent) and notify the LICF via the LIPF that the LI functions have been removed from the system. The LICF in the ADMF shall ensure that certificates associated with those LI functions are appropriately revoked.

5.6.3.1.6 Direct instantiation of LI Functions by ADMF

Procedures in clauses 5.6.3.1.3, 5.6.3.1.4 and 5.6.3.1.5 are based on the OSS/BSS being responsible for creating all LI functions as part of normal network operations (e.g. LI functions are embedded VNFC within a VNFs or are instantiated as part of network service descriptors where a whole slice or large set of VNFs are instantiated together as part of a complete network service).

In some scenarios, the ADMF needs to create specific virtualised LI functions (e.g. MDF) within the NFVI used to host other operator NFs but for security reasons requires that the OSS/BSS does not manage or have knowledge of these. In this scenario, the LICF, instructs the LI NFV Controller via LIPF over LI_NO to request NFV MANO via LI_MANO to instantiate an LI specific image. This LI VNF may either be inserted as part of an existing network service chain or create a new LI specific service chain.

In such scenarios, the ADMF shall play the role of the OSS/BSS and the LI_NO interface shall support the related operations; the LIPF should implement the equivalent logic of OSS/BSS for these operations.

NOTE: It is assumed that any required LI VNF or VNFC images are available within NFV MANO image software catalogue and the images are not sent over the LI_NO or LI_MANO interfaces.

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.

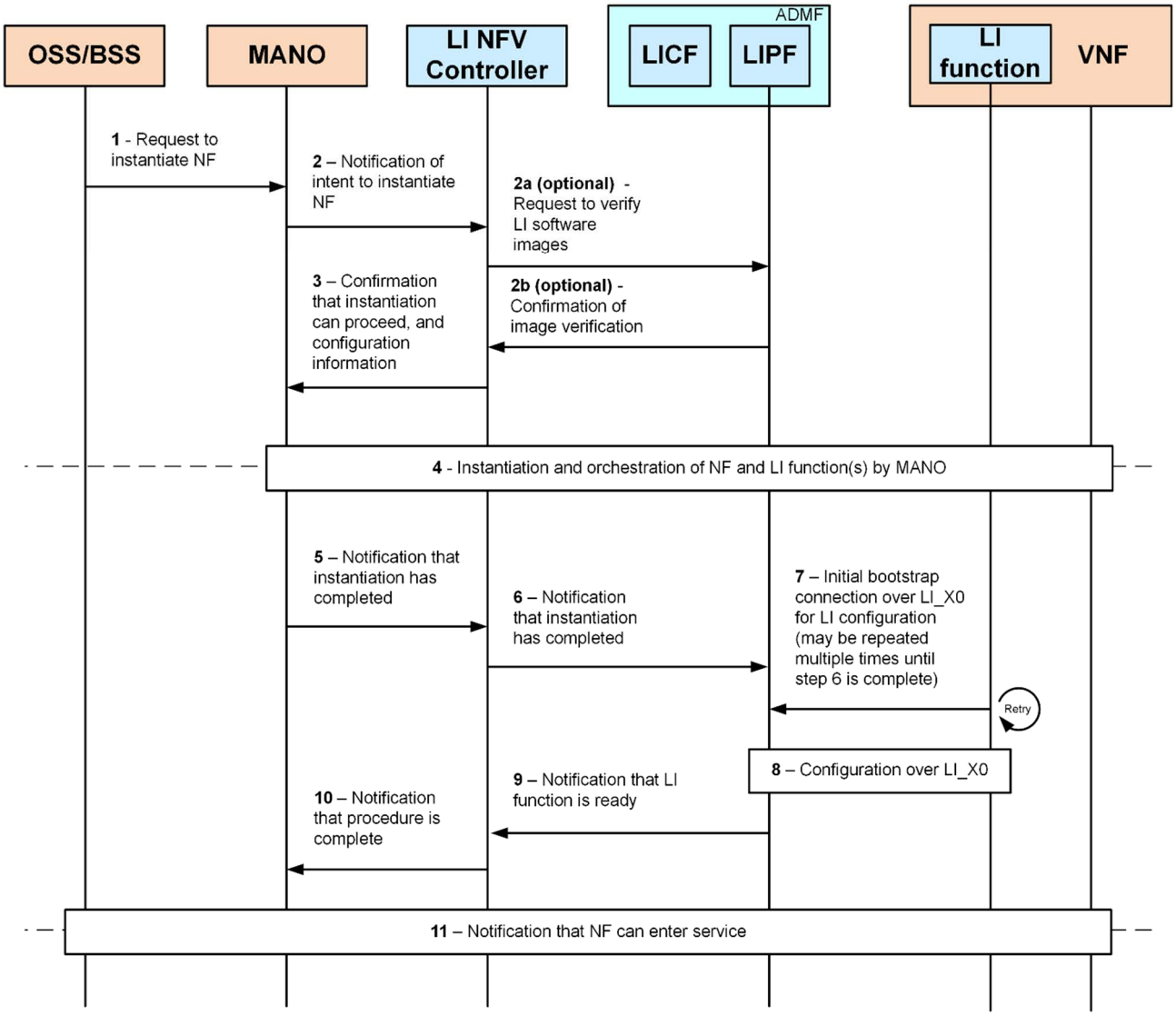

Figure 5.6-2: Example simplified flow-diagram for OSS / BSS originated LI instantiation procedures

5.6.3.3 Exception Procedures

If during normal LI system operation the ADMF (LIPF or LICF) detects or is informed of abnormal LI function behaviour, then subject to operator policy the LICF in the ADMF via the LIPF shall be able via the LI NFV Controller over LI_NO and LI_MANO to request immediate termination or quarantine of the LI function to NFV MANO as defined in ETSI GS NFV-IFA 026 [20]. For this purpose, the LI NFV Controller acts as a Semi-Active SM as described in ETSI GS NFV-IFA 026 [20].

If during normal operation the LICF in the ADMF via the LIPF is notified of a NF modification or instantiation event which does not comply with operator LI policy (e.g. NF location is not within allowed locations or LI functionality is not authorised for a given deployment scenario) the LICF via the LIPF shall be able to deny NFV MANO and the OSS/BSS authorisation to complete the system change. The ADMF shall be able to delegate responsibility for real-time termination handling to the NFV LI Controller. The NFV LI Controller shall be responsible for reporting detected events and subsequent actions taken by LI NFV Controller and NFV MANO to the LICF via the LIPF over LI_NO.

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.

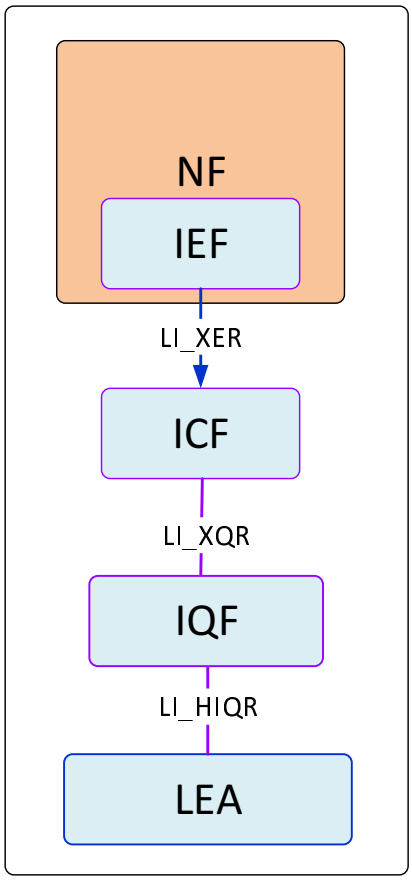

Figure 5.7-1 High-level identifier retrieval via Query and Response.

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 identifiers 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.

The ICF shall store identifier associations received from the IEF and hold them indefinitely as active associations until:

- A new association event is received which updates a previous association.
- A disassociation event is received for a stored association.
- A CSP defined maximum age is reached.

Upon receiving a disassociation event or a new association event from the IEF, the ICF shall match any corresponding identifier associations, mark them for deletion and begin the cache time for that association. After being marked for deletion, associations shall be deleted and purged irrecoverably from the ICF once their cache time limit is reached.

NOTE: 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.

6 Network layer based interception

6.1 General

Clause 6 gives details for the configuration of the high-level LI architecture for network layer based interception. It defines aspects of the LI configuration specific to each network under consideration (e.g. 5G), while aspects concerning services delivered over this network are considered in clause 7.

6.2 5G

6.2.1 General

Figure 6.2-1 depicts the 5G EPC-anchored LI architecture. The network functions are depicted in grey, while the LI elements are depicted in blue.

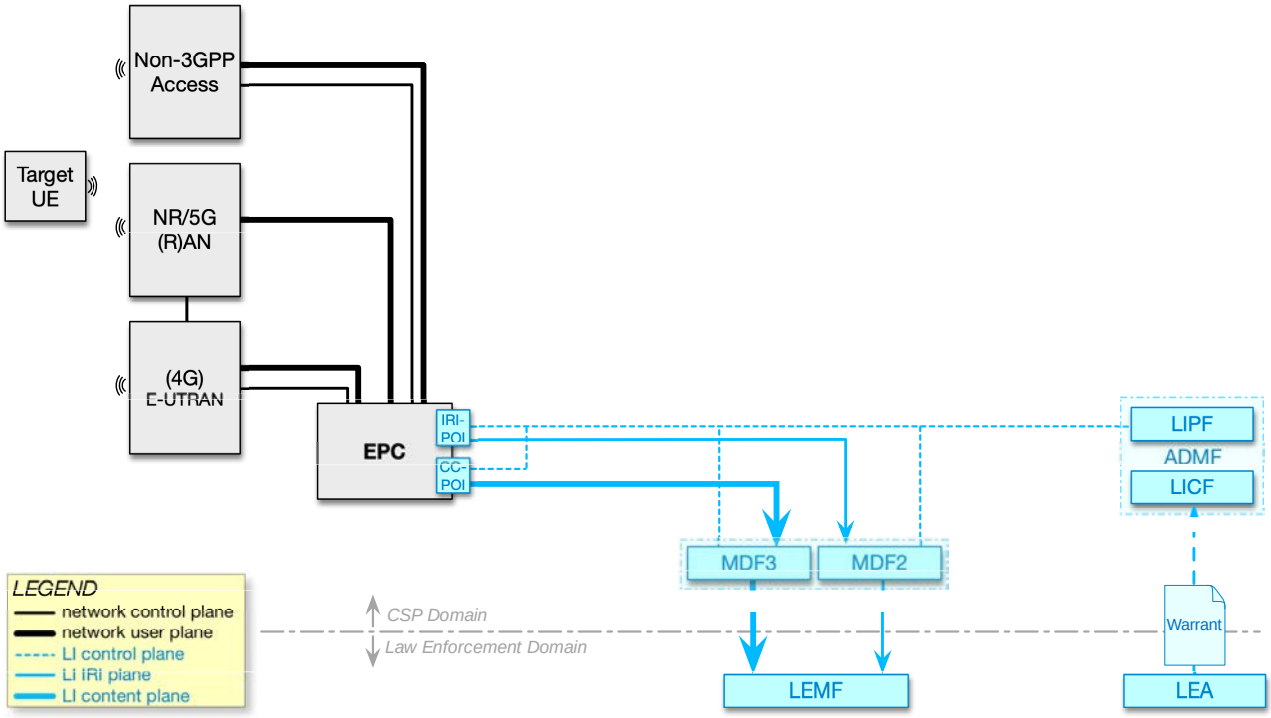

Figure 6.2-1: 5G EPC-anchored LI architecture

Figure 6.2-2 depicts the 5G core-anchored LI architecture. The network functions are depicted in grey, while the LI elements are depicted in blue.

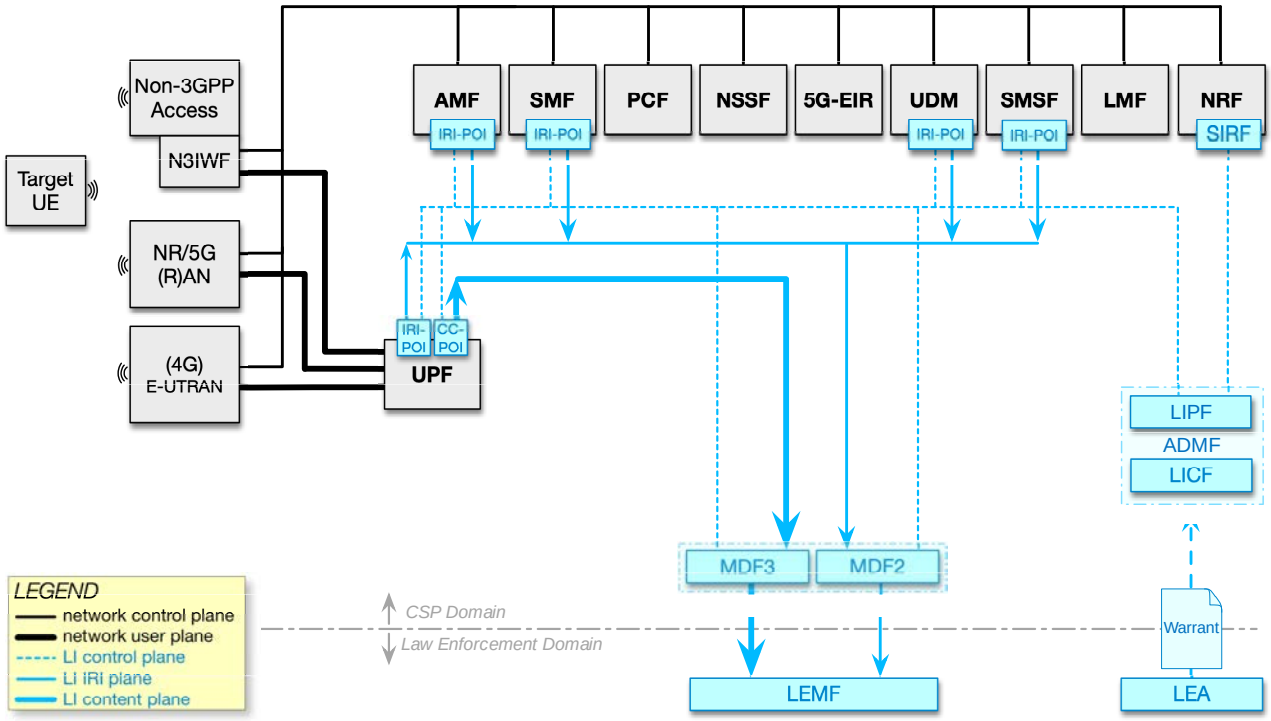

Figure 6.2-2: 5G core-anchored LI architecture

6.2.2 LI at AMF

6.2.2.1 Architecture

In the 5GC network, the AMF handles the access and mobility functions as well as provides or facilitates UE location information delivery to other NFs in the course of location-related service operations, such as LCS or Location Reporting. The AMF shall have LI capabilities to generate the target UE's network access, registration, connection management, and location update related xIRI. Extending the generic LI architecture presented in clause 5, figure 6.2-3 below gives a reference point representation of the LI architecture with AMF as a CP NF providing the IRI-POI functions.

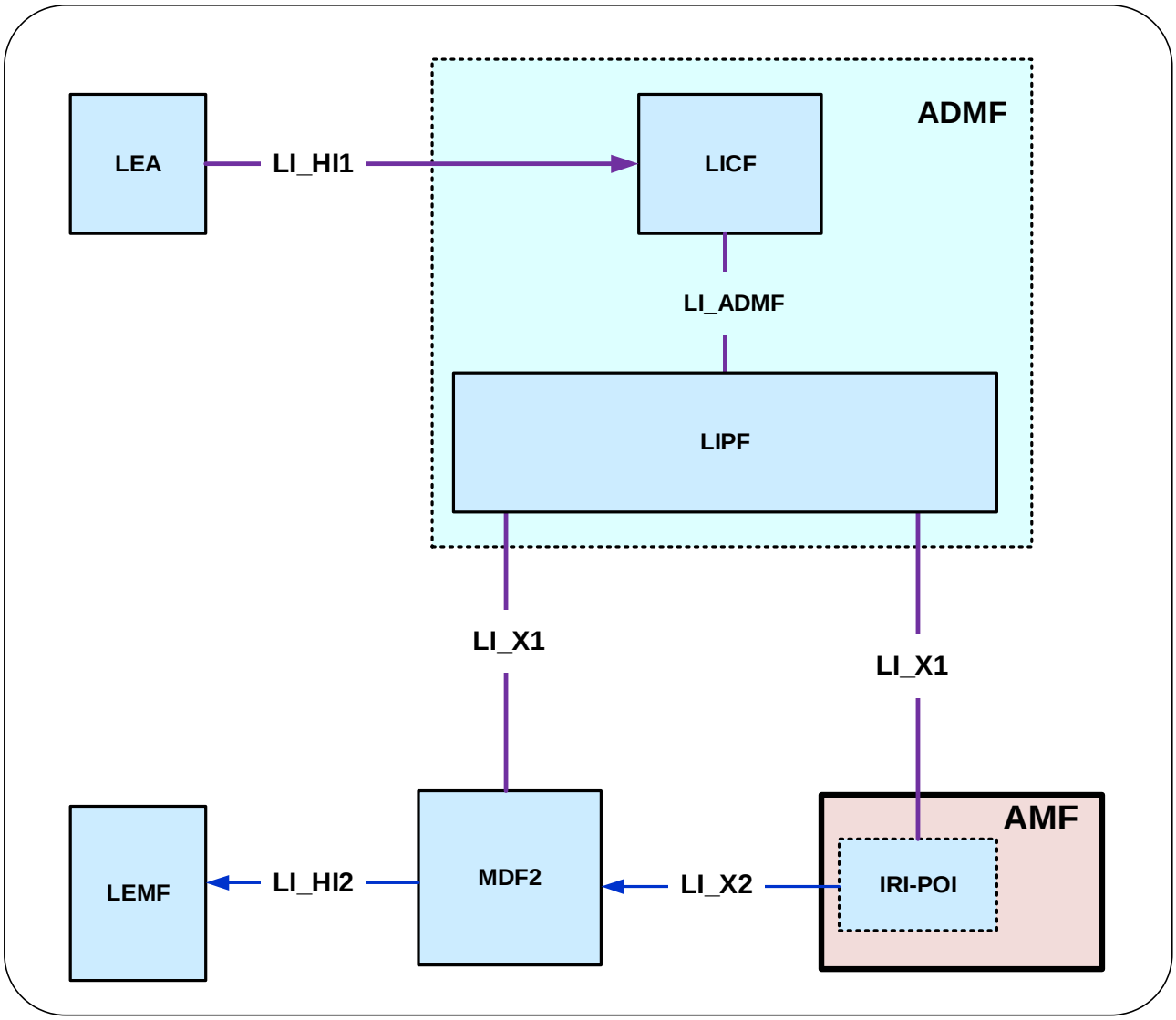

Figure 6.2-3: LI architecture for LI at AMF

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

The LIPF present in the ADMF provisions the IRI-POI (over LI_X1) present in the AMF and the MDF2. The LIPF may interact with the SIRF (over LI_SI) present in the NRF to discover the AMFs in the network.

The IRI-POI present in the AMF detects the target UE's access and mobility related functions (network access, registration and connection management), generates and delivers the xIRI to the MDF2 over LI_X2. The MDF2 delivers the IRI messages as part of the Interception Product to the LEMF over LI_HI2.

6.2.2.2 Target identities

The LIPF present in the ADMF provisions the intercept information associated with the following target identities to the IRI-POI present in the AMF:

- SUPI.
- PEI.
- GPSI.

The interception performed on the above three identities are mutually independent, even though, an xIRI may contain the information about the other identities when available.

6.2.2.3 Identity privacy

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

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

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

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 identifier association xIRI independently of activation of LI for all other events. When identifier association xIRI only reporting is activated, the IRI-POI in the AMF shall also generate location update xIRI.

6.2.2.5 Common IRI parameters

The list of xIRI parameters are specified in TS 33.128 [15]. All xIRI shall include the following:

- Target identity.
- Time stamp.
- Location information.
- Correlation information.

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.

6.2.2.7 Network topologies

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

- Non-roaming case.
- Roaming case, in VPLMN.
- Roaming case, in HPLMN for non-3GPP access.

In a roaming case, it is possible that the target UE may use non-3GPP access with the N3IWF present in the HPLMN.

6.2.2A Identifier Reporting for AMF

6.2.2A.1 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.

6.2.2A.2 IEF Events

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

- Association of a 5G-GUTI to a SUPI, (this may also include SUCI to SUPI association).
- De-association of a 5G-GUTI from a SUPI.

NOTE1: The de-association event is only generated if a new 5G-GUTI is not allocated to a SUPI to update a previous association (e.g. at inter-AMF handover).

NOTE 2: For SUCIs seen during registration, they shall only be reported if UE registration is successfully completed.

The association event shall be generated by the IEF in the AMF whenever the AMF initiates any action or procedure for which a new allocated 5G-GUTI is sent to the UE regardless of whether the action or procedure is completed sucessfully.

6.2.2A.3 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.

6.2.2A.4 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.

6.2.3 LI for SMF/UPF

6.2.3.1 Architecture

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

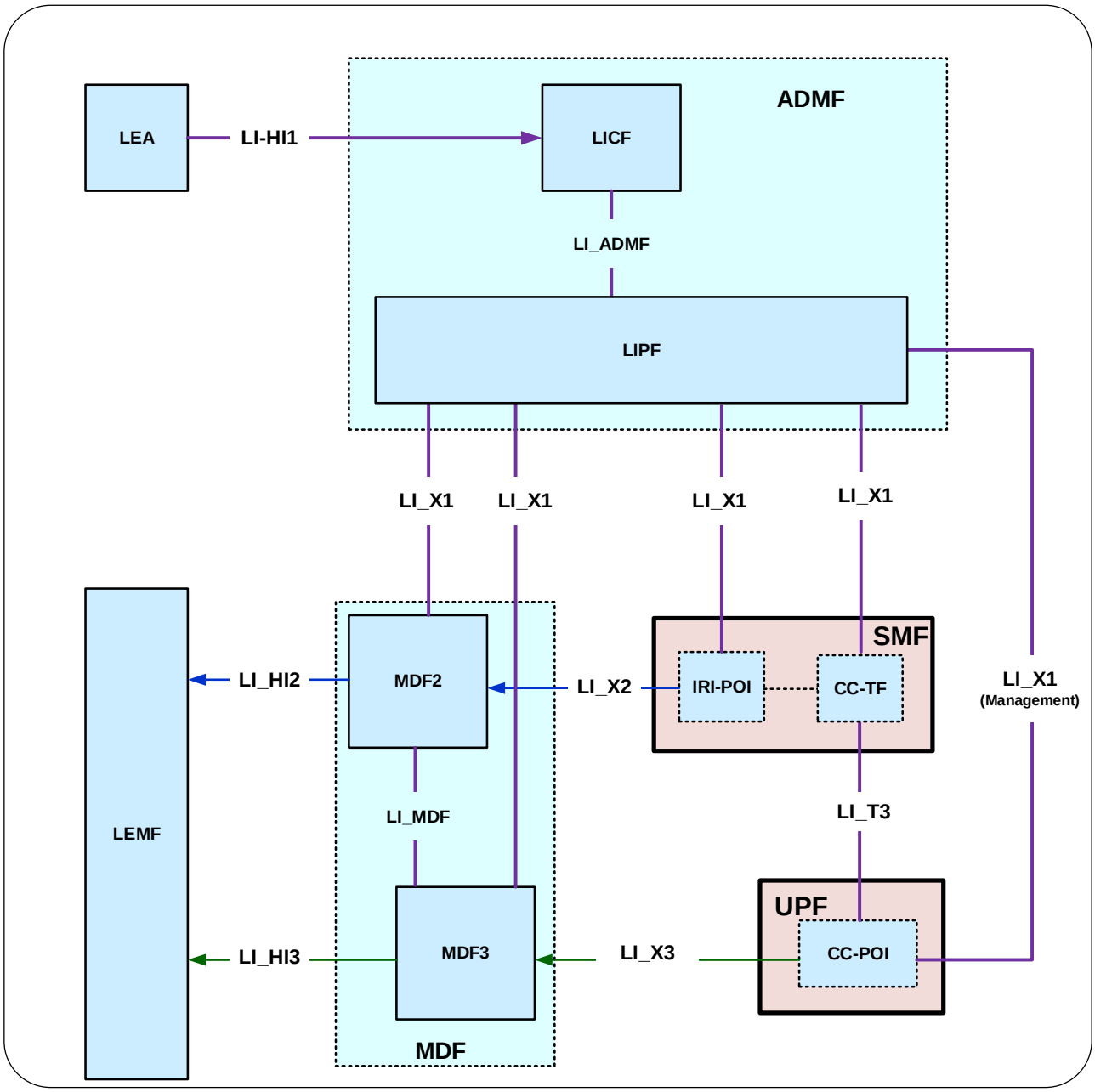

Figure 6.2-4: LI architecture showing LI at SMF/UPF

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

The LIPF present in the ADMF provisions IRI-POI (present in the SMF), MDF2 and MDF3 over the LI_X1 interfaces. To enable the interception of the target's user plane packets (e.g. when the warrant requires the interception of communication contents), the CC-TF present in the SMF is also provisioned with the intercept data.

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

The LIPF may interact with the SIRF (over LI_SI) present in the NRF to discover the SMFs and UPFs in the network. The IRI-POI present in the SMF detects the PDU session establishment, modification, and deletion related events, generates and delivers the related xIRI to the MDF2 over LI_X2. The MDF2 delivers the IRI messages to the LEMF over LI_HI2.

When interception of communication contents is required, the CC-TF present in the SMF sends a trigger to the CC-POI present in the UPF over the LI_T3 interface.

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

- User plane packet detection rules.
- Target identity.
- Correlation information.
- MDF3 address.

NOTE 2: When LI_T3 is used, the LI_X1 between LIPF and CC-POI present in the UPF is used to monitor the user plane data.

The CC-POI present in the UPF generates the xCC from the user plane packets and delivers the xCC (that includes the correlation number and the target identity) to the MDF3. The MDF3 delivers the CC to the LEMF over LI_HI3.

A warrant that does not require the interception of communication contents, may require IRI messages that have to be derived from the user plane packets. To support the generation of related xIRI (i.e. that requires access to the user plane packets), the present document supports two implementation approaches:

- In approach 1, the IRI-POI responsible for the generation of such xIRI resides in the UPF. Such an IRI-POI requires a trigger to enable it to detect the user plane packets. The corresponding Triggering Function (IRI-TF) resides in the same SMF that has the IRI-POI for the generation of other xIRI.
- The trigger sent by the IRI-TF (present in the SMF) to the IRI-POI (present in the UPF) includes the following:
  - User plane packet detection rules.
  - Target identity.
  - Correlation information.
  - MDF2 address.
- The IRI-POI present in the UPF generates the xIRI (that includes the correlation number and the target identity) from the user plane packets and sends it to the MDF2. The MDF2 generates the IRI messages and send them to the LEMF.
- In approach 2, xCC is generated by the CC-POI present in the UPF as if the warrant involves the interception of communication contents. To enable this, the CC-TF presumed to be present in the SMF even when the warrant does not require the interception of communication contents. As explained before, the CC-POI generates the xCC and sends it to the MDF3. The MDF3 (based on the provisioned intercept information) does not generate and deliver the CC to the LEMF. Instead, the MDF3 forwards the xCC to the MDF2 over LI_MDF interface. The MDF2 then generates the IRI messages from xCC and delivers those IRI messages to the LEMF.

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

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

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

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

6.2.3.2 Target identities

The LIPF provisions the intercept related information associated with the following target identities to the IRI-POI present in the SMF:

- SUPI.
- PEI.
- GPSI.

The interception performed on the above three identities are mutually independent, even though, an xIRI may contain the information about the other identities when available.

6.2.3.3 IRI events

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

- PDU session establishment.
- PDU session modification.
- PDU session release.
- Start of interception with an established PDU session.

The PDU session establishment xIRI is generated when the IRI-POI present in the SMF detects that a PDU session has been established for the target UE.

The PDU session modification xIRI is generated when the IRI-POI present in the SMF detects that a PDU session is modified for the target UE.

The PDU session release xIRI is generated when the IRI-POI present in the SMF detects that a PDU session is released for the target UE.

The start of interception with an established PDU session xIRI is generated when the IRI-POI present in a SMF detects that interception is activated on the target UE that has an already established PDU session in the 5GS. When a target UE has multiple PDU sessions, this xIRI shall be sent for each PDU session with a different value of correlation information.

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

When the warrant requires the packet data header information reporting, the following xIRI shall be generated:

- Packet data header information report.

The generation of packet data information report can be done by either the IRI-POI present in the UPF or the MDF2.

6.2.3.4 Common IRI parameters

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

- Target identity.
- Time stamp.
- Correlation information.
- Location information.
- Session related information.

6.2.3.5 Specific IRI parameters

The parameters in each xIRI are defined in TS 33.128 [15].

6.2.3.6 Network topologies

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

- Non-roaming case.
- Roaming case, in VPLMN.
- Roaming case, in HPLMN.
- Non-3GPP access case, in the PLMN where N3IWF resides.

When the target UE has multiple PDU sessions active, the generation and delivery of xCC for each PDU session shall be done independently, each with separate correlation information.

When a target UE's PDU session involves multiple Data Network (DN) connections (i.e. multiple connections to the same DN as described in clause A.3 of the present document), the generation and delivery of xCC shall be done in such a way that:

- All applicable user plane packets are captured and delivered.
- Duplicate delivery of CC is suppressed to the extent possible.
- Each user plane packet is delivered with the associated DN Access Identifier (DNAI).

A PDU session may involve more than one UPFs. In that case, the CC-TF present in the SMF shall determine which UPF(s) is (are) more suitable to provide the CC-POI functions adhering to the above requirements. Furthermore, independent of which UPF is used to generate the xCC, the CC delivered from the MDF3 shall be correlated to the IRI messages related to the PDU session.

6.2.3.7 Multi-Access PDU (MA PDU) Session Specific

The IRI-POI present in the SMF shall generate xIRI, for MA PDU sessions when it detects events or information as in clause 6.2.3.3, with the following clarifications.

The PDU session establishment xIRI:

- When a UE request for an MA PDU session is received at the SMF (for one or more access types).
- When a UE request for a single access PDU session is received at the SMF with an upgrade indicator to an MA PDU and the SMF chooses to establish an MA PDU session.

The PDU session modification xIRI:

- When an MA PDU Session is modified by releasing or adding an access type.
- When a UE request for a mid-session upgrade to MA PDU session is received at the SMF.

The PDU session release xIRI:

- When the entire PDU session is released.

Each user plane packet of the MA PDU session should be able to be associated to the access type.

6.2.4 LI at UDM for 5G

In 5G packet core network, the UDM provides the unified data management for UE. The UDM shall have LI capabilities to generate the target UE's service area registration related xIRI. See clause 7.2.2 for the details.

6.2.5 LI at SMSF

6.2.5.1 Architecture

In the 5GC network, the SMSF provides functionalities to support the SMS over NAS. The SMSF shall have LI capabilities to generate xIRIs when SMS related to the target's UE are handled. Extending the generic LI architecture presented in clause 5, figure 6.2-5 below gives a reference point representation of the LI architecture with SMSF as a CP NF providing the IRI-POI functions.

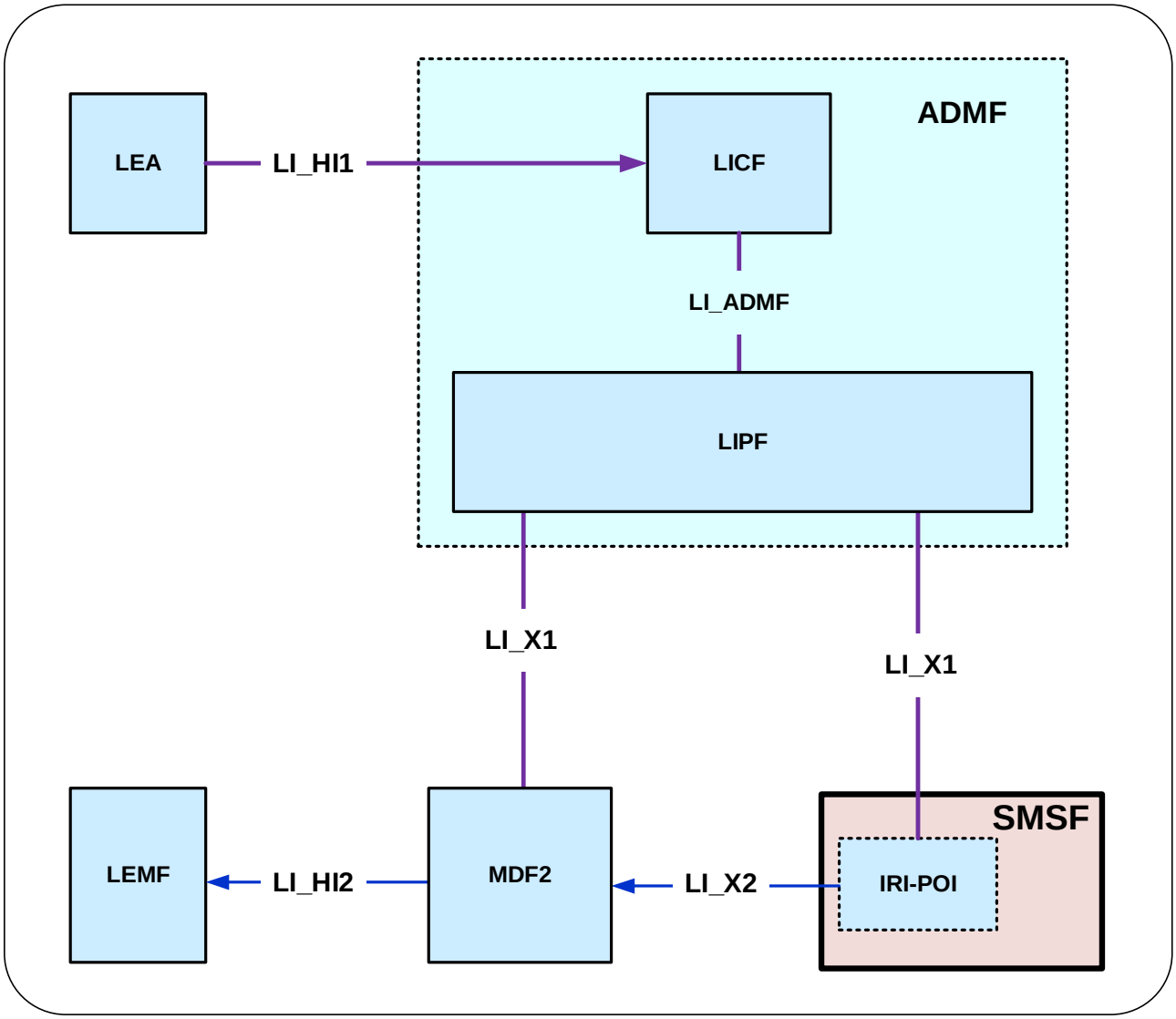

Figure 6.2-5: LI architecture for LI at SMSF

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

The LIPF present in the ADMF provisions the IRI-POI present in the SMSF and the MDF2 over LI_X1 interfaces. The LIPF may interact with the SIRF (over LI_SI) present in the NRF to discover the SMSFs in the network.

The IRI-POI present in the SMSF detects the target UE's SMS, generates and delivers the xIRI to the MDF2 over LI_X2. The xIRI will contain the SMS payload. The MDF2 shall support the capability to deliver the IRI messages including the SMS payload as part of the Interception Product to the LEMF over LI_HI2.

National regulations may require that the MDF2 remove information regarded as content from the payload in case of an IRI only warrant.

6.2.5.2 Target identities

The LIPF present in the ADMF provisions the intercept information associated with the following target identities to the IRI-POI present in the SMSF:

- SUPI.
- PEI.
- GPSI.

The interception performed on the above three identities are mutually independent, even though, an xIRI may contain the information about the other identities when available.

6.2.5.3 IRI events

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

- SMS message.

The SMS message xIRI is generated when the IRI-POI present in an SMSF detects that an SMS message for the target UE is handled.

6.2.5.4 Common IRI parameters

The list of xIRI parameters are specified in TS 33.128 [15]. The xIRIs shall include at the minimum the following information:

- Target identity.
- Time stamp.
- Location information.
- SMS message direction (mobile originated, mobile terminated).
- SMS message payload.

6.2.5.5 Specific IRI parameters

The parameters in each xIRI are defined in TS 33.128 [15].

6.2.5.6 Network topologies

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

- Non-roaming case.
- Roaming case, in VPLMN.

NOTE: SMS message delivery over non-3GPP access with N3IWF in the HPLMN is considered a non-roaming case.

6.2.6 LI support at NRF

6.2.6.1 Architecture

In 5G, network functions that support SBA register with the NRF after instantiation. The NRF thus provides the network repository functions and is aware of all the NFs that have been instantiated. The present document refers to this as system information.

The SIRF present in the NRF provides the system information to LIPF present in the ADMF, in order for the LIPF to establish which NFs (and therefore POIs) are applicable to a specific target user's services. LI function service discovery is described in clause 5.5.

An architecture diagram depicting this LI at NRF is shown in figure 6.2-6 below.

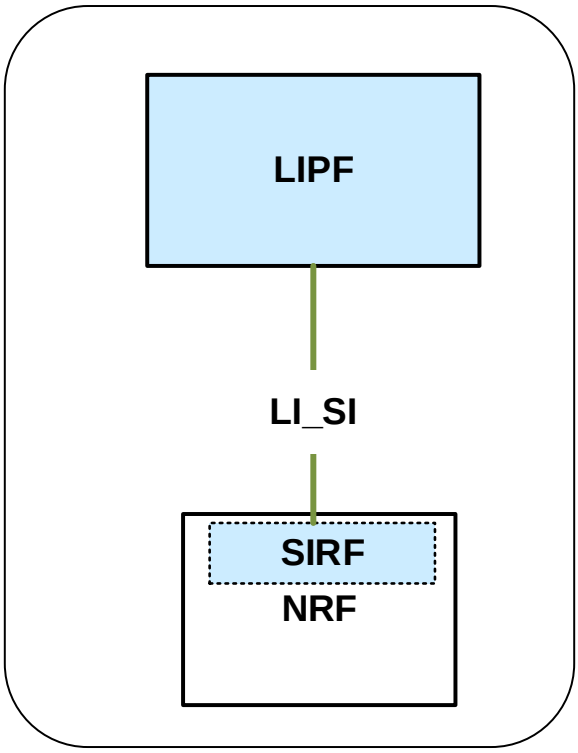

Figure 6.2-6: LI Architecture depicting NRF as an SIRF

Figure 6.2-6 shows the architecture illustrating the SIRF functions within the NRF.

The LIPF present in the ADMF interacts with the SIRF (over LI_SI) present in the NRF to obtain the system information.

6.2.6.2 LI_SI notifications

The SIRF present in the NRF shall generate notifications over LI_SI when the SIRF detects the following specific events or information:

- NF service registration.
- NF service update.
- NF service deregistration.
- NF service chain change.

The NF service chain change notification shall be generated whenever an NF is added to or removed from a service chain in response to NF discovery and selection events.

6.2.6.3 LI_SI parameters

The notifications reported over LI_SI by the SIRF shall include the following information elements:

- Event type (as defined in clause 6.2.6.2).
- NF details, including appropriate information elements defined in TS 23.501 [2] clause 6.2.6.

6.2.7 External data storage

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

- The UDSF/UDR shall be subject to the same location, geographic, security and other physical environment constraints as the NF POI for which it is storing data.
- No LI specific POI data (e.g. target list) shall be stored in the UDSF/UDR unless storage is directly under the control of the POI within the NF.
- LI data stored in a UDSF/UDR shall only be accessible by the specific individual POI for which the UDSF/UDR is storing data and that data shall not be shared between POIs unless specifically authorised by the LICF within the ADMF.
- By default, LI data shall not be stored in a UDSF/UDR which is shared by multiple NFs unless specifically authorised by the LICF.
- Any storage of LI data outside of the POI in the UDSF/UDR shall be auditable by the LICF.
- The interface between the POI/NF and the UDSF/UDR shall be protected such that an attacker cannot identify targeted users based on observation of this interface. (i.e. access to the UDSF/UDR shall be identical for both intercepted and non-intercepted user communications).
- The use and placement of a UDSF/UDR within an NF/POI design shall not introduce additional interception delay compared with non-separated compute and storage.
- Where the POI requires access to NF data that is stored in the UDSF/UDR, non-LI network functions and processes or non-LI authorised personnel shall not be able to detect POI access to that data in the UDSF/UDR.
- The POI and LICF/MDF shall be responsible for managing encryption of LI data stored for the POI in addition to any default encryption applied by the NF.

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

6.3 EPC

6.3.1 General

The present document specifies two options for EPC interception capabilities:

1. Use TS 33.107 [11] and TS 33.108 [21] natively as defined in those documents;
2. Use the capabilities specified below in the present document for stage 2 and in TS 33.128 [15] for stage 3.

Detailed LI architecture and functional requirements for Control and User Plane Separation (CUPS) are outside the scope of the present document. They are specified in TS 33.107 [11].

6.3.2 LI at the MME

6.3.2.1 Architecture

In the EPC network, the MME handles the mobility management and connection management as specified in TS 23.401 [22]. The MME shall have LI capabilities to generate the target UE's network access, registration and connection management related xIRI. Extending the generic LI architecture presented in clause 5, figure 6.3-1 below gives a reference point representation of the LI architecture with MME as a CP Network Element providing the IRI-POI functions.

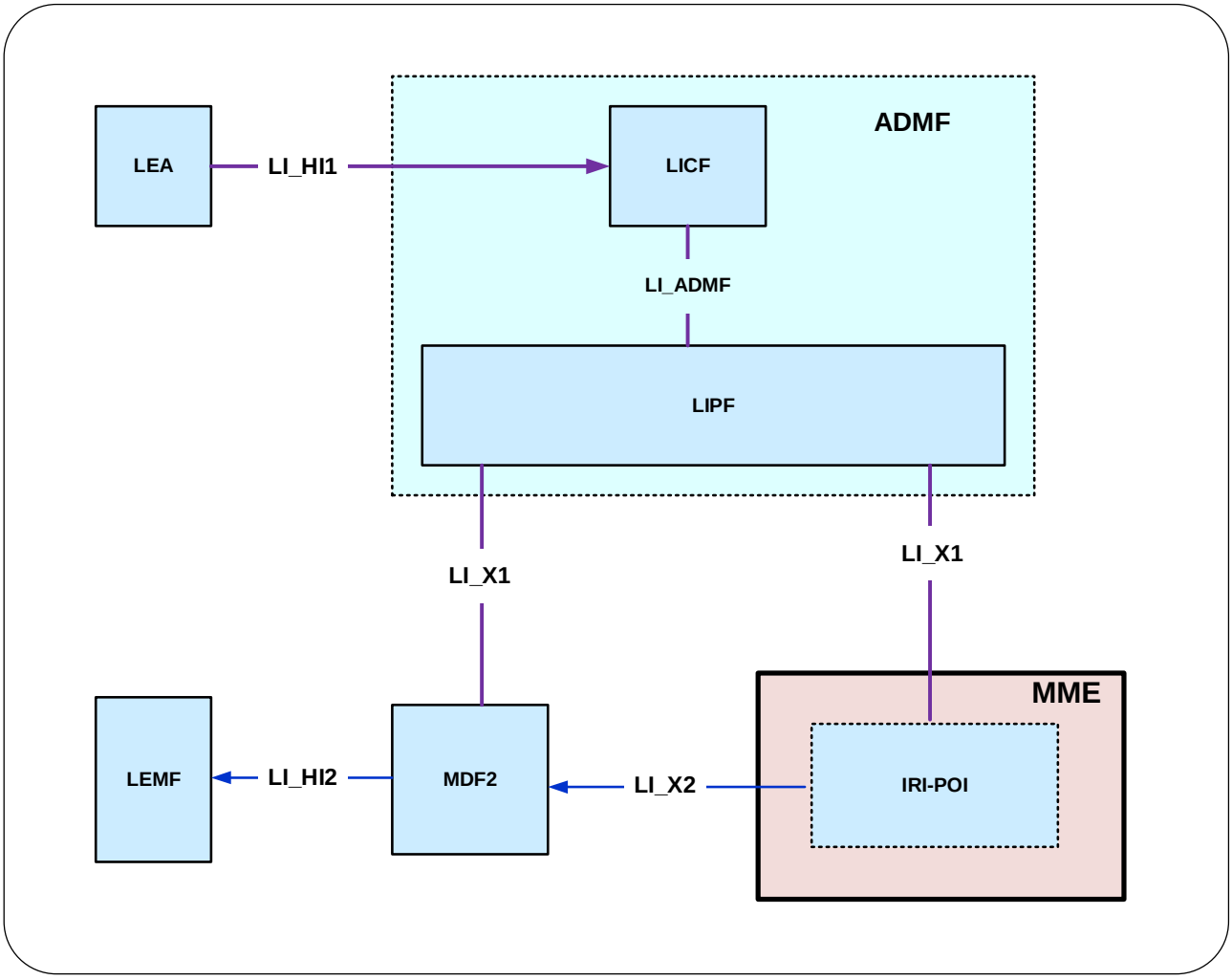

Figure 6.3-1: LI architecture for LI at MME

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

The LIPF present in the ADMF provisions the IRI-POI (over LI_X1) present in the MME and the MDF2.

The IRI-POI present in the MME detects the target UE's access and mobility related functions (network access, registration and connection management), generates and delivers the xIRI to the MDF2 over LI_X2. The MDF2 delivers the IRI messages as part of the Interception Product to the LEMF over LI_HI2.

6.3.2.2 Target identities

The target identities which the LIPF present in the ADMF provisions to the IRI-POI present in the MME are specified in TS 33.107 [11].

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. When identifier association xIRI only reporting is activated, the IRI-POI in the MME shall also generate Tracking Area/EPS Location Update xIRI (as defined in TS 33.107 [11] clause 12.2.1.2).

6.3.2.4 Common IRI parameters

The list of xIRI parameters are specified in TS 33.128 [15]. All xIRI shall include the following:

- Target identity.
- Time stamp.
- Location information.

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.

6.3.2.6 Network topologies

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

- Non-roaming case.
- Roaming case, in VPLMN.

6.3.3 LI at SGW/PGW

6.3.3.1 Architecture

In the EPC network, the SGW is the gateway which terminates the user plane interface as specified in TS 23.401 [22]. The PGW is the gateway which terminates the SGi interface towards the PDN as specified in TS 23.401 [22]. Additionally, the PGW is the user plane anchor for mobility between 3GPP access and non-3GPP access as specified in TS 23.402 [23].

NOTE 1: The present document supports LI for non-3GPP accesses connected to EPC using GTP-based S2a or GTP-based S2b as specified by TS 23.402 [23]. Other scenarios are covered by TS 33.107 [11].

The SGW and PGW shall include an IRI-POI that has the LI capabilities to generate the target UE's bearer related xIRI.

In addition, the SGW and PGW shall include a CC-POI that has the LI capabilities to duplicate the user plane packets from the EPS bearers related to a target UE.

Figure 6.3-2 shows the LI architecture for SGW/PGW based interception.

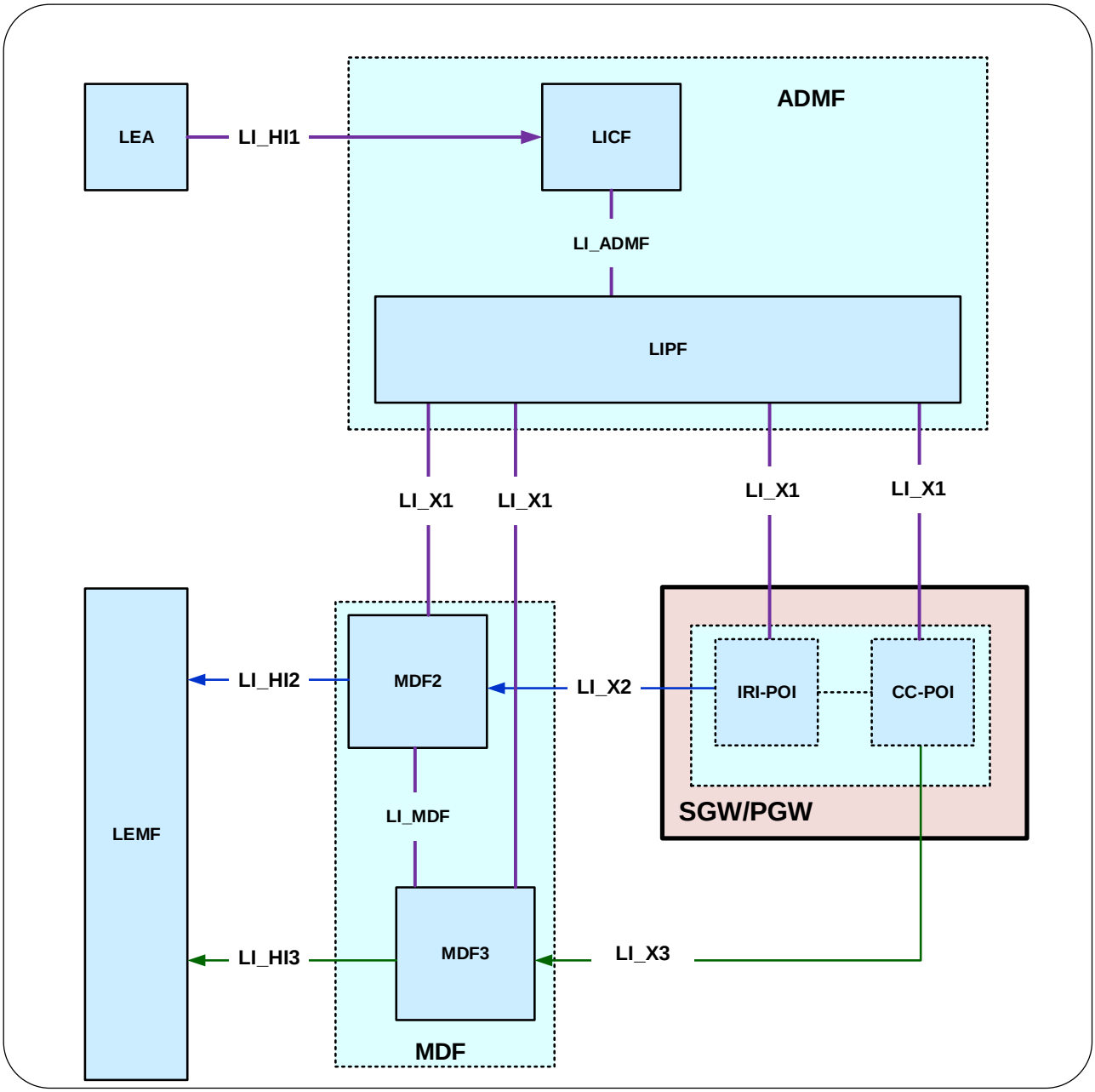

Figure 6.3-2: LI architecture for LI at SGW/PGW

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

The LIPF present in the ADMF provisions IRI-POI present in the SGW/PGW, MDF2 and MDF3 over the LI_X1 interfaces. To enable the interception of the target's user plane packets (e.g. when the warrant requires the interception of communication contents), the CC-POI present in the SMF is also provisioned with the intercept data.

NOTE 2: The IRI-POI and CC-POI represented in figure 6.3-2 are logical functions and require correlation information be shared between them; they may be handled by the same process within the SGW/PGW.

The IRI-POI present in the SGW/PGW detects the target UE's bearer activation, modification and deactivation, generates and delivers the xIRI to the MDF2 over LI_X2. The MDF2 delivers the IRI messages to the LEMF over LI_HI2.

The CC-POI present in the SGW/PGW generates the xCC from the user plane packets and delivers the xCC (that includes the correlation number and the target identity) to the MDF3. The MDF3 delivers the CC to the LEMF over LI_HI3.

A warrant that does not require the interception of communication contents, may require IRI messages that have to be derived from the user plane packets. To support the generation of related xIRI (i.e. that requires access to the user plane packets), the present document supports two implementation approaches:

- In approach 1, the IRI-POI responsible for the generation of such xIRI resides in the SGW/PGW. Such an IRI-POI requires a trigger to enable it to detect the user plane packets. The corresponding Triggering Function (IRI-TF) resides in the same SGW/PGW that has the IRI-POI for the generation of other xIRI.
- The trigger sent by the IRI-TF to the IRI-POI includes the following:
  - User plane packet detection rules.
  - Target identity.
  - Correlation information.
  - MDF2 address.
- The IRI-POI generates the xIRI (that includes the correlation number and the target identity) from the user plane packets and sends it to the MDF2. The MDF2 generates the IRI messages and send them to the LEMF.
- In approach 2, xCC is generated by the CC-POI as if the warrant involves the interception of communication contents. To enable this, the CC-POI is presumed to be present in the SGW/PGW even when the warrant does not require the interception of communication contents. As explained before, the CC-POI generates the xCC and sends it to the MDF3. The MDF3 (based on the provisioned intercept information) does not generate and deliver the CC to the LEMF. Instead, the MDF3 forwards the xCC to the MDF2 over LI_MDF interface. The MDF2 then generates the IRI messages from xCC and delivers those IRI messages to the LEMF.

NOTE 3: The IRI-POI and IRI-TF present in the SGW/PGW may be handled by the same process in the node.

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

6.3.3.2 Target identities

The target identities which the LIPF present in the ADMF provisions to the IRI-POI, CC-POI and IRI-TF present in the SGW/PGW are specified in TS 33.107 [11].

6.3.3.3 IRI events

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

6.3.3.4 Common IRI parameters

The list of xIRI parameters are specified in TS 33.128 [15]. All xIRI shall include the following:

- Target identity.
- Time stamp.
- Location information.

6.3.3.5 Specific IRI parameters

The parameters in each xIRI are defined in TS 33.128 [15].

6.3.3.6 Network topologies

The SGW shall provide the IRI-POI, CC-POI and IRI-TF functions in the following network topology cases:

- Optionally in non-roaming case for E-UTRAN.
- Roaming case, in VPLMN.

The PGW shall provide the IRI-POI, CC-POI and IRI-TF functions in the following network topology cases:

- Optionally in non-roaming case for E-UTRAN.
- Roaming case, in HPLMN.
- Non-3GPP access case, in the HPLMN.

For the case of access to EPC via E-UTRAN, in case of non-roaming, at least one between SGW and PGW shall provide IRI-POI, CC-POI and IRI-TF.

When the target UE has multiple bearers active, the generation and delivery of xCC for each bearer shall be done independently, each with separate correlation information.

6.3.4 LI at ePDG

6.3.4.1 Architecture

In the EPC network, the ePDG is the gateway which allows interworking between non-3GPP access and 3GPP network. The ePDG functionalities are specified in TS 23.402 [23].

NOTE 1: The present document supports LI for non-3GPP accesses connected to EPC using GTP-based S2a or GTP-based S2b as specified in TS 23.402 [23]. Other scenarios are covered by TS 33.107 [11].

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

In addition, the ePDG shall include a CC-POI that has the LI capabilities to duplicate the user plane packets from the EPS bearers related to a target UE.

Figure 6.3-3 shows the LI architecture for ePDG based interception.

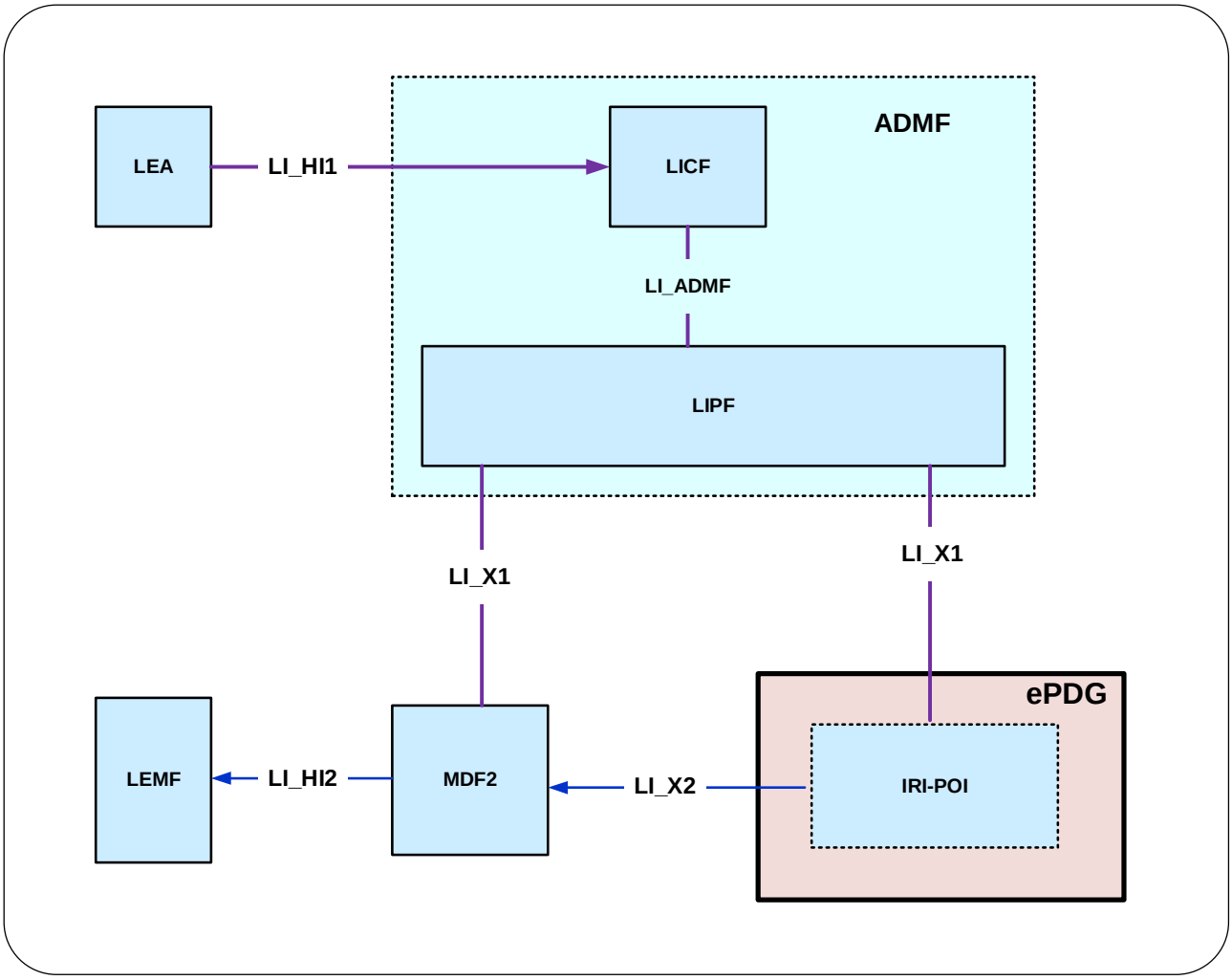

Figure 6.3-3: LI architecture for LI at ePDG

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

The LIPF present in the ADMF provisions IRI-POI present in the ePDG, MDF2 and MDF3 over the LI_X1 interfaces. To enable the interception of the target's user plane packets (e.g. when the warrant requires the interception of communication contents), the CC-POI present in the ePDG is also considered to be provisioned with the intercept data.

NOTE 2: The IRI-POI and CC-POI represented in figure 6.3-4 are logical functions, require a close coupling between the two and as such may be handled by the same process within the ePDG.

The IRI-POI present in the ePDG detects the target UE's bearer activation, modification and deactivation, generates and delivers the xIRI to the MDF2 over LI_X2. The MDF2 delivers the IRI messages to the LEMF over LI_HI2.

The CC-POI present in the ePDG generates the xCC from the user plane packets and delivers the xCC (that includes the correlation number and the target identity) to the MDF3. The MDF3 delivers the CC to the LEMF over LI_HI3.

6.3.4.2 Target identities

The target identities which the LIPF present in the ADMF provisions to the IRI-POI and CC-POI present in the ePDG are specified in TS 33.107 [11].

6.3.4.3 IRI events

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

6.3.4.4 Common IRI parameters

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

- Target identity.
- Time stamp.
- Correlation information.
- Location information.
- Bearer related information.

6.3.4.5 Specific IRI parameters

The parameters in each xIRI are defined in TS 33.128 [15].

6.3.4.6 Network topologies

The ePDG shall provide the IRI-POI and CC-POI functions in the following network topology cases:

- Roaming case, in VPLMN.

6.4 3G

For virtualised 4G implemenations from Release 15 onwards (including combined 4G / 5G scenarios), 4G shall be virtualised based on the architecture in clause 5.6. For such implementations the LI architecture for 4G / LTE shall be implemented using an ADMF as defined in the present document (including LIPF and LICF split). However, equivalent reference points as specified in TS 33.107 [11] shall be used where appropriate (e.g. X2 is equivalent to LI_X2 in the present document and MDF is equivalent to MF/DF). Security and audit requirements as defined in clause 8 of the present document shall be applied to such 4G scenarios.

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

6.5 VoNR

Voice over NR as defined in TS 23.501 [2] and TS 23.502 [4] is intended to provide equivalent functionality to VoLTE in 4G.

LI requirements for VoNR based on IMS are defined in clause 7.4 of the present document.

6.6 4G/5G Interworking

Figure 6.6-1 depicts interworking between EPC and the 5G architecture. The network functions are depicted in grey, while the LI elements are depicted in blue.

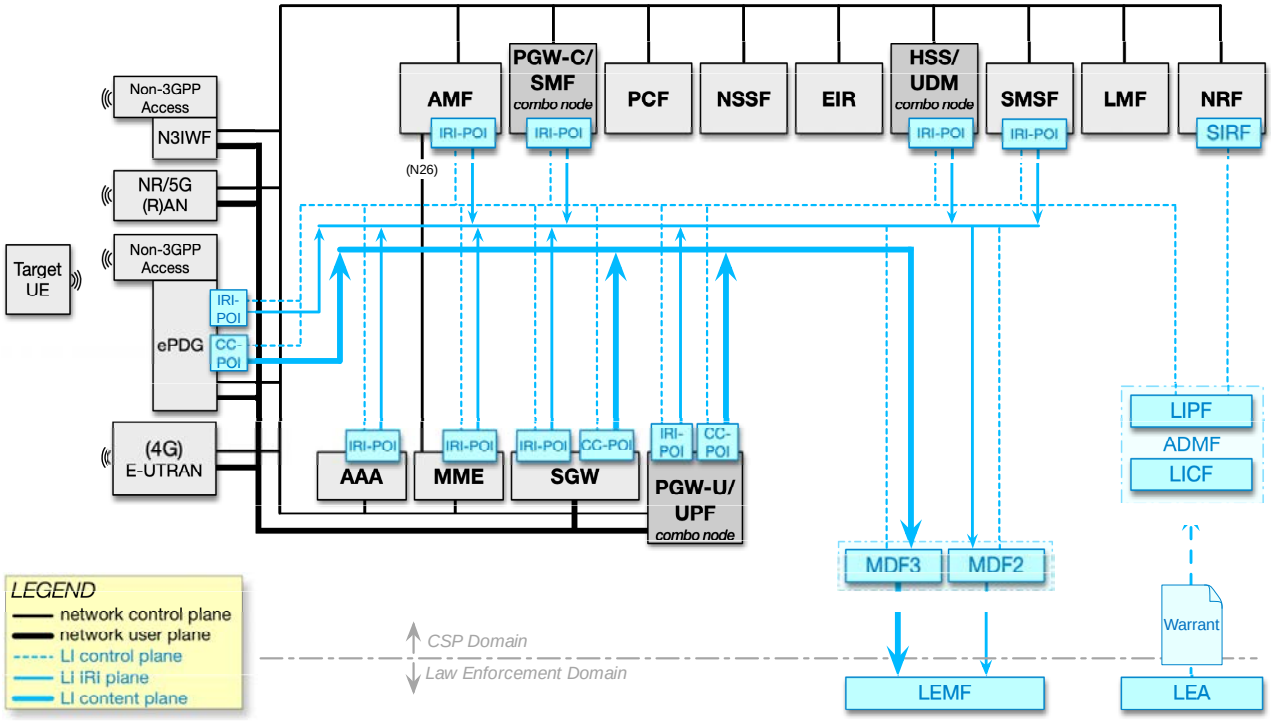

Figure 6.6-1: EPC/5G Interworking LI architecture

7 Service layer based interception

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.

7.2 Central subscriber management

7.2.1 General

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

7.2.2 LI at UDM

7.2.2.1 Architecture

The UDM provides the unified data management for UE. The UDM shall have LI capabilities to generate the target UE's serving system (e.g. VPLMN Id or AMF Id related xIRI). Extending the generic LI architecture presented in clause 5, figure 7.2-1 below gives a reference point representation the LI architecture with UDM as a CP NF providing the IRI-POI functions.

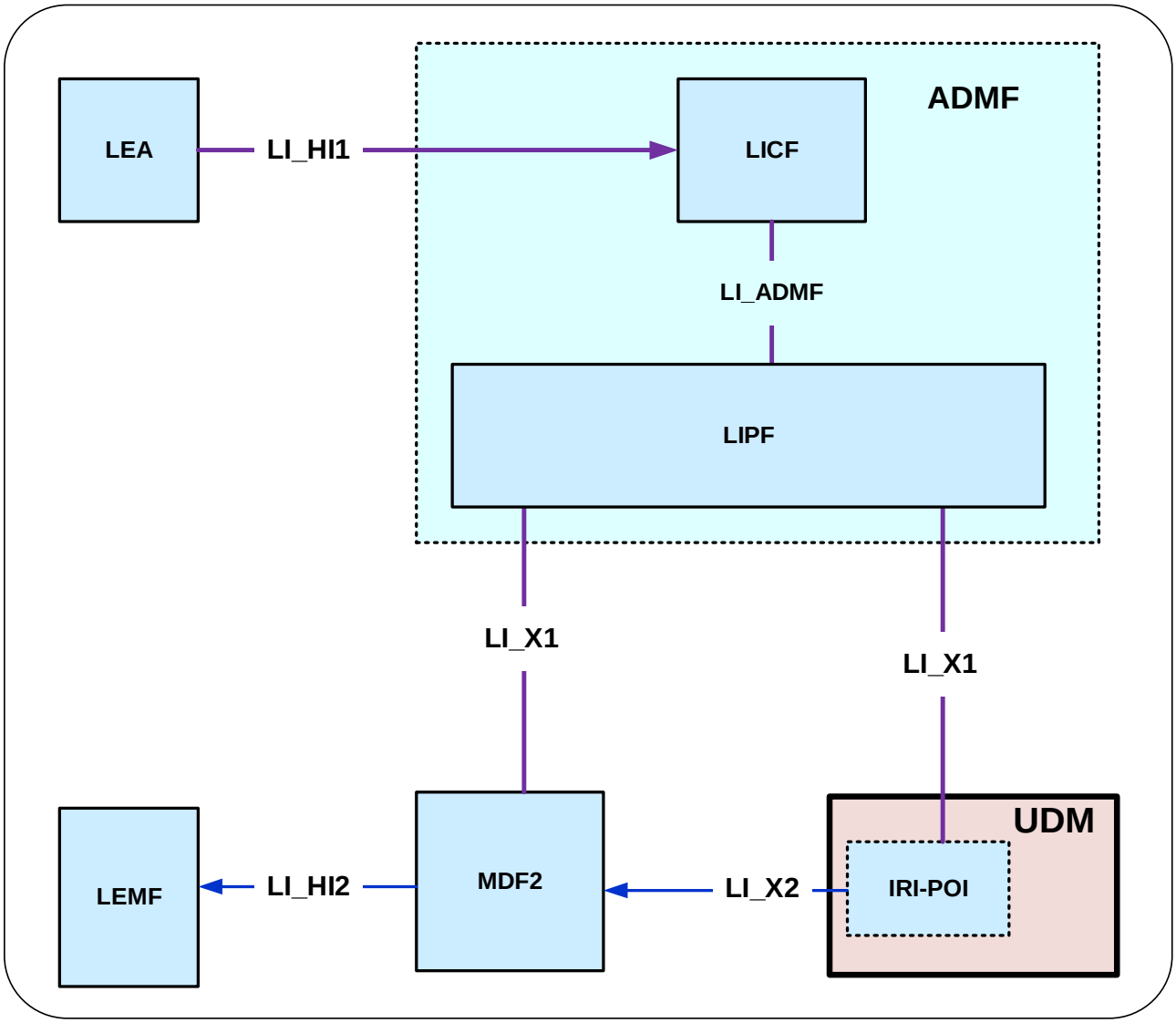

Figure 7.2-1: LI architecture for LI at UDM

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

The LIPF present in the ADMF provisions IRI-POI (over LI_X1) present in the UDM and MDF2. The LIPF may interact with the SIRF (over LI_SI) present in the NRF to discover the UDM in the network.

The IRI-POI present in the UDM detects the target UE's service area registration and subscription related functions, generates and delivers the xIRI to the MDF2 over LI_X2. The MDF2 generates and delivers the IRI messages based on received xIRI to the LEMF over LI_H2.

7.2.2.2 Target identities

The LIPF present in the ADMF provisions the intercept information associated with the following target identities to the IRI-POI present in the UDM:

- SUPI.
- PEI.
- GPSI.
- IMPU/IMPI.

The interception performed on the above identities are mutually independent, even though, an xIRI may contain the information about the other identities when available.

7.2.2.3 Identity privacy

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

The UDM IRI-POI shall provide both the SUPI and the current SUCI in all applicable events defined in clause 7.2.2.4.

7.2.2.4 IRI events

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

- Serving system.
- Subscriber record change.
- Cancel location.
- Location information request.

A serving system xIRI is generated when the IRI-POI present in the UDM detects the target UE registration or re-registration related notifications. The AMF Id or the MME Id, or the VPLMN Id (when the other two are not known) is used as the serving system identifier in a serving system xIRI.

NOTE: The serving system xIRI may carry the information of one or more serving systems based on the target UE's network connectivity.

A subscriber record change xIRI is generated when the IRI-POI present in the UDM detects that the associated GPSI, or SUPI, or PEI is changed. In addition, a subscriber record change xIRI is generated when the associated GPSI or, SUPI, or PEI is de-provisioned. A subscriber record change xIRI is also generated when the target UE's user service identifiers are modified (e.g. subscribed S-NSSAIs, subscribed CAG).

A cancel location xIRI is generated when the IRI-POI present in the UDM detects that a de-registration notification is sent, or received, by the UDM.

A location information request xIRI is generated when the IRI-POI present in the UDM detects that the UDM receiving a query for the location information of the target UE from a different PLMN (e.g. inbound SMS routing) with a known PLMN Id.

7.2.2.5 Common IRI parameters

The list of xIRI parameters are specified in TS 33.128 [15]. All xIRIs shall include the following information:

- Target identity.
- Time stamp.

7.2.2.6 Specific IRI parameters

The parameters in each xIRI are defined in TS 33.128 [15].

7.2.2.7 Network topologies

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

- Non-roaming case.
- Roaming case, in HPLMN.

7.2.3 LI at HSS

7.2.3.1 Architecture

The HSS contains the subscription-related information for all users served by the CSP. The HSS provides the support functions in the mobility management, session setup, user authentication and access authorization.

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

1. Use TS 33.107 [11] and TS 33.108 [21] natively as defined in those documents.
2. Use the capabilities specified below in the present document for stage 2 and in TS 33.128 [15] for stage 3.

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

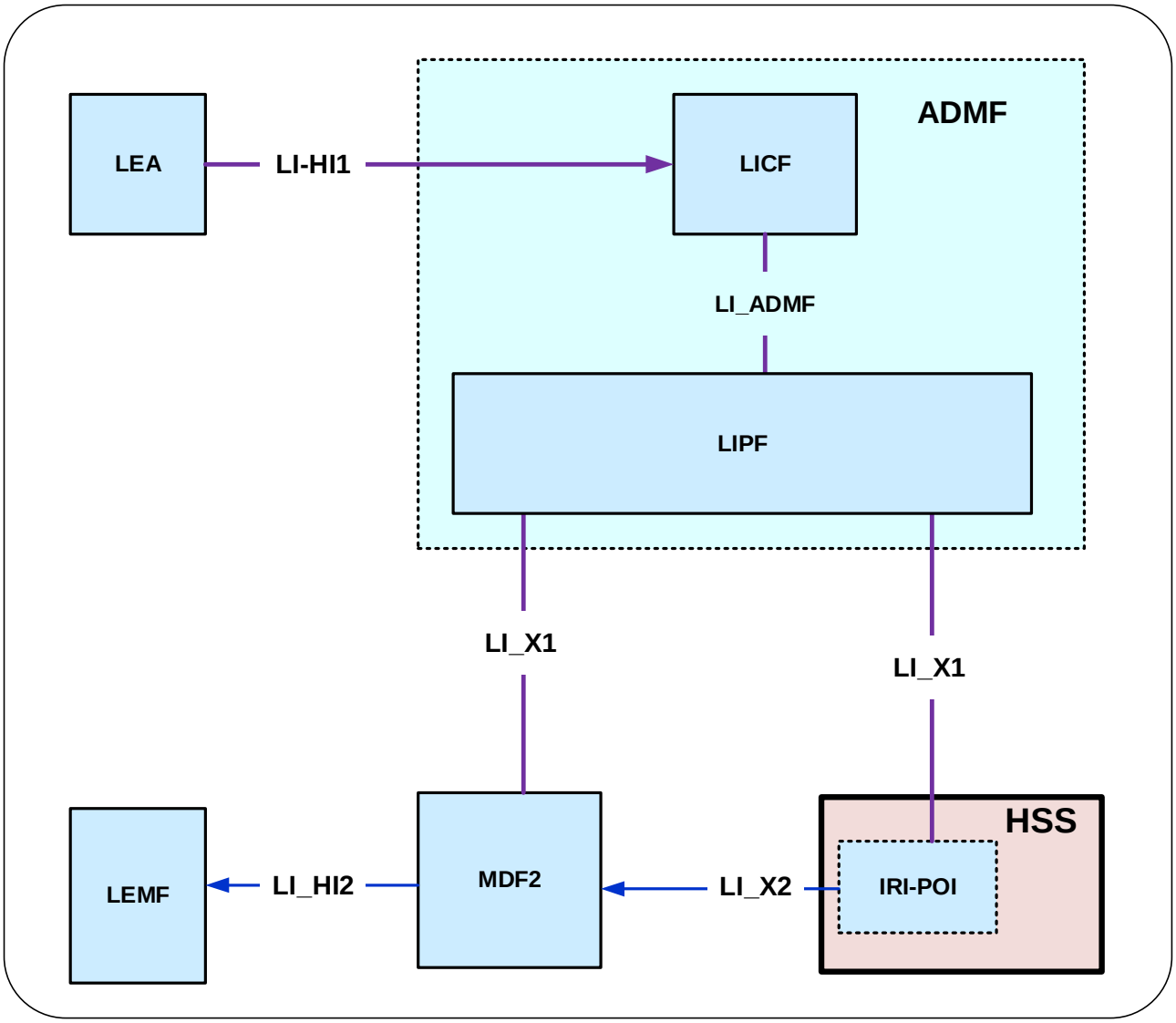

Figure 7.2-2: LI architecture for LI at HSS

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

The LIPF present in the ADMF provisions IRI-POI (over LI_X1) present in the HSS and MDF2.

The IRI-POI present in the HSS detects the target UE's service area registration and subscription related functions, generates and delivers the xIRI to the MDF2 over LI_X2. The MDF2 generates and delivers the IRI messages based on received xIRI to the LEMF over LI_H2.

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

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

7.2.3.2 Target identities

The LIPF present in the ADMF provisions the intercept information associated with the following target identities to the IRI-POI present in the HSS:

- IMSI.
- IMEI.
- MSISDN.

- IMPU/IMPI.

The interception performed on the above identities are mutually independent, even though, an xIRI may contain the information about the other identities when available.

7.2.3.3 IRI events

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

7.2.3.4 Common IRI parameters

The list of xIRI parameters are specified in TS 33.128 [15]. All xIRIs shall include the following information:

- Target identity.
- Time stamp.

7.2.3.5 Specific IRI parameters

The parameters in each xIRI are defined in TS 33.128 [15].

7.2.3.6 Network topologies

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

- Non-roaming case.
-

7.3 Location

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.

7.3.2 Service usage location reporting

7.3.2.1 General

This clause specifies requirements relating to location reporting that is obtained as part of target user usage of network services. Only location reporting that is available as part of the network service being used by the target user is specified in this clause.

7.3.2.2 Embedded location reporting

This clause defines requirements for reporting of location when location is provided as part of other associated interception information sent from the POI to the MDF2.

Location shall be available at the start and end of a user communication. In addition, where available, a POI shall be able to provide location updates to the MDF2 (e.g. due to UE mobility at the AMF or MME).

The following information shall be transferred from the POI to the MDF2 as part of POI events for which location reporting is required:

- Target location(s).
- Date/time of UE location(s) (if target location provided).
- Source location information (if target location provided).

7.3.2.3 Separated location reporting

This clause defines a dedicated location reporting event when location cannot be reported (or is not available) at the same time as the POI output event for which the location was required is sent to the MDF2. The event shall also be used when an updated location becomes available and no other suitable POI output event message is triggered (e.g. mid-session location update).

Location reporting availability shall be the same as for embedded location reporting in clause 7.3.2.2.

The following information needs to be transferred from the POI to the MDF2 in order to enable a MDF2 to perform its functionality:

- Target identity.
- Event date/time.
- Target location(s).
- Date/time of UE location(s).
- Nature and identity of the POI.
- Location source(s).

7.3.3 Lawful Access Location Services (LALS)

7.3.3.1 General

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

LALS shall adhere to the requirements in clauses 6.6 (Security) and 6.3 (Detect and Capture) of TS 33.126 [3]. The LCS supporting LALS shall be able to provide priority to LALS requests. The subscriber location privacy settings (see clause 9 of TS 23.271 [5]) shall be overridden for LALS.

For inbound roaming targets, the VPLMN LCS functional entities fulfilling LALS requests should not communicate with the target's HPLMN, as it may cause detectability issues. Detectability issues may also exist when LALS is invoked for outbound roaming targets.

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

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

The parameters controlling the LALS output are either delivered per warrant over the LI_X1 interface from the ADMF to the LI-LCS Client, or to the Location Triggering Function (LTF, see Clause 7.3.3.3), or are pre-configured in the LI-LCS Client. The LI-LCS Client is an IRI-POI in the CSP network fulfilling the role of the LCS client for LALS purposes.

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

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

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

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

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

7.3.3.2 Target positioning

7.3.3.2.1 General

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

Figure 7.3-1 shows the architecture for LALS where the LI-LCS client provides the target's location and associated information towards the MDF2 over the LI_X2 interface as per the ADMF request for target positioning delivered over LI_X1 interface.

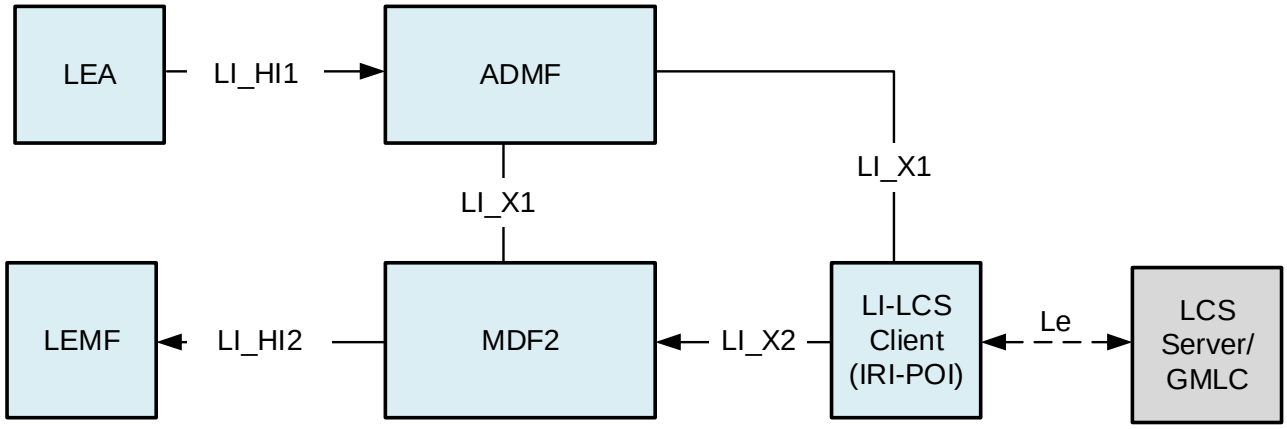

Figure 7.3-1: LALS model for target positioning

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

7.3.3.2.2 Immediate location provision

The request for immediate location provision is delivered to the LI-LCS client over the LI_X1 interface. Upon receiving the request, the LI-LCS client initiates a Location Immediate Request (LIR, see TS 23.271 [5]) to the LCS Server/GMLC supporting LALS over the Le interface and reports the acquired location to the MDF2 over LI_X2.

While waiting for response to an LIR from the LCS Server/GMLC, the LI-LCS client may receive and process additional LIRs from the ADMF over the LI_X1.

NOTE: The LCS Server/GMLC supporting LALS may be optimized to provide the same single location estimation in response to multiple positioning requests arriving in temporal proximity of each other.

The resulting immediate location information is delivered over LI_X2 to the MDF2 and propagated to the LEMF over LI_HI2.

7.3.3.2.3 Periodic location provision

The request for periodic location provision is delivered to the LI-LCS client over the LI_X1 interface.

The request for periodic location from the ADMF to the LI-LCS client may include a set of parameters defining the

duration of reporting, report periodicity, etc. The description of the service response parameters is provided in clause 7.3.3.4. The periodic location result is delivered over LI_X2 to the MDF2 and propagated to the LEMF over LI_HI2.

The periodicity of the LALS reports shall be controlled by the LI-LCS client. The LI-LCS client shall issue a series of Location Immediate Requests (LIR, see TS 23.271 [5]) at required time intervals.

The LI-LCS client provides the acquired location reports to the MDF2 over LI_X2.

7.3.3.3 Triggered location

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

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

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

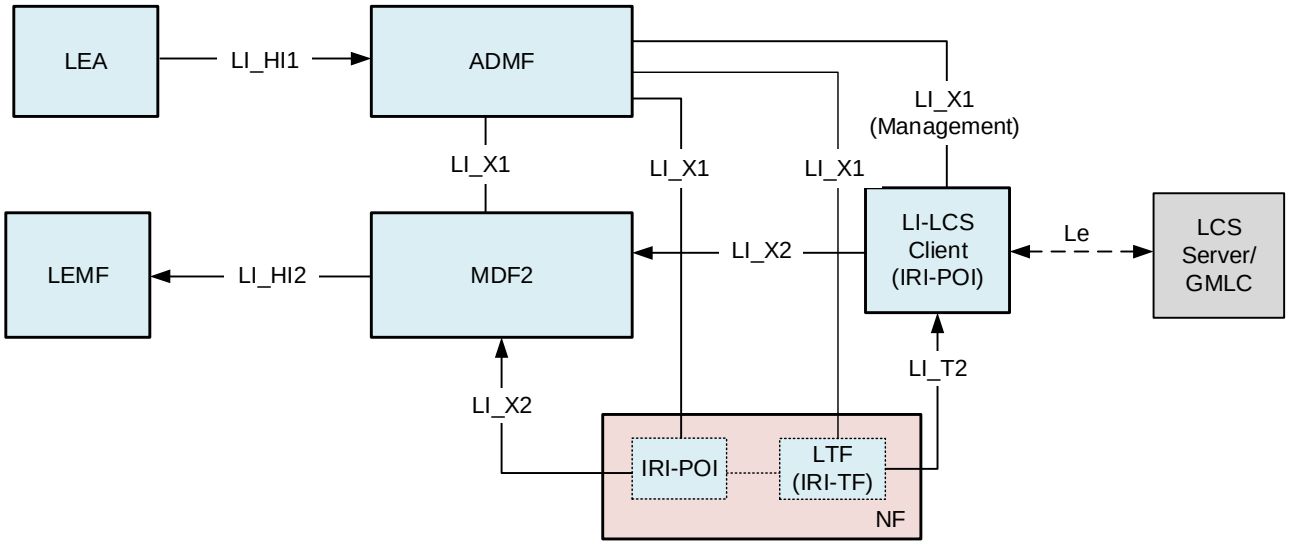

Figure 7.3-2: LALS model for triggered location (POI/LTF option)

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

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

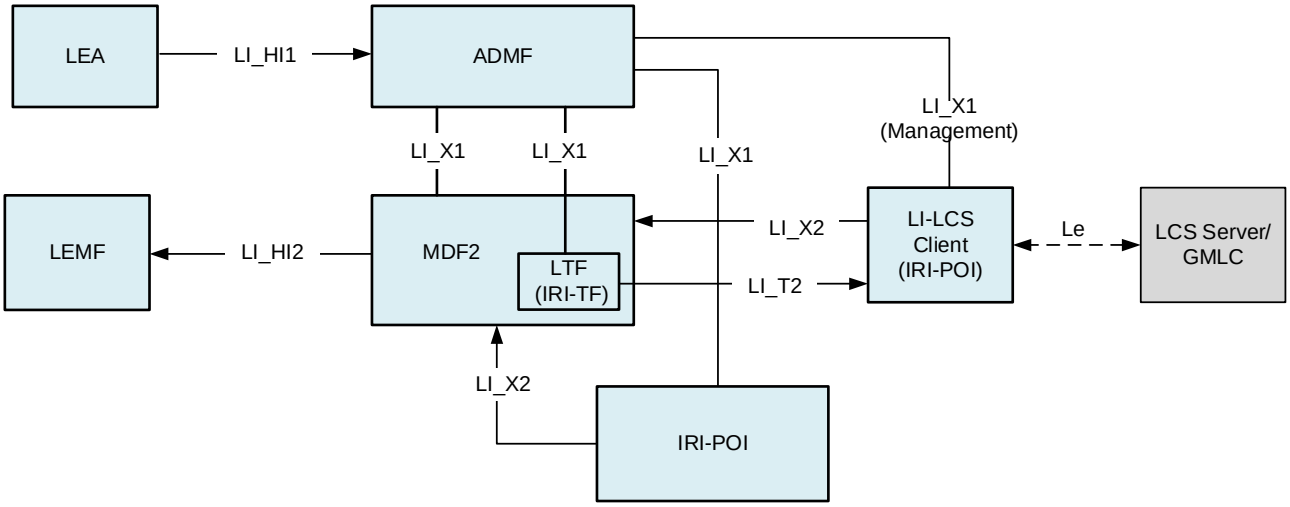

Figure 7.3-3: LALS Model for triggered location (MDF/LTF option)

The request for triggered location is delivered from the ADMF to either an IRI-POI or to a MDF2 over LI_X1 interface along with other parameters of IRI intercept authorization/activation. The IRI-POI (s) or the MDF2 then arm the LTF(s).

The LTF triggers the LI-LCS client over the LI_T2 interface.

The LALS result is delivered to MDF2 from the LI-LCS Client over the LI_X2 interface asynchronously with the associated IRI events delivered by the IRI-POI. To enable correlation between the LALS reports and the associated IRI events, the LTF shall include the correlation information of the IRI event, if provided by the IRI-POI, into the LI_T2 trigger.

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

7.3.3.4 LI_X2 interface for target positioning and triggered location

The following information needs to be delivered from the LI-LCS Client to MDF2 in order to enable the MDF2 to format and deliver LALS intercept product to LEMF:

- Target identity.
- Target reported location(s).
- Date/time(s) location(s) established by reporting function.
- Additional location parameters based on operator policy.
- Correlation information.

7.3.4 Cell database information reporting

When a cell identity is provided for the target's location in an IRI message, the CSP may also provide CSI for the reported cell identity. The MDF2 may retrieve CSI by access to a CSP maintained database (referred to as CSP Cell Database) as shown in figure 7.3.4-1. The CSP delivers the CSI either via the IRI message generated from the corresponding xIRI, or asynchronously in a stand-alone Cell Site Report (CSR) IRI message.

The following information shall be delivered when CSI is provided in IRI message or a MDF2 generated CSR:

- LIID.
- Cell identity.
- Date/time(s) established by MDF2.
- Cell supplemental information.

If CSI for a cell identity has been previously reported to the LEMF for the current interception, CSI may be omitted, if allowed by the warrant.

If the CSP does not support CSR or CSI, the database can be provided by non-real-time means.

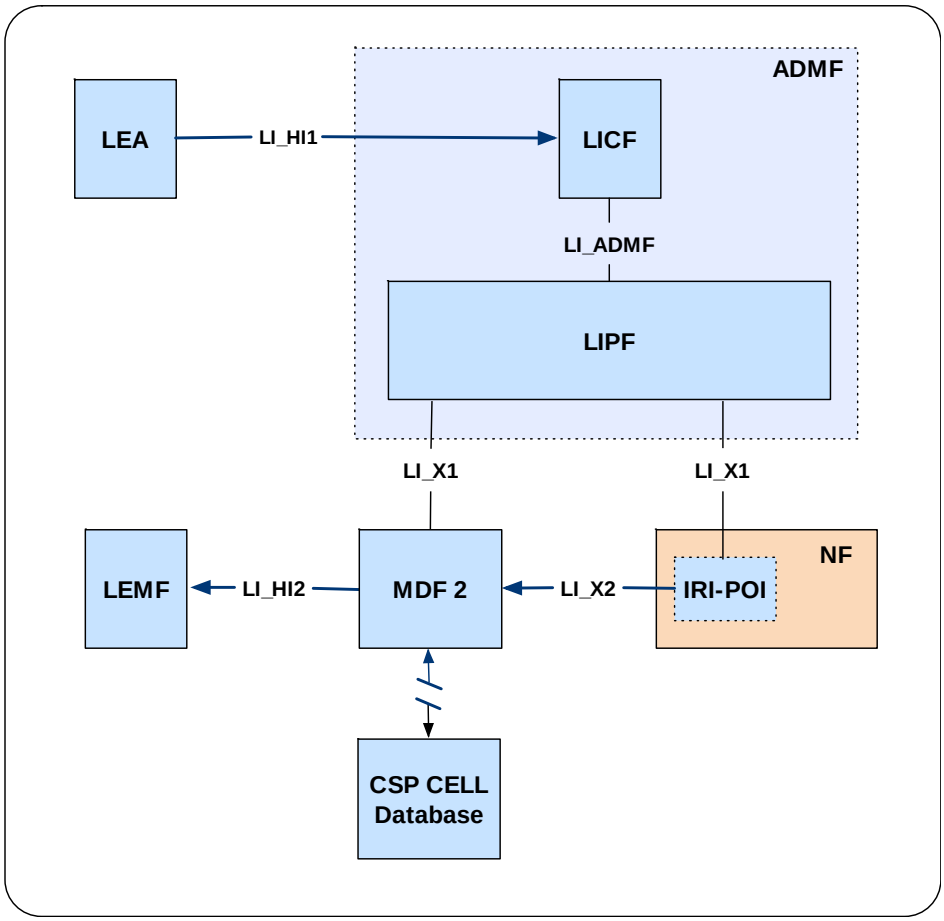

Figure 7.3.4-1: CSP cell database

7.4 IMS

7.4.1 General

Figure 7.4-1 depicts the EPS/5GS-Anchored IMS High Level LI Architecture.

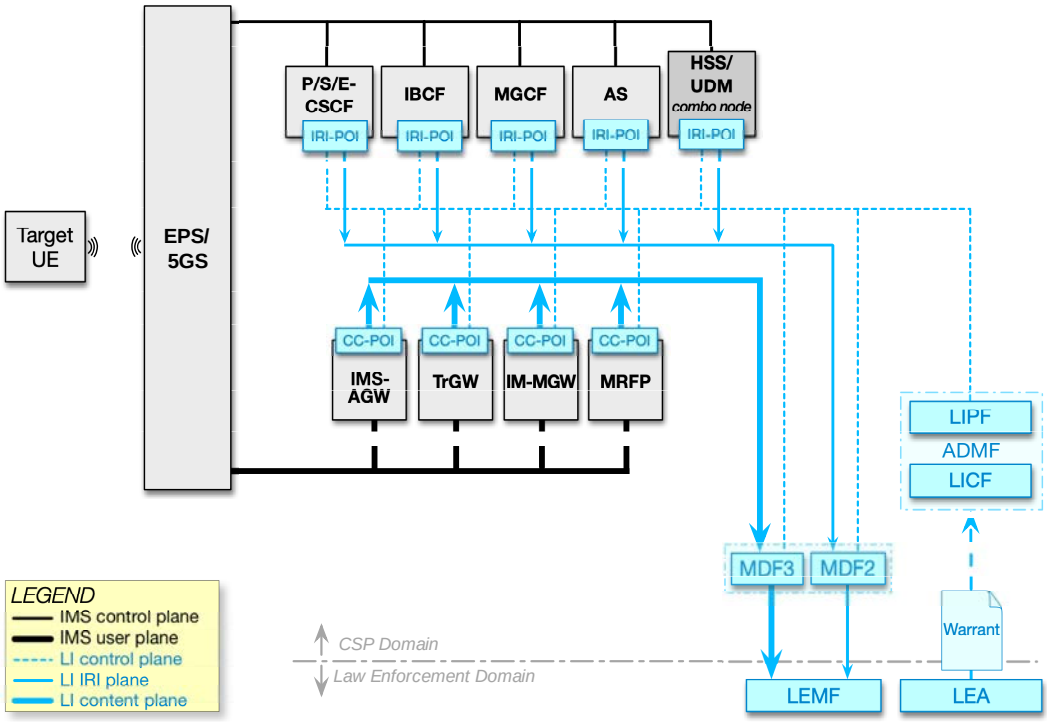

Figure 7.4-1: EPS/5GS-Anchored IMS High Level LI Architecture

7.4.2 Architecture

7.4.2.1 Overview

The capabilities defined in this clause apply for the interception of IMS-based services. The target of interception can be a subscriber of the CSP or a non-local ID.

The network function involved in providing the interception of IMS-based services are determined based on the deployment option, the network configuration, LI service scope and the IMS session including the roaming scenarios. The IRI-POI functions are provided by the network functions that handle the SIP messages (those network functions are referred to as IMS Signalling Functions) and the triggered CC-POI functions are provided by the network functions that handle the media (these network functions are referred to as IMS Media Functions). The CC-TF functions are also provided by the network functions that handle the SIP messages (referred to as IMS Signalling Functions) and manage the IMS Media Functions. The network functions that provide the CC-TF functions can be different from the network functions that provide the IRI-POI functions.

An architecture depicting the LI for IMS is depicted in figure 7.4-2 below.

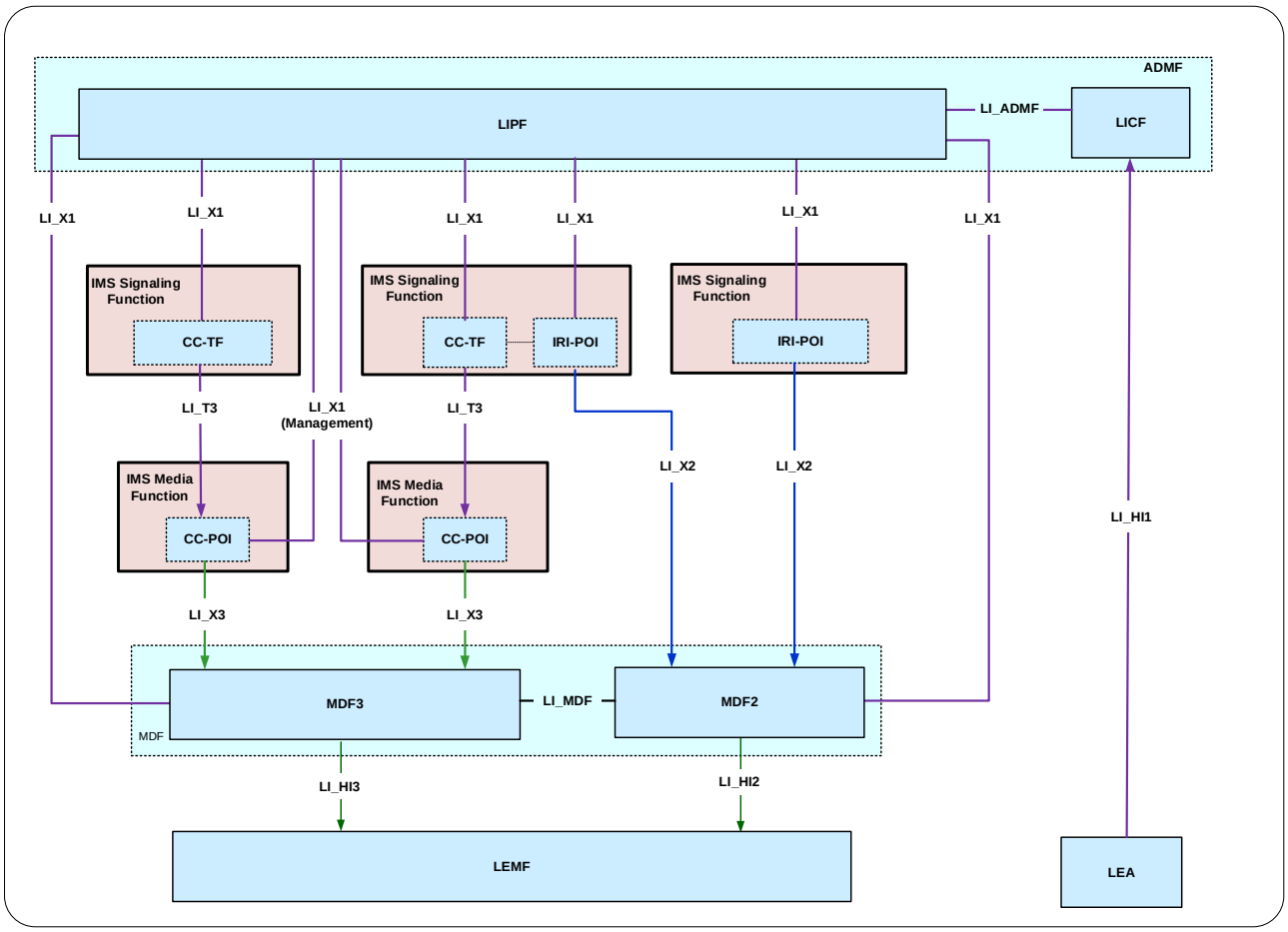

Figure 7.4-2: IMS LI architecture

The LICF present in the ADMF receives the warrant from an LEA, derives the intercept information from the warrant and provides it to the LIPF. The LIPF present in the ADMF provisions IRI-POI, CC-TF, MDF2 and MDF3 over the LI_X1 interfaces.

The CC-TF sends the CC intercept trigger to the CC-POI over LI_T3 interface. The IRI-POI generates the xIRI and delivers the same to the MDF2 over LI_X2 interface. The CC-POI generates the xCC and delivers the same to the MDF3 over LI_X3 interface.

The MDF2 generates IRI messages from the received xIRI and delivers those IRI messages to the LEMF over LI_HI2 interface. The MDF3 generates the CC from the received xCC and delivers that CC to the LEMF over LI_HI3 interface.

The network configuration and IMS service scenarios including the roaming scenarios determine the network functions that provide the IRI-POI, CC-TF and CC-POI functions. The network function that provides the IRI-POI or CC-TF is referred to as IMS Signalling Function in figure 7.4-2 and the network function that provides the CC-POI functions is referred to as IMS Media Function in figure 7.4-1.

NOTE: The details of correlation between the xIRI and the xCC when IRI-POI and CC-TF are not co-located is not defined in the present document. The IRI-POI and CC-TF are logical functions and they may be handled by the same process when they are co-located in the same IMS Signalling Function.

7.4.2.2 Target identities

The LIPF provisions the intercept related information associated with the following target identities to the IRI-POI and CC-TF present in the IMS Signalling Functions:

- IMPU.
- IMPI.
- PEI (IMEI only).

- IMEI.

The IRI-POI and CC-TF shall also support interception of non-local identities in any of the IMPU formats (SIP URI, TEL URI as well as the E.164 number in a SIP URI or TEL URI).

NOTE It is assumed that GPSI/MSISDN is mapped to IMPU, and SUPI/IMSI is mapped to IMPI.

7.4.2.3 Target identification

Depending on the session direction, different SIP parameters are used to identify the target subscriber.

Further details on the use of SIP parameters in identifying a target is described in TS 33.128 [15].

7.4.3 IRI-POI

7.4.3.1 General

The IRI-POI detects the SIP messages that are related to a target subscriber and then generates and delivers the related xIRI to the MDF2 over LI_X2.

The following IMS Network Functions (i.e. IMS Signalling Functions) that handle SIP signalling for IMS sessions may provide the IRI-POI functions:

- S-CSCF.
- E-CSCF.
- P-CSCF.
- IBCF.
- MGCF.
- Conference AS/MRFC.
- PTC server.

Clause 7.4.6 gives more information from network topology/session perspective how different IMS Network Functions are to be used in providing the IRI-POI functions.

7.4.3.2 IRI events

The IRI-POI present in the IMS Signalling Function generates the following xIRI:

- Encapsulated SIP message.
- CC unavailable in serving PLMN.
- Start of interception with an established IMS session.

The encapsulated SIP message xIRI is generated and delivered to the MDF2 when the IRI-POI in the IMS Signalling Function detects that a SIP message is received from, or sent to, a target or processed on behalf of a target at the IMS Signalling Function.

The CC unavailable in PLMN xIRI is generated and delivered to the MDF2 for the session scenarios where access to the target media is not available to the CSP (see clause 7.4.7.1).

The start of interception with an established IMS session xIRI is generated when an interception is activated on an established IMS session. To support the possibility of generating such an xIRI, the IMS Signalling Function shall store and maintain the session related information including the media information for the life of all IMS sessions.

7.4.3.3 Common IRI parameters

The list of parameters in each xIRI are defined in TS 33.128 [15]. Each xIRI shall include at the minimum the following information:

- Target identity.
- Additional identities associated with the target as observed by the IRI-POI.
- Time stamp.
- Correlation information.

7.4.3.4 Specific IRI parameters

The parameters in each xIRI are defined in TS 33.128 [15].

7.4.4 CC-TF and CC-POI

7.4.4.1 General

The CC-TF detects the SIP messages that are related a target and then generates and sends a trigger to the CC-POI over the LI_T3 reference point.

The CC-POI based on the trigger detects the media to be intercepted, generates the xCC and delivers the same to the MDF3.

The following IMS Network Functions (i.e. IMS Media Functions and IMS Signalling Functions) may provide the CC-POI and CC-TF functions:

- IMS-AGW with CC-TF in P-CSCF.
- TrGW with CC-TF in IBCF.
- IM-MGW with CC-TF in MGCF.
- MRFP with CC-TF in Conference AS/MRFC (see NOTE 2).
- PTC Server with CC-TF in PTC Server (see NOTE 1).

Clause 7.4.6 gives more information from network topology/session perspective how different IMS Network Functions are to be used in providing the CC-TF/CC-POI functions.

NOTE 1: The PTC Server provides the IRI-POI and CC-POI functions, accordingly, PTC Server itself is the CC-TF.

NOTE 2: Conference AS, MRFC and MRFP together are referred to as Conference Server. Conference AS/MRFC provide the conference focus functions as defined in TS 24.147 [28].

7.4.4.2 CC intercept trigger

The CC-TF shall send CC intercept trigger to the CC-POI over LI_T3. The CC intercept trigger, at the minimum, shall consist of the following:

- Correlation Identifier.
- Media Identifier (e.g. SDP information).

The Correlation Identifier is used to correlate the xCC with the corresponding xIRI and is delivered from the CC-POI over the LI_X3 interface to the MDF3.

The Media Identifier is used to identify the media packets that have to be intercepted.

7.4.4.3 Common CC parameters

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

- target identity.
- correlation identifier
- time stamp.
- direction (indicates media is from or to the target).

7.4.5 Correlation of xCC and xIRI

The IRI messages derived from the xIRI and CC derived from xCC for a session shall be correlated to each other using the correlation information received in the xIRI and xCC. The details of this are specified in TS 33.128 [15].

7.4.6 Network topologies

7.4.6.1 General

The IMS Network Functions that provide the IRI-POI, CC-TF and CC-POI functions can vary based on the network topology and session scenarios such as:

- Network topologies:
  - Non-roaming.
  - Roaming case with Local Break Out (LBO), VPLMN.
  - Roaming case with LBO, HPLMN.
  - Roaming case with Home Routed (HR), VPLMN.
  - Roaming case with HR, in HPLMN.
- Session types:
  - Normal sessions.
  - Emergency sessions.
  - Redirected sessions.
  - IMS specific services such as conferencing, PTC.
- Target type:
  - Non-local ID target.

A deployment option within the CSP may also have a role in selection of the Network Functions. In the case of roaming case, the interception performed in the VPLMN and HPLMN are based on separate independent warrants.

More detailed description of these scenarios is given in TS 33.128 [15].

7.4.6.2 IMS Network Functions providing the IRI-POI

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

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

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

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

NOTE 1: For originated emergency sessions handled in the fixed networks, where S-CSCF is also part of an emergency session, the S-CSCF based IRI-POI as a deployment option may also be considered.

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

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

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

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

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

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

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

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

Table 7.4.6.2-3: Extension of table 7.4.6.2-2

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

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

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

7.4.6.3 IMS Network Functions providing the CC-TF and CC-POI functions

The IMS Network Functions that handle the target side (including the non-local ID target) of the session provide the CC-TF and CC-POI functions. For redirected scenarios, the IMS Network Functions that handle the redirected-to-user side of the session provide the CC-TF and CC-POI functions.

Table 7.4.6.3-1 provides the IMS Network Functions that provide the CC-TF functions when the CC-POI functions are provided by the IMS Media Functions as indicated (also see clause 7.4.4.1).

Table 7.4.6.3-1: Mapping between the IMS Network Functions providing the CC-TF and the CC-POI functions

CC-POI	CC-TF
PGW (NOTE 1)	P-CSCF
PGW-U (NOTE 1)	P-CSCF
IMS-AGW	P-CSCF
MRFP	Conference AS/MRFC
PTC-Server	PTC-Server
TrGW	IBCF
IM-MGW	MGCF

NOTE 1: This is defined in TS 33.107 [11] and outside the scope of the present document.

Table 7.4.6.3-2 below identifies the IMS Media Functions that provide the CC-POI functions in a non-roaming case for session scenarios (PGW and PGW-U based options are not shown in the table).

Table 7.4.6.3-2: IMS Media Functions providing the CC-POI functions (non-roaming case)

Session type/target type	CC-POI
Normal sessions	IMS-AGW
Emergency sessions	IMS-AGW
Redirected sessions: intra-PLMN	IMS-AGW
Redirected sessions: inter-PLMN (CS domain)	IM-MGW
Redirected sessions: inter-PLMN (IMS-domain)	TrGW
Conference (NOTE 4)	MRFP
PTC	PTC- Server
Non-local ID in CS domain (NOTE 2)	IM-MGW
Non-local ID in IMS domain (NOTE 2)	TrGW

NOTE 2: Non-roaming means that the local served user is non-roaming.

Table 7.4.6.3-3 below identifies the IMS Media Functions that provide the CC-POI functions in a roaming case for various session scenarios (PGW and PGW-U based options are not shown in the table).

Table 7.4.6.3-3: IMS Media Functions providing the CC-POI functions (roaming case)

Session type/target type		Local Breakout (LBO)			Home Routed (HR)	
		HPLMN	VPLMN		HPLMN	VPLMN
			Default	Alternate Option		
Normal sessions		TrGW	IMS-AGW	-	IMS-AGW	N9HR/ S8HR
Emergency sessions		-	IMS-AGW	-	-	IMS-AGW
Redirected sessions: intra-PLMN	Redirected-to-party non-roaming	IMS-AGW	-	-	IMS-AGW	-
	Redirected-to-party roaming	TrGW	-	-	IMS-AGW	-
Redirected sessions: inter-PLMN	Redirected-to-party in CS domain	IM-MGW	-	-	IM-MGW	-
	Redirected-to-party in IMS domain	TrGW	-	-	TrGW	-
Conference (NOTE 4)		MRFP	-	-	MRFP	-
PTC		PTC-Server	-	-	PTC-Server	-
Non-local ID in CS domain (NOTE 3)		IM-MGW	IMS-AGW	TrGW	IM-MGW	N9HR/ S8HR
Non-local ID in IMS domain (NOTE 3)		TrGW	IMS-AGW	TrGW	TrGW	N9HR/S8HR

NOTE 3: Roaming means that the local served user is roaming.

NOTE 4: When a normal session is extended to a conference session, the IMS-AGW that provides the CC-POI functions prior to the conference may continue to provide the CC-POI functions as an alternate, or in addition, to the MRFP. In that case, the P-CSCF provides the CC-TF functions for the CC-POI in the IMS-AGW.

7.4.7 Roaming cases

7.4.7.1 Media unavailable in a roaming case

For roaming targets, depending on the roaming architecture deployed, media of the target may not enter the HPLMN for certain session scenarios. In such situations, the HPLMN served with the warrant shall be able to do the following:

- Perform the interception without the CC and report to the LEMF that the CC is unavailable due to target's roaming situation. Note that the Serving System message (reported by the UDM/HSS) also indicates to the LEMF that the target is roaming.
- When a new warrant is activated on a target with an ongoing IMS session with the CC not available, the HPLMN serving the new warrant shall report the CC unavailability indication to the LEMF associated with the new warrant.

See TS 33.128 [15] for the method used to report the CC unavailability indication.

7.4.7.2 S8HR

7.4.7.2.1 Background

The term S8HR is used to denote the home-routed roaming architecture for VoEPS UEs. Within the VPLMN with S8HR, the IMS signalling messages are carried over the GTP tunnel that corresponds to the IMS signalling bearer and the media packets are carried over the GTP tunnel that corresponds to the media bearer. (i.e. a dedicated EPS Bearer is used to carry the media packets). The EPS Bearer ID of the IMS signalling bearer is always linked to the dedicated EPS Bearer used as a media bearer.

The SGW/PGW within the EPC may implement control plane and user plane functions in a combined form or in a separated form. In a separated form, the SGW-C/PGW-C provides the control plane functions and SGW-U/PGW-U provides the user plane functions.

NOTE: With S8HR, the PGW (or PGW-C/PGW-U) resides in the HPLMN.

7.4.7.2.2 LI architecture

The present document specifies two options for implementing the LI functions for voice services with S8HR as the roaming architecture:

1. Use the capabilities specified below in the present document for stage 2 and in TS 33.128 [15] for stage 3.
2. Use the capabilities defined in TS 33.107 [11] and TS 33.108 [21] natively as defined in those documents.

According to the present document, to provide the lawful interception of voice services in the VPLMN with S8HR, the architecture presented in figure 7.4.7.4-1 is used with SGW-C providing the BBIFF-C and SGW-U providing the BBIFF-U functions.

NOTE 1: The overall architecture and functions related to the lawful interception of voice services of inbound roaming targets with S8HR as the roaming architecture is also referred in the present document as S8HR LI.

NOTE 2: The LI functions for SGW in a combined form can be visualized presuming that SGW-C and SGW-U are provided by the same network function. In this mode, the BBIFF-C and BBIFF-U functions are provided by BBIFF.

S8HR LI solution requires that Access Point Name (APN) can be identified as being used for S8HR and therefore can be used to identify that the EPS Bearers are used for inbound roamers with S8HR.

7.4.7.2.3 S8HR LI Process

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

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

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

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

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

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

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

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

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

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

7.4.7.2.4 CC intercept trigger

The CC-POI and IRI-POI functions are provided by the embedded functions LMISF-CC and LMISF-IRI within the LMISF. As such the only interaction required between the two is to establish the correlation between the xCC and xIRI at an IMS session-leg level.

The LMISF-IRI instructs the BBIFF-C present in the SGW-C to deliver the user plane packets (to LMISF-CC) from the IMS media bearer linked to the IMS signalling bearer when it determines that an IMS session is associated with a target and requires CC interception. The BBIFF-C forwards the instruction along with the linked IMS signalling bearer information to BBIFF-U present in the SGW-U.

7.4.7.2.5 S8HR LI and Target UE Mobility

During a session that involves the target UE, the SGW-C/SGW-U associated with the BBIFF-C/BBIFF U can change.

To support the continued interception of IMS sessions, the BBIFF-C in the new SGW-C notifies the LMISF-IRI that a BBIFF relocation has occurred.

The LMISF-IRI provides the functions described in clause 7.4.7.4.12 to support the continued and correlated interception for the CC.

NOTE: The LMISF should not disrupt the ongoing interception, if an IMS signalling bearer deletion notification is received from the BBIFF-C present in the old SGW-C.

7.4.7.3 N9HR

7.4.7.3.1 Background

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

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

7.4.7.3.2 LI architecture

To provide the lawful interception of voice services in the VPLMN with N9HR, the architecture presented in figure 7.4.7.4-1 is used with SMF providing the BBIFF-C and UPF providing the BBIFF-U functions.

NOTE: The overall architecture and functions related to the lawful interception of voice services of inbound roaming targets with N9HR as the roaming architecture is also referred in the present document as N9HR LI.

N9HR LI requires that a Data Network Name (DNN) can be identified as being used for N9HR and therefore can be used to identify that PDU sessions are used for inbound roamers with N9HR.

The BBIFF-C and BBIFF-U functions are provided by adopting a subset of LI functions defined for LI at SMF/UPF as defined in clause 6.2.3 and TS 33.128 [15].

7.4.7.3.3 N9HR LI Process

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

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

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

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

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

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

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

- The LIPF configures the BBIFF-C present in the SMF to notify the LMISF-IRI whenever a PDU session is created, modified, or deleted for inbounding roaming UEs with an N9HR DNN.
- The BBIFF-C present in the SMF notifies the LMISF-IRI whenever it detects that a PDU session is created, modified, or deleted for inbound roaming UEs with N9HR DNN. The UE location information and the PDU session ID is included in such notifications.
- When the LMISF-IRI determines that IMS voice media interception is required, the LMISF-IRI instructs the BBIFF-C present in the SMF with the PDU session information that the IMS voice media related user plane packets from that PDU session are to be delivered to LMISF-CC.

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

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

7.4.7.3.4 CC intercept trigger

The CC-POI and IRI-POI functions are provided by the embedded functions LMISF-CC and LMISF-IRI within the LMISF. As such the only interaction required between the two is to establish the correlation between the xCC and xIRI at an IMS session-leg level.

The LMISF instructs the BBIFF-C present in the SMF to deliver to (to LMISF-CC) the IMS voice media related user plane packets from the PDU session associated with the intercepted IMS session. The BBIFF-C present in the SMF forwards the instruction along with the PDU session information to BBIFF-U present in the UPF.

7.4.7.3.5 N9HR LI and Target UE Mobility

During a session that involves the target UE, the SMF that has the BBIFF-C, or the UPF that has the BBIFF-U can change.

To support the continued interception of IMS sessions, the BBIFF-C in the new SMF notifies the LMISF-IRI that a BBIFF (i.e., SMF or UPF) relocation has occurred.

The LMISF-IRI provides the functions described in clause 7.4.7.4.12 to support the continued and correlated interception of CC.

NOTE: The LMISF should not disrupt the ongoing interception, if a PDU session deletion related notification is received from the BBIFF-C present in the old SMF.

7.4.7.4 LI in VPLMN with home-routed roaming architecture

7.4.7.4.1 Background

With home-routed roaming architecture, all the IMS Signalling Functions and IMS Media Functions reside in the HPLMN. National regulations may still require the VPLMN to have the capabilities to perform the lawful interception of voice services involving the inbound roaming targets. The LI capabilities provided in the VPLMN with home-routed roaming architecture shall be to the same extent as the LI capabilities provided in the VPLMN with LBO approach as the roaming architecture.

The IMS signalling messages are exchanged between the UE and the P-CSCF (in HPLMN) and the media is exchanged between the UE and the IMS-AGW (in HPLMN).

7.4.7.4.2 LI architecture

To provide the lawful interception of voice services in the VPLMN with home-routed roaming architecture, new LI-specific functions are introduced to examine the packets that flow through the VPLMN packet core network functions in order to generate IRI and CC when the communication involves an inbound roaming target.

Figure 7.4.7.4-1 shown below illustrates a generic LI architecture for home-routed roaming architecture in the VPLMN.

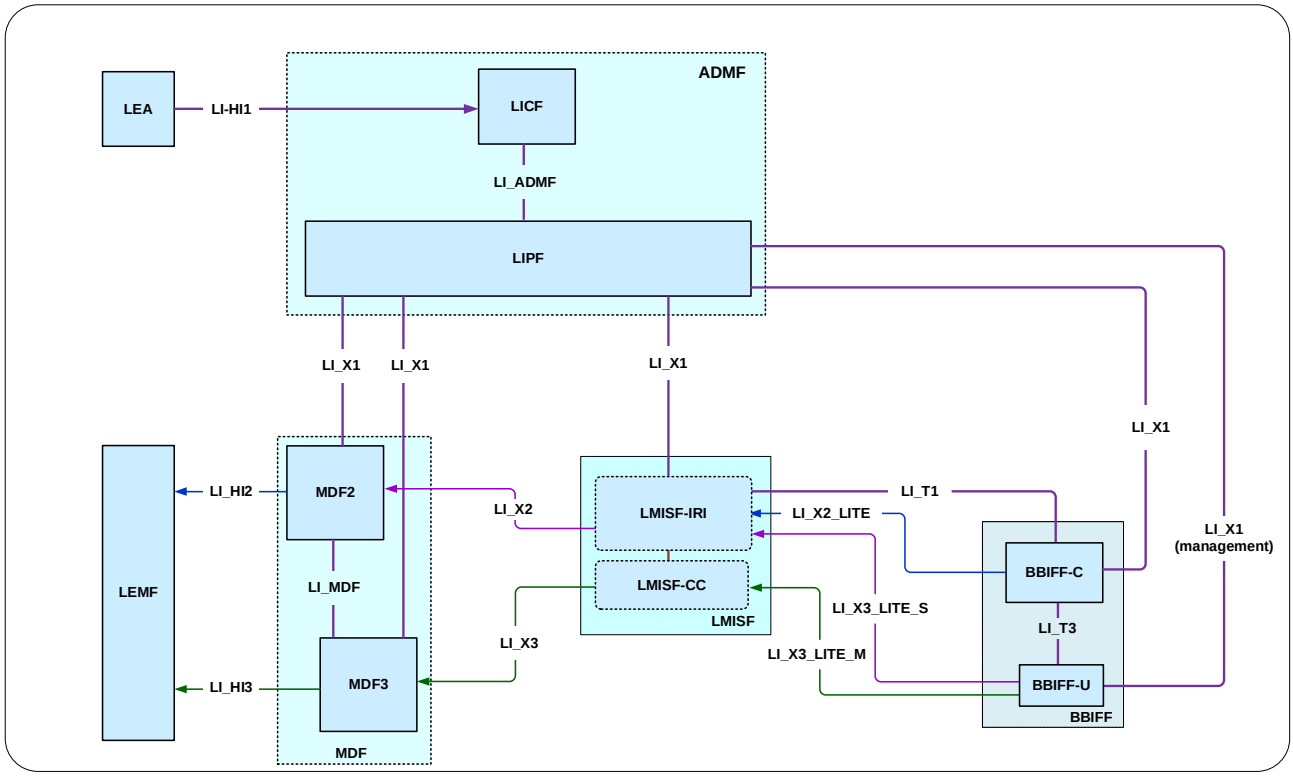

Figure 7.4.7.4-1: VPLMN generic LI architecture for home-routed roaming

NOTE: See clause 7.4.7.4.10 for brief descriptions of the LI functions and interfaces depicted in figure 7.4.7.4-1.

7.4.7.4.3 Target identifiers

The target identifiers used for inbound roaming UEs are same as the identifiers used for IMS sessions in the VPLMN with LBO as the roaming architecture. See clause 7.4.2.2 for further details.

7.4.7.4.4 Target identification

Depending on the session direction, different SIP parameters are used to identify the target. The SIP parameters used to identify the target can be different from the SIP parameters used to identify a target at the P-CSCF (with LBO as the roaming architecture).

Further details on the use of SIP parameters in identifying a target are described in TS 33.128 [15].

7.4.7.4.5 IRI events

The IRI events are same as the xIRI defined for IMS sessions in the VPLMN with LBO as the roaming architecture. See clause 7.4.3.2 for details.

7.4.7.4.6 IRI parameters

The IRI parameters are the same as those defined for IMS sessions in the VPLMN with LBO as the roaming architecture. See clauses 7.4.3.3 and 7.4.3.4 for details.

7.4.7.4.7 CC intercept trigger

The LMISF-IRI instructs the BBIFF-C (over the LI_T1 interface) to deliver the IMS media packets when it determines that an IMS session is associated with a target and requires CC interception. The BBIFF-C forwards the instruction to BBIFF-U over the LI_T3 interface.

7.4.7.4.8 CC parameters

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

7.4.7.4.9 Correlation of xCC and xIRI

The LMISF assigns the correlation number for an IMS session and uses the same correlation number in the associated xIRI and xCC. The interaction between the LMISF-IRI that generates the xIRI and LMISF-CC that generates the xCC is an internal function of LMISF.

7.4.7.4.10 LI specific functions and interfaces

The additional LI specific functions and interfaces introduced to support the LI with home-routed roaming architecture shown in figure 7.4.7.4-1 are listed below:

- LMISF (LI Mirror IMS State Function): A logical LI specific function that provides the IMS state function for LI purposes. The LMISF provides the IRI-POI and CC-POI functions. The LMISF also initiates the required trigger for IMS media interception. The LMISF may be viewed as consisting of two embedded functions: 1) LMISF-IRI (handling the IMS signalling related LI functions, i.e. IRI-POI), 2) LMISF-CC (handling the IMS media related LI functions, i.e. CC-POI). The interface between the two embedded functions is not defined.

NOTE 1: The present document assumes one LMISF per VPLMN for a given roaming agreement.

NOTE 2: The term LMISF is used when a description applies to LMISF-IRI or LMISF-CC.

- BBIFF (Bearer Binding Intercept and Forward Function): Binds the IMS signalling and media to the LMISF for interception purpose. The BBIFF may be split into two BBIFF-C and BBIFF-U, with the former present in the NF that provides the control plane related functions and the latter present in the NF that provides the user plane related functions associated with the inbound roaming UEs.

- LI_X2_LITE: Used to carry the control plane information (e.g. packet data connection related notifications, UE location) from BBIFF-C to LMISF-IRI.

- LI_X3_LITE_S: Used to forward the IMS signalling related user plane packets of inbound roaming UEs from BBIFF-U to the LMISF-IRI.

- LI_X3_LITE_M: Used to forward the IMS media related user plane packets of inbound roaming target's UE from BBIFF-U to the LMISF-CC.

- LI_T1: Used to instruct the BBIFF-C that user plane packets of the associated IMS media need to be captured and delivered to the LMISF-CC.

- LI_T3: Used to instruct the BBIFF-U to capture and deliver the selective user plane packets of inbound roaming UEs to the LMISF.

The user plane packets reported by BBIFF-U include the IMS signalling related packets and IMS media related packets. A condition required for this LI architecture is that LMISF shall have access to the IMS signalling messages and the IMS media packets in an unencrypted form.

NOTE 3: The LI functions available within the VPLMN network functions that have access to the packet data connections that carry the IMS signalling and IMS media may be used to provide the BBIFF-C, BBIFF-U functions.

7.4.7.4.11 LI Process

The following steps happen for all home-routed inbound roaming UEs irrespective of whether those UEs are associated with a target:

- The LIPF configures the BBIFF-C (over LI_X1 interface) to notify the LMISF-IRI whenever home-routed inbound roaming UEs establish, modify or delete the IMS signalling and the IMS media channels. The UE exchanges the IMS signalling messages with the P-CSCF residing in the HPLMN over the IMS signalling channel and IMS media with the IMS-AGW residing in the HPLMN over the IMS media channel. The LIPF also provides the same information to LMISF-IRI (over LI_X1 interface) in order to let it know the notifications to be expected from the BBIFF-C.

NOTE 1: The term *channel* is a generic term used in this description to represent IMS signalling or media related packet data connection within a PDN (Packet Data Network) connection.

- The BBIFF-C notifies the LMISF-IRI (over LI_X2_LITE interface) whenever the IMS signalling channel or the IMS media channel is established, modified or deleted for home-routed inbound roaming UEs. The UE location information is included in such notifications. The BBIFF-C instructs the BBIFF-U (over LI_T3 interface) to deliver the appropriate IMS signalling related user plane packets to the LMISF-IRI.

- The BBIFF-U delivers the IMS signalling related user plane packets to the LMISF-IRI (over the LI_X3_LITE_S interface).

The following steps are performed for the target UEs:

- The LIPF provisions the LMISF-IRI, MDF2 and MDF3 (over LI_X1 interface) with the IMS target information.

- When the received user plane packets from the BBIFF-U represent IMS signalling messages associated with a target, the LMISF-IRI generates the xIRI and delivers them to the MDF2 over the LI_X2 interface.

- Upon identifying that IMS signalling messages are associated with a target that requires CC interception, the LMISF-IRI instructs the BBIFF-C (over LI_T1 interface) that the user plane packets that represent associated IMS media (i.e. from the IMS media channel associated with the IMS signalling channel) are to be delivered to LMISF-CC.

- The BBIFF-C instructs the BBIFF-U (over LI_T3 interface) to deliver user plane packets that represent the associated IMS media to the LMISF-CC.

- The BBIFF-U delivers the indicated user plane packets that represent the IMS media to the LMISF-CC (over LI_X3_LITE_M interface). The LMISF-CC generates xCC from the received IMS media related user plane packets and delivers them to the MDF3 over LI_X3 interface along with the information that correlates the xCC with the xIRI.

NOTE 2: LMISF-CC interacts with the LMISF-IRI to correlate the xCC with the xIRI.

- When all IMS sessions for a target UE have ended, LMISF-IRI instructs the BBIFF-C (over LI_T1 interface) to stop the delivery of IMS media related user plane packets. Upon receiving such a notification, the BBIFF-C instructs the BBIFF-U (over LI_T3 interface) to stop the delivery of the IMS media related user plane packets to the LMISF-CC.

NOTE 3: In the above steps, BBIFF-C and BBIFF-U functions are not aware of any IMS target information (i.e. SIP URI or TEL URI).

NOTE 4: The LMISF-IRI includes the target UE location (when required) in the xIRI based on the UE location that it receives from the BBIFF-C.

The LMISF-IRI stores the IMS signalling messages received from the BBIFF-U for a potential future LI activation (i.e. mid-call interception). Furthermore, the xCC generated from the IMS media related user plane packets may be associated with different session-legs, and hence may have different correlation numbers.

When the inbound roaming UE deregisters for the IMS signalling (i.e. with HPLMN), the LMISIF shall ensure that deregistration is mirrored in its own maintained state for that UE.

7.4.7.4.12 Target UE Mobility

During a session that involves the target UE, the network function associated with the BBIFF-C, or the BBIFF U can change. The lawful interception of IMS sessions involving a target shall continue when such a relocation happens. The xIRI and xCC delivered before and after the relocation shall be correlated.

To support the continued interception of IMS sessions, the BBIFF-C in the new network function notifies the LMISF-IRI (over LI_X2_LITE interface) that a BBIFF relocation has occurred.

The LMISF-IRI provides the following functions to support the continued and correlated interception of CC:

- When a notification is received from the BBIFF-C that a BBIFF relocation has occurred, examine to see whether any IMS session is setup for the UE and is being intercepted.
- If an intercepted IMS session is setup, examine to see whether a CC interception for that IMS session is required.
- If the intercepted IMS session requires CC interception, inform the new BBIFF-C (over the LI_T1 interface) with an instruction that the user plane packets that represent associated IMS media are to be delivered to LMISF-CC.

Further handling of CC interception is as defined in clause 7.4.7.4.11.

7.5 MMS

7.5.1 Overview

MMS service is defined in TS 22.140 [19], OMA's MMS Architecture OMA-AD-MMS-V1_3-20110913-A [17], and OMA's Multimedia Messaging Service Encapsulation Protocol OMA-TS-MMS_ENC-V1_3-20110913-A [18].

In a 3GPP network, the MMS Proxy-Relay handles the MMS related functions. More specifically, the MMS Proxy-Relay is responsible for:

1) receiving an MMS from a served UE and forwarding that to the MMS Proxy-Relay of the destination UE;
2) receiving an MMS from an originating MMS Proxy-Relay and forwarding this MMS or a notification of it to its served UE;
3) receiving a request for retrieval of an MMS from a served UE and delivering that MMS to the served UE;
4) providing the served UE with delivery status and read reports of served UE originated MM;
5) providing an MMS/Relay of another UE with delivery status and read reports of MMS received for the served UE.

7.5.2 LI at MMS Proxy-Relay

7.5.2.1 Architecture

The MMS Proxy-Relay shall have LI capabilities to generate the target UE's MMS related xIRI and xCC.

The IRI-POI present in the MMS Proxy-Relay detects the MMS related events, generates and delivers the related xIRI to the MDF2 over LI_X2. The MDF2 delivers the IRI messages to the LEMF over LI_HI2.

When interception of communication contents is required, the CC-POI present in the MMS Proxy-Relay generates the xCC from the MMS messages and delivers the xCC (that includes the correlation number and the target identity) to the MDF3. The MDF3 delivers the CC to the LEMF over LI_HI3.

7.5.2.2 Target Identities

The LIPF provisions the intercept related information associated with the following target identities to the IRI-POI/CC-POI present in the MMS Proxy-Relay:

- Email Address.
- GPSI.
- IMPI.
- IMPU.
- IMSI.
- SUPI.

The interception performed on the above identities are mutually independent, even though, an xIRI may contain the information about the other identities when available. The IRI-POI and CC-POI present in the MMS Proxy-Relay shall also support interception of non-local identities in any of the IMPU formats (SIP URI, TEL URI as well as the E.164 number in a SIP URI or TEL URI), GPSI formats (E.164 number, external identifier) and email address.

7.5.2.3 IRI Events

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

- An MMS message is sent by the target or sent to the target.

7.5.2.4 Common IRI parameters

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

- Target identity.
- Time stamp.
- Correlation information (when xCC is also reported).
- MMS related information.

7.5.2.5 Specific IRI parameters

The parameters in each xIRI are defined in TS 33.128 [15].

7.5.2.6 CC

The MMS xCC is generated when the CC-POI in the MMS Proxy-Relay detects that CC related to an MMS message is either received from the target, sent to the target, or stored on behalf of the target.

7.5.2.7 Network Topologies

LI at the MMS Proxy-Relay is only applicable at the HPLMN.

7.6 PTC service

7.6.1 General

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

The following servers support PTC architecture:

- MCPTT servers (Including Common services core as defined in 3GPP TS 23.280 [24]).

- PoC servers (Including Shared XDMS as defined in OMA-AD-PoC-V2_1-20110802-A [25]).

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

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

7.6.2 Target identities

A provisioned target identity can be the following:

- MCPTT ID.
- IMEI.
- SIP URI.
- TEL URI.

The interception performed on the above identities are mutually independent, even though, an xIRI may contain the information about the other identities when available.

7.6.3 IRI events

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

- PTC service registration.
- PTC serving system.
- PTC session initiation.
- PTC session abandon.
- PTC session start.
- PTC session end.
- PTC start of interception.
- PTC pre-established Session.
- PTC instant personal alert.
- PTC party join.
- PTC party drop.
- PTC party hold.
- PTC party retrieve.
- PTC media modification.
- PTC group advertisement.
- PTC floor control.
- PTC target presence.
- PTC associate presence.
- PTC list management.
- PTC access policy.

- PTC media type notification.
- PTC encryption message.

The events above trigger the transmission of information from the IRI-POI to the MDF2.

7.6.4 Common IRI parameters

Each xIRI shall include at the minimum the following information:

- Target identity.
- Time stamp.
- Correlation information.
- Location information (if required and available).
- PTC related information (e.g., PTC group ID, PTC party).
- Encryption parameters (if required and available).
- Direction (floor control source or destination port).

7.6.5 Specific IRI parameters

The parameters in each xIRI are defined in TS 33.128 [15].

7.6.6 Common CC parameters

In addition to the intercepted content of communications, the following information needs to be transferred from the CC-POI to the MDF3 in order to allow the MDF3 to perform its functionality:

- Target identity.
- Correlation information.
- Time stamp.
- Identity of source of media (communications content) for group call.

7.6.7 Specific CC parameters

The parameters in xCC are defined in TS 33.128 [15].

7.6.8 Network topologies

The PTC server resides in the home network and shall provide IRI-POI and CC-POI functionality.

7.7 Identity Caching Function

7.7.1 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.

7.7.2 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.

7.7.3 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.

7.7.4 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.

8 LI security and deployment considerations

8.1 Introduction

The most sensitive information in the LI system is the target list. This is the list of all the subjects in the network currently under surveillance, whether active, suspended or in any other state. The security measures used by the carrier to prevent unauthorized access to this list is not subject to standardization, but the architectural choices made in the design of the LI system do impact the security of the target list directly.

Since completeness of the interception product is a legal requirement in most jurisdictions, the LI system shall ensure that no events that are lawfully authorized for interception are missed (or collected in error). To ensure that no events are missed there are two architectural alternatives.

8.2 Architectural alternatives

8.2.1 Full target list at every POI node

A carrier may choose to deploy the full target list at all POIs, such that when a UE arrives in the network and commences registration, the POI is fully armed and in position to recognize if the target identifier is in the target list. The choice to push the full list to every node is the simplest, and arguably the riskiest, since the compromise of any node will leak the complete target list.

8.2.2 Full target list only in LICF

A Communication Service Provider (CSP) may choose to selectively distribute specific target identifiers to specific POIs, rather than distributing the full target list to all POIs. This choice introduces a race condition. When the UE appears, the POI shall query the ADMF/LICF to find out if the user identifier is part of the target list. As the registration sequence progresses, the NF POI is waiting for a response from the ADMF/LICF. When the reply arrives, the POI can take action if the reply is positive. If the reply is negative, the POI's involvement ends.

If the reply is positive, depending on how long the POI-(ADMF/LICF)-POI round trip for the query/reply took, it is possible that some reportable events are missed. To mitigate this there are two further alternatives:

1) the carrier may choose to delay completion of the registration for all users for the time it takes the ADMF/LICF to answer, thus inducing a registration delay in all registrations, whether the user is a target or not, or
2) the carrier may choose to cache the reportable registration events while the POI-(ADMF/LICF)-POI query is running, and either report them if the answer is positive, or delete them if the answer is negative.

These are choices at the discretion of the CSP, but the trade-off cannot be avoided.

8.2.3 Provisioning for registered users

When a new target is provisioned in the LI system, after the target is already registered in the CSP network, the CSP will be faced with the race condition consequences of the implementation choice made as described in clauses 8.2.1 and 8.2.2. The ADMF has a choice to either wholesale pre-arm every POI with the new target (and expect every POI to immediately start interception on the new target, as in clause 8.2.1), or, the ADMF can poll every serving UDM POI for all target UEs, and arm the associated POI (and start interception, as in clause 8.1.2) *only* if a target UE is discovered to be served by that particular NF. The second approach would take comparatively longer and would be expected to miss more of the on-going target interactions with the network than the first approach.

8.3 LI key management at ADMF

8.3.1 General

The ADMF is responsible for overall management of the LI system as defined in clause 5.3.2.4. The ADMF is responsible for creating and managing intermediate, client and root certificates used for both identity verification and establishing encrypted communications between LI components.

NOTE: The exact mechanism for installation of certificates in POIs, MDFs or other LI components (manual or automated) is outside the scope of the present document.

8.3.2 Key management

The ADMF shall implement an LI Certificate Authority (LI CA) which shall be used as the issuing CA for all LI components.

By default, the LI CA shall be a sub-CA of the CSP root CA, and may issue intermediate certificates.

The LI CA shall be responsible for creating, maintaining and revoking all identity verification and encryption certificates and root keys used by LI components communicating on LI_X interfaces. It may also be responsible for issuing certificates and root keys for LI_HI interfaces if these are not issued by the LEA/LEMF.

For virtualised implementations, the LICF shall support automated certificate enrolment for POIs, TFs and MDFs. For non-virtualised deployments, support for automatic certificate enrolment is optional.

The LICF shall maintain a list of all valid LI components for which the LI CA has generated certificates. The LICF shall instruct the LI CA to revoke any certificate belonging to LI components that are removed from the system (e.g. de-instantiated).

The LI CA shall provide a single certificate for each LI component. The LI component shall generate individual session keys for each LI_X link.

8.4 Virtualised LI security

8.4.1 General

This clause provides requirements and deployment constraints relating to the virtualisation of LI in 3GPP networks.

8.4.2 NFVI and host requirements

NFVIs hosting LI functions defined in the present document, shall provide functionality for protecting sensitive functions as defined in ETSI GS NFV-SEC 012 [29] or equivalent specification.

8.4.3 Virtualised LI function implementation

LI functions as defined in the present document when virtualised shall include the use of one or more HMEEs as defined in ETSI GS NFV-SEC 012 [29] or equivalent specification, to protect as a minimum:

- LI target lists.
- Any LI dynamic selectors used internally within the NF to select target communications to be intercepted.
- Any cryptographic keys and LI_X1/LI_X2/LI_X3 end points.

During runtime, NFs containing LI functions should not share NFVI hosts with any other NF, VNF or VNFC.

During runtime, NFs containing LI functions shall not share NFVI hosts with any other NF, VNF or VNFC which does not contain other authorised LI functions.

The NF runtime restriction requirements do not prevent hosts being used for different NFs over the lifetime of the NFVI, following termination of the previous VNF instances. However, both where hosts are newly allocated for LI use and when subsequently released, host memory and storage secure erase procedures as defined in ETSI GS NFV-SEC 012 [29] or equivalent specification shall be used.

8.4.4 Container based deployments

Where containers are used for implementing LI functionality, and when images corresponding to those containers are required to be stored at runtime in a system wide container cache, the LI Controller shall ensure that each time the container image is retrieved from the cache, the integrity of the image is validated. In addition, when the image is no longer required by a live running Network Function, the image is erased from the cache.

8.5 Points of Interception

CSPs use a wide range of 3GPP NFs to provide services to users. In order to intercept a service, POIs are associated with specific NFs, as depicted in Figure 8.5-1. The manner the POI obtains the required information from the NF depends on the service and can range from something as simple as a copy-and-forward mechanism, to sophisticated

isolation and filtering. The POI may be embedded in the NF or external to the NF, connected to its interfaces. The choice of one, the other, or both approaches is service specific.

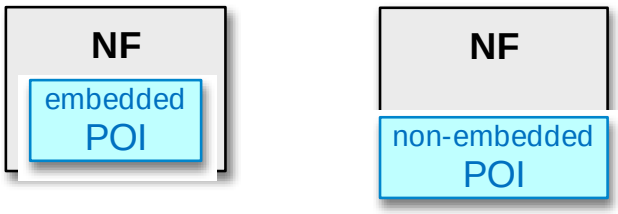

Figure 8.5-1: Embedded vs. external POIs

In figures that follow the POI will be depicted straddling the edge of the NF to simultaneously indicate both approaches.

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

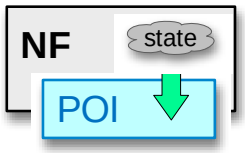

Figure 8.5-2: POI state capture

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

The same requirements apply to TFs.

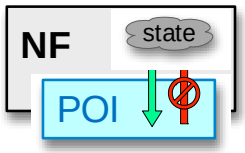

Figure 8.5-3: POI state capture security

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

8.6 Deployment considerations

8.6.1 General

This clause provides deployment considerations for Lawful Interception.

8.6.2 CC-PAG

This clause introduces CC-PAG (CC-POI Aggregator) as an architectural extension that is located between the MDF3 and CC-POI. The CC-PAG performs the function of aggregating the xCC from different CC-POIs towards the MDF3 and is shown in Figure 8.6-1.

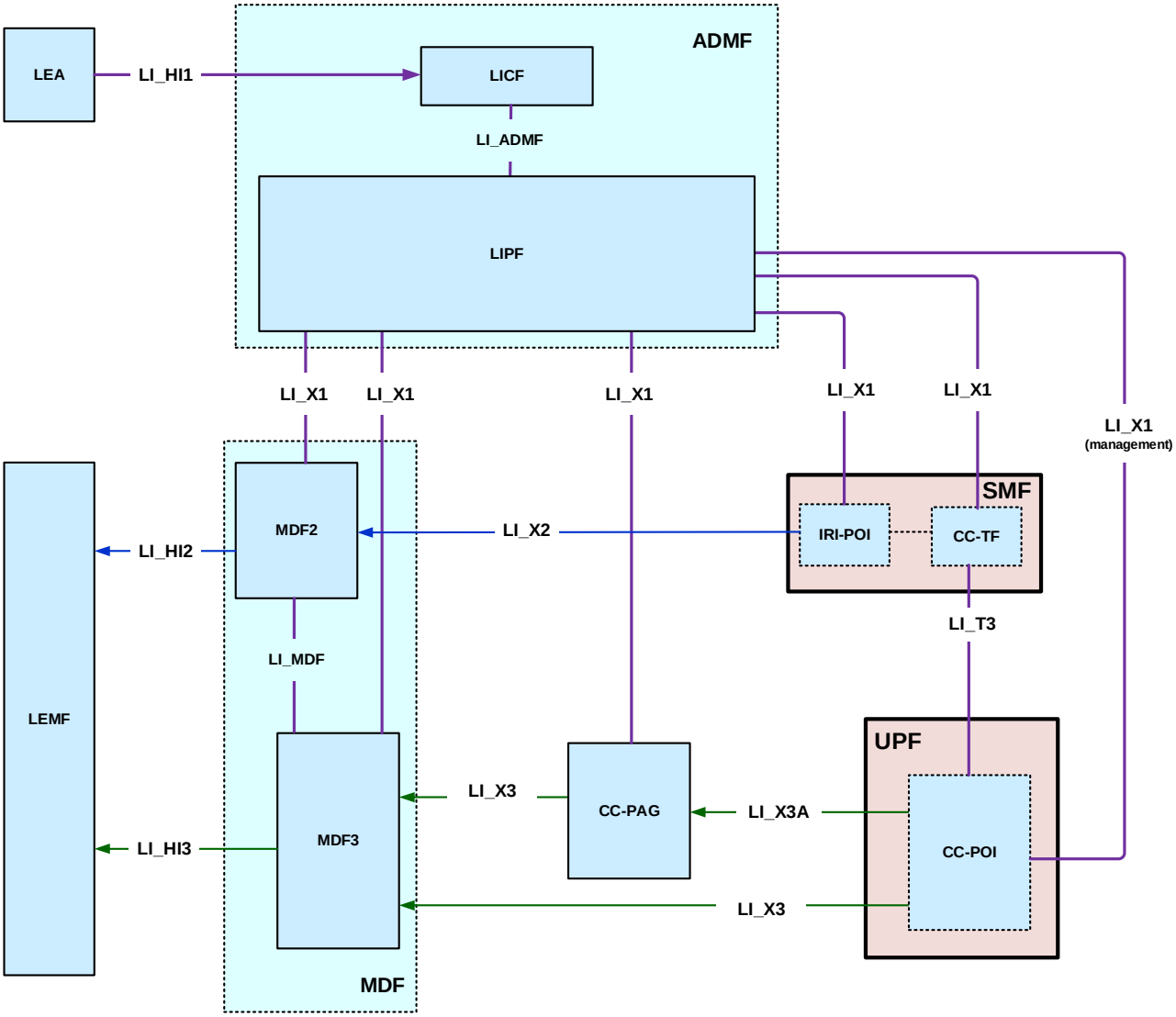

Figure 8.6-1: LI architecture showing CC-PAG.

NOTE: The IRI-POI and CC-TF represented in figure 8.6-1 are logical functions and require correlation information be shared between them; they may be handled by the same process within the SMF.

The CC-PAG is an optional LI function and may be deployed in networks that need aggregation of xCC from potentially large number of different CC-POIs towards the MDF3. The CC-PAG may be deployed closer to the UPFs, to reduce the impact of latencies, packet drops, and buffering on UPFs for lawful interception of highspeed user plane traffic. The system resources such as hardware interfaces, CPUs and memory for the CC-PAG node may be tuned to balance the forwarding/reception capabilities of CC-POI and MDF3.

As shown in figure 8.6-1, the CC-POI is triggered by the CC-TF to deliver the xCC (on a per flow basis) to the CC-PAG (via LI_X3A interface) or to the MDF3 (via LI_X3 interface as described in clause 6.2.3).

In the option where CC-PAG is involved, the LIPF configures the CC-PAG with the appropriate MDF3 address. The CC-PAG address is provided to the CC-POI using one of the two methods:

1) pre-provisioned (e.g. by LIPF over LI_X0 interface) while instructed to use the pre-provisioned address over LI_X1;
2) as a part of the CC intercept trigger by the CC-TF which in turn is provisioned by the LIPF over LI_X1.

The CC-PAG aggregates the xCC received from different CC-POIs before forwarding the same to the MDF3. The xCC is not modified. The LI_X3A interface is the same as LI_X3 interface on the application level but may be used with other transport protocol options as described in ETSI TS 103 221-2 [16].

Annex A (informative): 5G LI network topology views

A.1 Non-roaming scenario

A.1.1 General

In a non-roaming scenario, the POIs present in the following NFs provide the LI functions:

- AMF.
- UDM.
- SMF.
- UPF.
- SMSF.

For the interception of PDU sessions, the EPC CUPS LI model is not extended to 5G where SMF and UPF are involved in delivering the xIRI and xCC associated with the PDU sessions.

NOTE: The above list of NFs that provide the POI functions may have to be expanded once a deployment scenario for such a case is defined in the normative part of the present document.

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

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

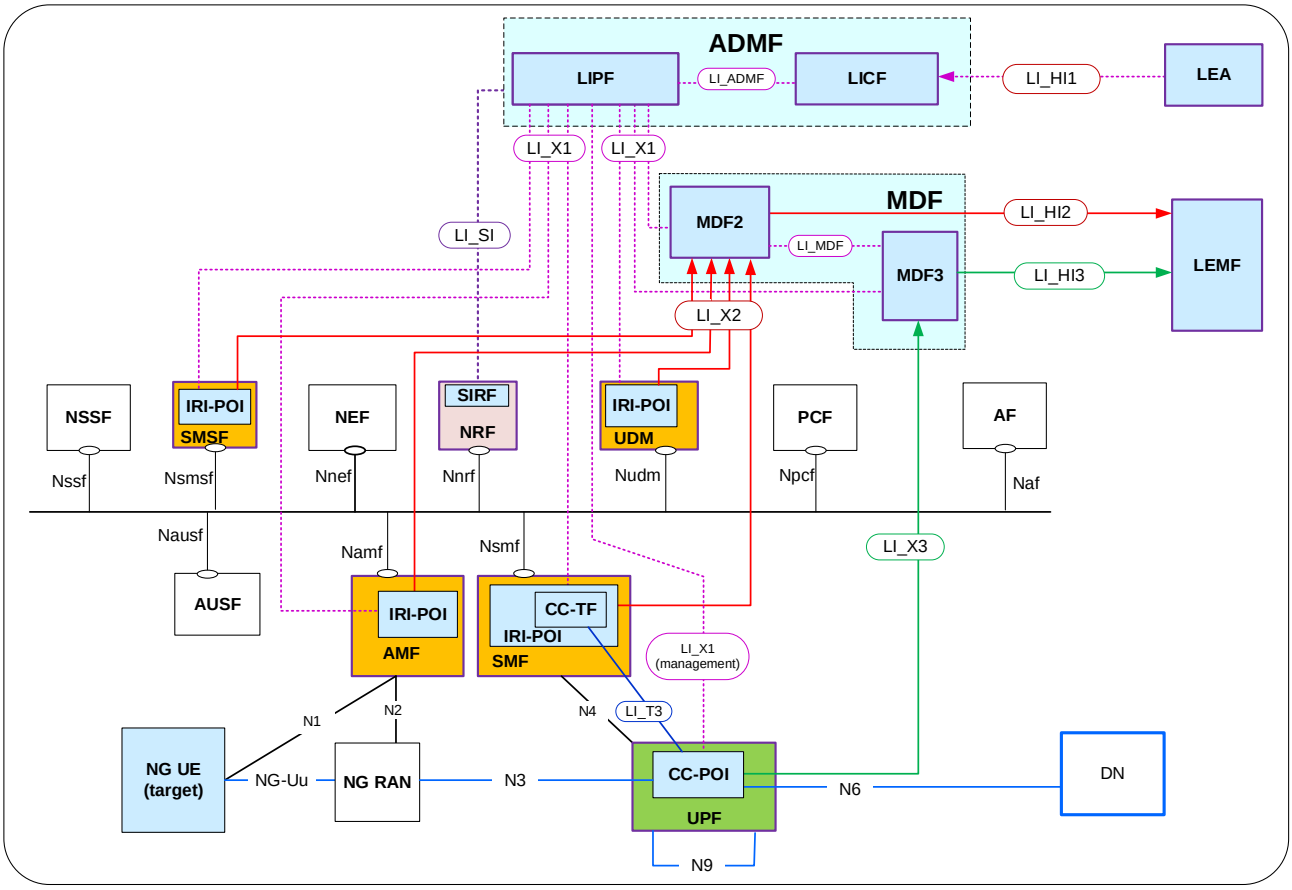

Figure A.1-1: Network topology showing LI for 5G (service-based representation) with point-to-point LI system

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

The IRI-POIs present in the AMF, UDM SMF and SMSF deliver the xIRI to the MDF2 and CC-POI present in the UPF delivers the xCC to the MDF3. The MDF3 address to CC-POI present in UPF is provided by the CC-TF present in the SMF over LI_T3 reference point.

The LIPF present in the ADMF provisions the IRI-POIs present in the NFs with the intercept related data. The LI_X1 interfaces between the LIPF and the UPF is to monitor the user plane data.

A.2 Interworking with EPC/E-UTRAN

A.2.1 General

In EPC/E-UTRAN, the NFs that provide the POI functions are:

- MME.
- SGW.
- PGW (optional).
- HSS.

In a 5GS, the NFs that provide the POI functions are:

- AMF.

- SMF/UPF.
- UDM.
- SMSF.

In an interworking scenario between the EPC and the 5GS, the AMF in 5GS and MME in EPC provide the IRI-POI functions for the related attach/registration related aspects. When the network topology includes SMF + PGW-C and UPF + PGW-U as the interworking NFs, it is recommended that these provide the POI functions for the PDU sessions as the target communication traffic coming from either of the two interworking networks pass through these NFs. In that case, the interception at the SGW and UPF (if present between the NG-RAN and the UPF + PGW-U) is not required unless the condition specified in NOTE 1 in clause A.2.1 applies.

In a non-roaming scenario, the IRI-POI present in the HSS + UDM also provide the LI functions. The IRI-POI present in the SMSF provides the LI functions for the SMS-related IRI events.

A.2.2 Topology view for a non-roaming scenario

The overall network configuration for interworking between EPC-EUTRAN and 5GS in non-roaming scenario with the LI aspects is shown in figure A.2-1.

The 5G core system is shown using the service-based representation (as shown in TS 23.501 [2]) with the use of point-to-point LI system.

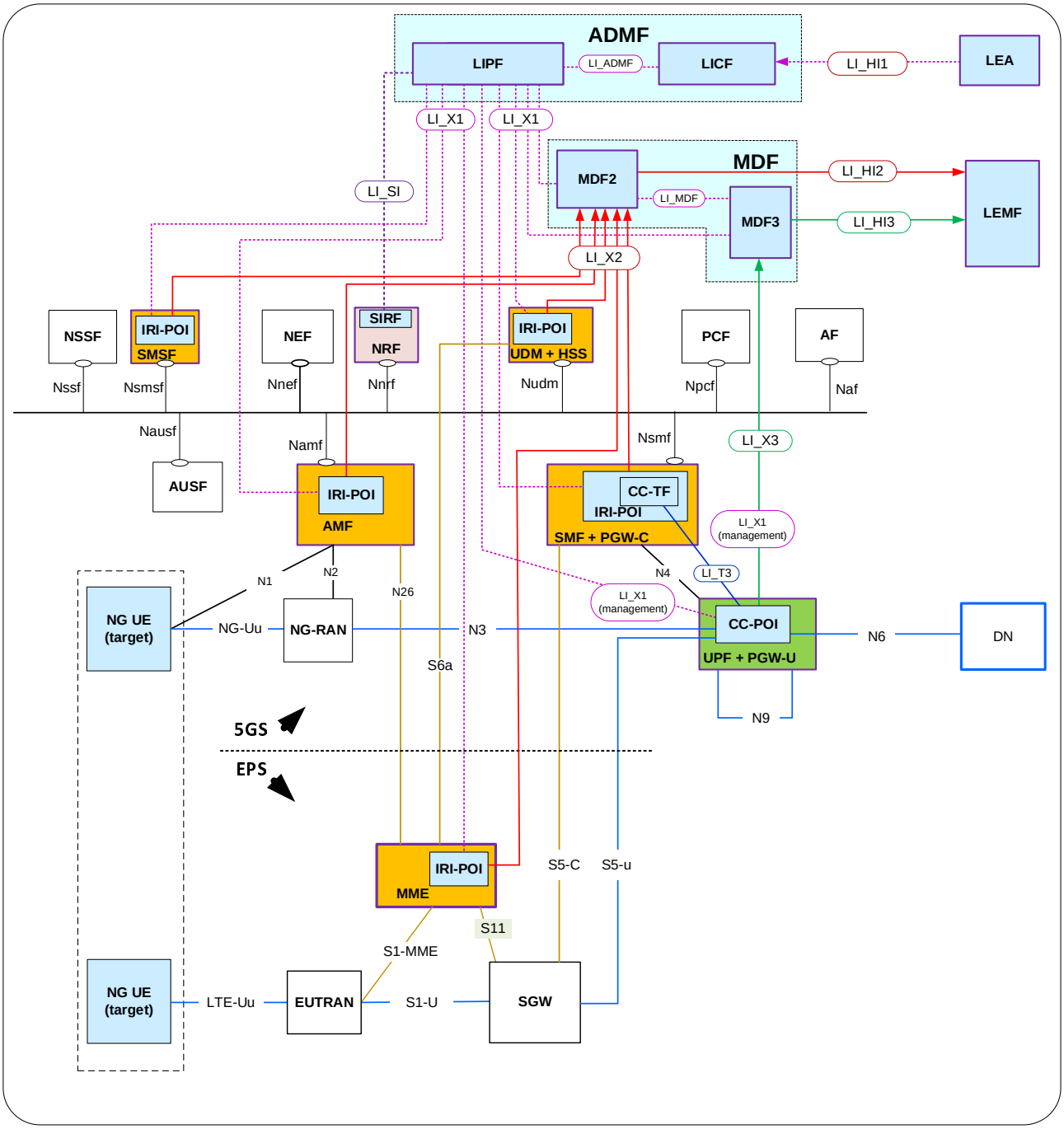

Figure A.2-1: Network topology showing LI for interworking with EPC/E-UTRAN

Figure A.2-1 shows the network topology of 5G system in a service-based representation, however, all the LI-related interfaces remain to be point-to-point.

The IRI-POIs present in the AMF, MME, UDM, SMSF and SMF + PGW-C deliver the xIRI to the MDF2 and CC-POI present in the UPF + PGW-U delivers the xCC to the MDF3. The MDF3 address to CC-POI present in UPF + PGW-U is provided by the CC-TF present in the SMF over LI_T3 reference point.

The LIPF present in the ADMF provisions the IRI-POIs present in the NFs with the intercept related data. The LI_X1 interfaces between the LIPF and the UPF + PGW-U is to monitor the user plane data.

NOTE: The TS 23.501 [2] notes that there can another UPF between the NG-RAN and PGW-U + UPF. In that case, the other UPF may also provide the CC-POI functions for any user plane packets that do not reach the PGW-U + UPF.

A.3 Multiple DN connections in a PDU session

A.3.1 General

According to 3GPP TS 23.501 [2], a PDU session can involve multiple UPFs, but regardless of how many UPFs are involved in the session, the session only connects to a single DN through one or more DN connections (i.e. connections to the same DN).

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

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

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

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

A.3.2 Topology view for a non-roaming scenario

The overall network configurations to illustrate the LI with multiple DN connections (to the same DN) in a PDU session is illustrated in figure A.3-1 and A.3-2.

The 5G core system is shown using the service-based representation (as shown in TS 23.501 [2]) with the use of point-to-point LI system.

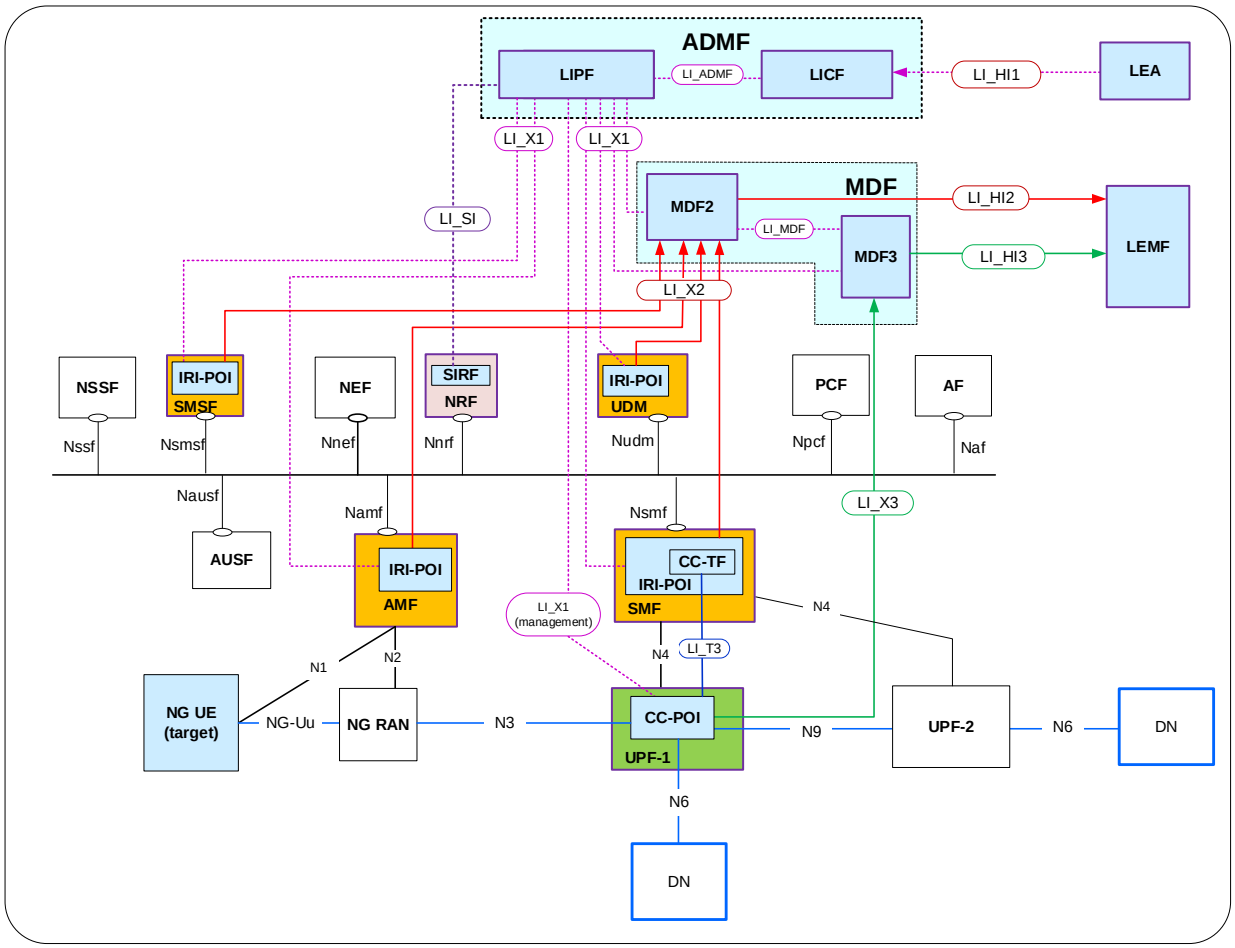

Figure A.3-1: Network topology showing CC-POI at one UPF

The IRI-POIs present in the AMF, MME, UDM, SMSF and SMF deliver the xIRI to the MDF2 and CC-POI present in the branching UPF (shown as UPF-1) on the common path to both DN connections delivers the xCC to the MDF3. The MDF3 address to CC-POI present in UPF-1 is provided by the CC-TF present in the SMF over LI_T3 reference point. In this view, all user plane packets pass through UPF-1.

The LIPF present in the ADMF provisions the IRI-POIs present in the NFs with the intercept related data. The LI_X1 interfaces between the LIPF and the UPF is to monitor the user plane data.

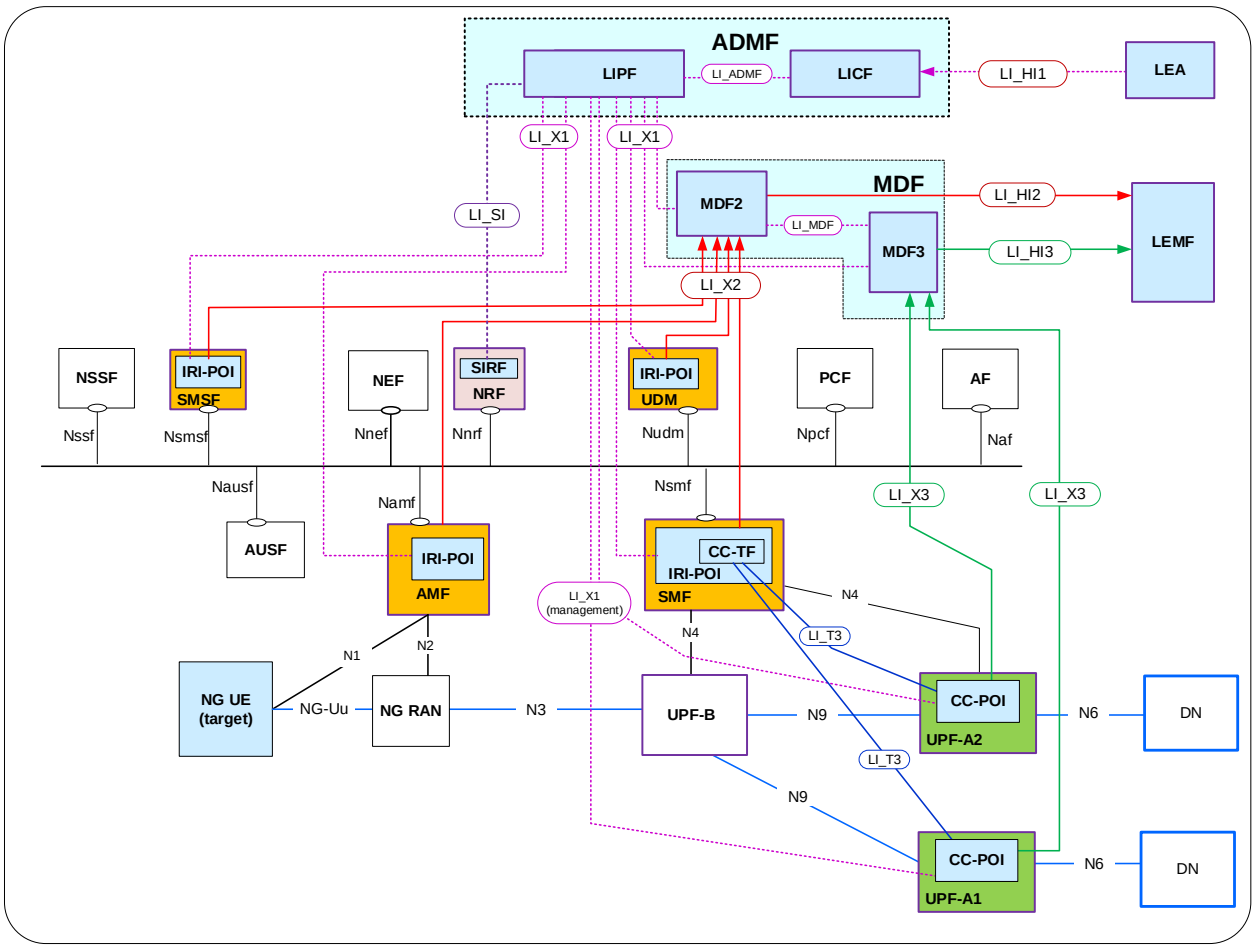

Figure A.3-2: Network topology showing CC-POI at two UPFs

The IRI-POIs present in the AMF, MME, UDM, SMSF and SMF deliver the xIRI to the MDF2. In this example, there is a branching UPF (UPF-B), an anchor UPF for the DN (UPF-A1) and another anchor UPF for the same DN (UPF-A2). The second approach (i.e. CC interception at the anchor UPFs) mentioned in A.3.1 is used to provide the CC interception. The UPF-A1 delivers the xCC generated from the user plane packets that flow from UE to the DN via UPF-A1 to the MDF3. The CC-POI present in the UPF-A2 delivers the xCC generated from the user plane packets that flow UE to the DN via UPF-A2 to the MDF3. The MDF3 address in the CC-POIs present in UPF-1 and UPF-2 are provided by the CC-TF present in the SMF over LI_T3 reference point.

The LIPF present in the ADMF provisions the IRI-POIs present in the NFs with the intercept related data. The LI_X1 interfaces between the LIPF and the UPFs are to monitor the user plane data.

NOTE: In some cases, the branching UPF may be merged with one of the anchor UPFs. In this case care needs to be taken to avoid duplication of xCC e.g. by intercepting only on the external N6 interface of each anchor UPF.

A.4 Non-3GPP access in a non-roaming scenario

A.4.1 General

When the target UE is connected to the 5G core network via non-3GPP access, the POIs present in the following NFs of the PLMN where the N3IWF resides provide the LI functions:

- AMF.
- SMF.
- UPF.
- SMSF.

When the PLMN that has the N3IWF is the HPLMN, as illustrated in clause A.1, the IRI-POI present in the UDM also provide the LI functions.

When the PLMN that has N3IWF is different from the PLMN that provides the 3GPP access to the target UE, two different AMFs are involved in handling the target UE's registration accepts (this is not illustrated in this clause). In this case, depending on the operator policy, the SMSF present in either of the two networks may perform the routing of SMS messages to and from the target UE.

The PLMN that provides the 3GPP access can be a VPLMN and PLMN where the N3IWF resides can be the HPLMN. In this case, the AMF in the HPLMN provides the IRI-POI functions for non-3GPP access related registration events when the target UE is roaming. The SMSF present in the HPLMN may have to provide the IRI-POI functions for the SMS related messages routed via non-3GPP access network.

A.4.2 Topology view

The overall network configuration for non-3GPP access in a non-roaming scenario with the LI aspects is shown in figure A.4-1. In this view, the target UE is not connected to a 3GPP access network.

The 5G core system is shown using the service-based representation (as shown in TS 23.501 [2]) with the use of point-to-point LI system.

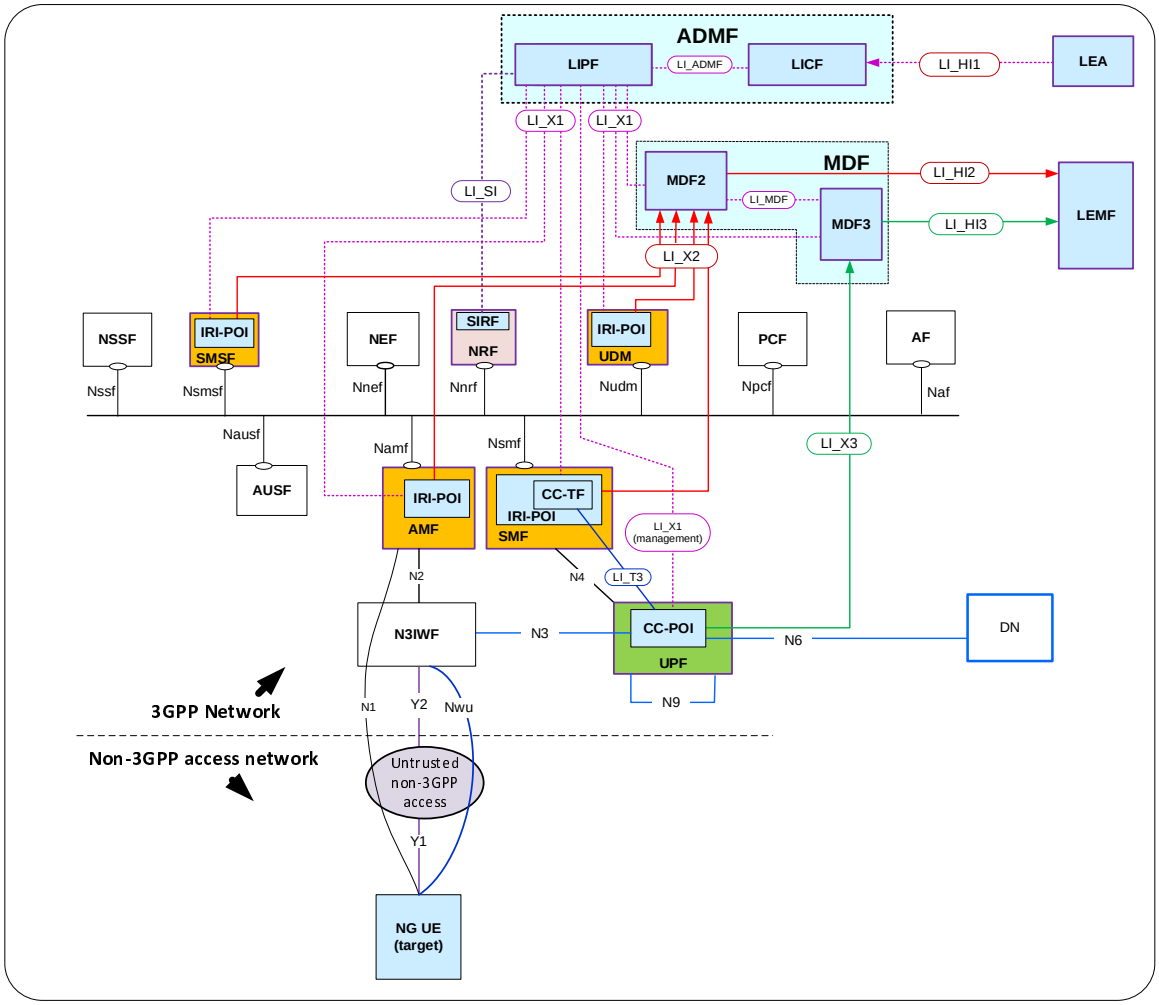

Figure A.4-1: Network topology showing LI for non-3GPP access to 5G

Figure A.4-1 shows the network topology of 5G system in a service-based representation, however, all the LI-related interfaces remain to be point-to-point.

The IRI-POIs present in the AMF, UDM, SMSF and SMF deliver the xIRI to the MDF2 and CC-POI present in the UPF delivers the xCC to the MDF3. The MDF3 address to CC-POI present in UPF is provided by the CC-TF present in the SMF over LI_T3 reference point.

The LIPF present in the ADMF provisions the IRI-POIs present in the NFs with the intercept related data. The LI_X1 interfaces between the LIPF and the UPF is to monitor the user plane data.

Annex B (normative): ADMF functionality

The Administration Function (ADMF) provides the CSP's administrative and management functions for the LI capability.

The ADMF’s primary roles and responsibilities include:

- The logical point of contact from the LEA to the CSP via LI_HI1 for Lawfully authorised requests (e.g. warrant).
- Maintaining the CSP / LEA mutually agreed unique Lawful Interception IDentifier (LIID) for the warrant which is used for all corresponding LI_HI2, LI_HI3, and LI_HI4 communications for warrant correlation.
- CSP administration and local management of the warrant including start/stop times, filter criteria, LEA policy toggles, etc.
- Deriving internal information (ID mappings, potential POIs, etc.) from the warrant.
- For virtualised instances, verifying the authenticity/integrity of CSP LI functions (e.g. LI function's software image) prior to instantiation, see e.g. ETSI NFV-SEC 011 [10] or equivalent.
- When required, providing keys to newly instantiated LI functions to enable decryption of LI specific software.
- LI functions physical location policy control ensuring LI functions are within the legal location policy of the warrant.
- LI Certificate Authority (LI CA, sub-CA of the CSP root CA) for issuing certificates to LI functions as part of their LI provisioning via LI_X0 interface, see clause 5.6.3.2.
- Provisioning of all required and valid LI functions instantiated by the CSP network.
- Maintaining the master list of all authorised and provisioned LI functions.
- Managing the termination of LI instances across all impacted LI functions when the warrant expires or the LEA specifically requests termination of a LI instance.
- Certificate revoking when the LI function is terminated or the LI function is de-instantiated.
- Maintaining the status of the warrant execution within the CSP (e.g. accepted, pending/provisioning, active, suspended, de-provisioned, etc.).
- As agreed between the LEA and CSP, reporting warrant execution status changes to the LEA as well as responds to warrant audit requests from the LEA.
- Keeping records of the CSP's management of LI related activities (e.g. log files).

Refer to clause 5.4 LI interfaces, and figures 5.4-1 and 5.6-1 for details on specific interfaces between the ADMF and other network functions.

Annex C (informative): LEA initiated suspend and resume

This annex presents a means within current ETSI and 3GPP specifications to support the temporary suspension (suspend) and subsequent resuming (resume) of a Lawful Intercept. Temporary suspension of LI is either directly initiated by the LEA or automatically initiated based on predefined criteria/policy between the LEA and CSP as part of the warrant. This clause only addresses the case of LEA initiated temporary suspension of the delivery of LI product to the LEA.

The underlying baseline is that a Lawful Intercept has been fully authorised and established between the LEA and the CSP via LI_HI with an agreed LIID to map the warrant to the CSP provided LI product via LI_HI2, LI_HI3 and LI_HI4.

The LEA may request that this active LI instance be temporarily suspended. This means, at a minimum, that the CSP no longer delivers (or buffers) LI product to the LEA.

LEA initiated LI suspension may involve the following steps:

- The LEA, via LI_HI1, sends an Update Request, referencing the intercept, with the DesiredStatus of Suspended; reference ETSI TS 103 120 [7].
- The ADMF, via LI_X1, deactivates/deprovisions the required LI Functions, reference ETSI TS 103 221-1 [8]. These LI Functions then locally fully delete the active intercept as required and hence stops any subsequent LI_HI2/3 delivery.
- The ADMF should maintain all the intercept warrant information of the original intercept, with the status advanced to Suspended.
- The MDFs for which the intercept instance has been de-activated send an LI_HI4 deactivation notification to the LEMF.
- The ADMF sends an Update Response message to the LEA, via LI_HI1, with a status of Suspended.

To resume the LI product delivery, this may involve the following steps:

- The LEA sends the CSP, via LI_H1, an Update Request, referencing the original intercept, with the DesiredStatus of Active. This is equivalent to the initial LI activation but without having to repeat all the warrant information in the original intercept request, and the existing LIID is maintained. Sessions that were active before the intercept suspension that are still active when resumed, or new sessions initiated while the intercept is resumed, are handled as per mid-call intercept activation.
- The ADMF, via LI_X1, re-provisions the de-activated LI Functions just as for a new intercept to re-instantiate the intercept.

  NOTE: This implies all LI Product deliveries will restart just as for a new intercept; e.g. PDU sequence numbers will restart at zero, etc.

- The re-provisioned MDFs send an LI_HI4 activation notification to the LEMF.
- The ADMF sends an Update Response message to the LEA, via LI_HI1, with a status of Active.

If the intercept (warrant) timespan expires or the LEA directly requests intercept deactivation while the intercept is in a suspended state, all remaining LI Functions are deactivated/deprovisioned and the rest of LI instance is taken down as per usual warrant deactivation.

Annex Z (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2018-12	SA#82	SP-180991				Release 15 draft Approved at TSG SA#82	15.0.0
2019-03	SA#83	SP-190042	0001	1	F	LI Support for VoNR in R15	15.1.0
2019-03	SA#83	SP-190042	0003	1	F	Virtualised EPC Clarification	15.1.0
2019-03	SA#83	SP-190042	0006	-	F	Non-3GPP Access IP Address	15.1.0
2019-06	SA#84	SP-190343	0014	1	B	SecondaryCellGroupPSCell Reporting	15.2.0
2019-06	SA#84	SP-190345	0015	1	F	Missing references	15.2.0
2019-06	SA#84	SP-190344	0010	1	F	Usage of LIID and other parameters	16.0.0
2019-06	SA#84	SP-190344	0011	1	B	Coverage of subscriber de-provisioning while under a warrant	16.0.0
2019-06	SA#84	SP-190346	0019	2	C	Introducing CC POI Aggregator for 5GC LI	16.0.0
2019-09	SA#85	SP-190635	0028	1	F	Minor corrections to TS 33.127	16.1.0
2019-09	SA#85	SP-190635	0029	1	F	Editorial fixes to pass consistency check	16.1.0
2019-09	SA#85	SP-190635	0030	1	F	Fix pic for CC POI Aggregator for 5GC LI	16.1.0
2019-09	SA#85	SP-190635	0032	2	C	Introductory clause for IMS from the pCR	16.1.0
2019-09	SA#85	SP-190635	0033	1	F	Additional text to the IMS clause	16.1.0
2019-09	SA#85	SP-190635	0034	1	B	Updated architecture figures	16.1.0
2019-09	SA#85	SP-190635	0035	1	B	IMS Architecture Figures	16.1.0
2019-09	SA#85	SP-190635	0036	1	F	Support for MMS	16.1.0
2019-09	SA#85	SP-190661	0038	1	A	Removal of notes on LI_X2 and LI_X3	16.1.0
2019-09	SA#85	SP-190662	0040	3	C	LI Virtualisation Procedures	16.1.0
2019-09	SA#85	SP-190662	0044	1	B	LI in VPLMN with home routed roaming scenario	16.1.0
2019-12	SA#86	SP-190985	0047	1	B	Porting LI for EPC into TS 33.127	16.2.0
2019-12	SA#86	SP-190985	0049	1	B	Support for PTC Stage 2	16.2.0
2019-12	SA#86	SP-190985	0056	1	D	Editorial name change for ETSI TS 103 221-x references	16.2.0
2020-03	SA#87	SP-200031	0057	1	F	LI in VPLMN with home routed roaming scenario – updates to the common part	16.3.0
2020-03	SA#87	SP-200031	0058	1	F	LI in VPLMN with home routed roaming scenario – S8HR LI	16.3.0
2020-03	SA#87	SP-200031	0059	1	F	LI in VPLMN with home routed roaming scenario – N9HR LI	16.3.0
2020-03	SA#87	SP-200031	0060	2	C	ADMF descriptive details	16.3.0
2020-03	SA#87	SP-200031	0061	2	B	Support of manual LI Suspend and Resume	16.3.0
2020-03	SA#87	SP-200030	0063	-	A	Correction of the MLP reference	16.3.0
2020-03	SA#87	SP-200031	0064	1	F	MMS Stage 2	16.3.0
2020-03	SA#87	SP-200031	0065	1	F	CC-PAG provisioning and deployment corrections	16.3.0
2020-07	SA#88-e	SP-200407	0069	-	F	Fixing the typos	16.4.0
2020-07	SA#88-e	SP-200407	0070	1	F	Clarifications on the NFs that provide POI/TF functions for conferencing	16.4.0
2020-07	SA#88-e	SP-200407	0072	2	C	Virtualisation details	16.4.0
2020-07	SA#88-e	SP-200407	0073	-	F	Fixing the incorrect internal references	16.4.0
2020-07	SA#88-e	SP-200407	0074	-	F	Clarification to the IMS clause for the legacy CC-POI functions	16.4.0
2020-09	SA#89-e	SP-200807	0076	-	F	Correction on LI_X3_LITE_M interface	16.5.0
2020-09	SA#89-e	SP-200807	0078	1	F	Porting of HSS LI stage 2 from TS 33.107 to TS 33.127	16.5.0
2020-09	SA#89-e	SP-200807	0079	1	F	Clarification on the LI architecture	16.5.0
2020-09	SA#89-e	SP-200807	0086	1	F	One PDU session connects to only one DN	16.5.0
2020-09	SA#89-e	SP-200807	0088	1	F	MA-PDU LI at the SMF	16.5.0
2020-09	SA#89-e	SP-200807	0089	1	F	Addition of DNAI to SA PDU Reporting	16.5.0
2020-09	SA#89-e	SP-200807	0090	1	F	MA-PDU LI requirements at the AMF	16.5.0
2020-09	SA#89-e	SP-200807	0091	1	F	Clarification of LMF and GMLC Event Reporting at the AMF	16.5.0
2020-12	SA#90-e	SP-200940	0092	-	F	Missing functional requirements on logging at ADMF	16.6.0
2020-12	SA#90-e	SP-200940	0094	1	C	ADMF LI Function Targeting	16.6.0
2020-12	SA#90-e	SP-200940	0095	1	F	Corrections to specify non-local ID as a target type rather than as target identifier	16.6.0
2020-12	SA#90-e	SP-200940	0096	1	B	Enhancement for Subscriber Record Change	16.6.0
2020-12	SA#90-e	SP-200940	0097	3	B	Identifier Association	16.6.0
2020-12	SA#90-e	SP-200940	0098	1	F	Corrections to the architecture for SMF/UPF	16.6.0
2020-12	SA#90-e	SP-200940	0099	-	F	Changes to the architecture in the EPC clause	16.6.0
2020-12	SA#90-e	SP-200940	0100	-	F	Changes to the architecture diagrams in the LALS clause	16.6.0
2021-03	SA#91-e	SP-210031	0102	2	F	GUTI allocation procedure reporting correction	16.7.0
2021-03	SA#91-e	SP-210031	0110	1	F	IMS LI: Alternate option has potentially missing IRI-POI for certain scenarios	16.7.0
2021-03	SA#91-e	SP-210031	0111	1	F	IMS LI: Independent default/alternate option for non-local ID targets	16.7.0
2021-03	SA#91-e	SP-210031	0112	1	F	IMS LI: Separate LI_X1 to CC-TF and IRI-POI when in the same NF	16.7.0

History

Document history		
V16.4.0	November 2020	Publication
V16.5.0	November 2020	Publication
V16.6.0	January 2021	Publication
V16.7.0	April 2021	Publication