ETSI TS 133 128 V15.0.0 (2019-04)

LTE;
5G;
Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
Security;
Protocol and procedures for Lawful Interception (LI);
Stage 3
(3GPP TS 33.128 version 15.0.0 Release 15)

Reference
DTS/TSGS-0333128vf00

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 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

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 describes protocols and procedures for Lawful Interception based on 3GPP specifications. These protocols and procedures cover both internal 3GPP interfaces (those required to intercept communications and manage interception within a 3GPP network) and external handover interfaces (those used for delivery of intercepted communications to Law Enforcement, or handling of warrants).

Lawful Interception needs to be done in accordance with the applicable national or regional laws and technical regulations. Such national laws and regulations define the extent to which capabilities in the present document are applicable in specific jurisdictions.

1 Scope

The present document specifies the protocols and procedures required to perform Lawful Interception within a 3GPP network. The present document addresses both internal interfaces used internally with a 3GPP network and external handover interfaces used to handover intercepted communications to law enforcement.

The present document describes the detailed targeting of communications in each point of interception within a 3GPP network and the information that a point of interception needs to be able to capture. Furthermore, the detailed data formats for both the internal and external interfaces are also defined.

National regulations determine the applicable set of information that needs to be handed over or excluded from handover to law enforcement for a given 3GPP operator service.

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 33.127: "Lawful Interception (LI) Architecture and Functions".

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

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

[8] ETSI TS 103 221-2: "Lawful Interception: Internal Network Interface X2/X3".

[9] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[10] ETSI TS 102 232-7: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services".

[11] 3GPP TS 33.501: "Security Architecture and Procedures for the 5G System".

[12] 3GPP TS 33.108: "3G security; Handover interface for Lawful Interception (LI)".

[13] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS)".

[14] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General Aspects".

[15] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane nodes".

[16] 3GPP TS 29.502: "5G System; Session Management Services; Stage 3".

[17] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[18] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[19] 3GPP TS 23.003: "Numbering, addressing and identification ".

[20] OMA-TS-MLP-V3-4-20150512-A: "Open Mobile Alliance; Mobile Location Protocol, Version 3.4".

[21] 3GPP TS 29.540: "5G System; SMS Services; Stage 3".

[22] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

[23] 3GPP TS 38.413: "NG Application Protocol (NGAP)".

[24] 3GPP TS 29.572: "Location Management Services; Stage 3".

[25] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[26] IETF RFC 815: "IP DATAGRAM REASSEMBLY ALGORITHMS".

[27] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[28] IETF RFC 793: "TRANSMISSION CONTROL PROTOCOL".

[29] IETF RFC 768: "User Datagram Protocol".

[30] IETF RFC 4340: "Datagram Congestion Control Protocol (DCCP)".

[31] IETF RFC 4960: "Stream Control Transmission Protocol".

[32] IANA (www.iana.org): Assigned Internet Protocol Numbers, "Protocol Numbers".

[33] IETF RFC 6437: "IPv6 Flow Label Specification".

[34] IETF RFC 791: "Internet Protocol".

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].

3.2 Symbols

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

<symbol> <Explanation>

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].

ADMF LI Administration Function
CC Content of Communication
CSP Communication Service Provider

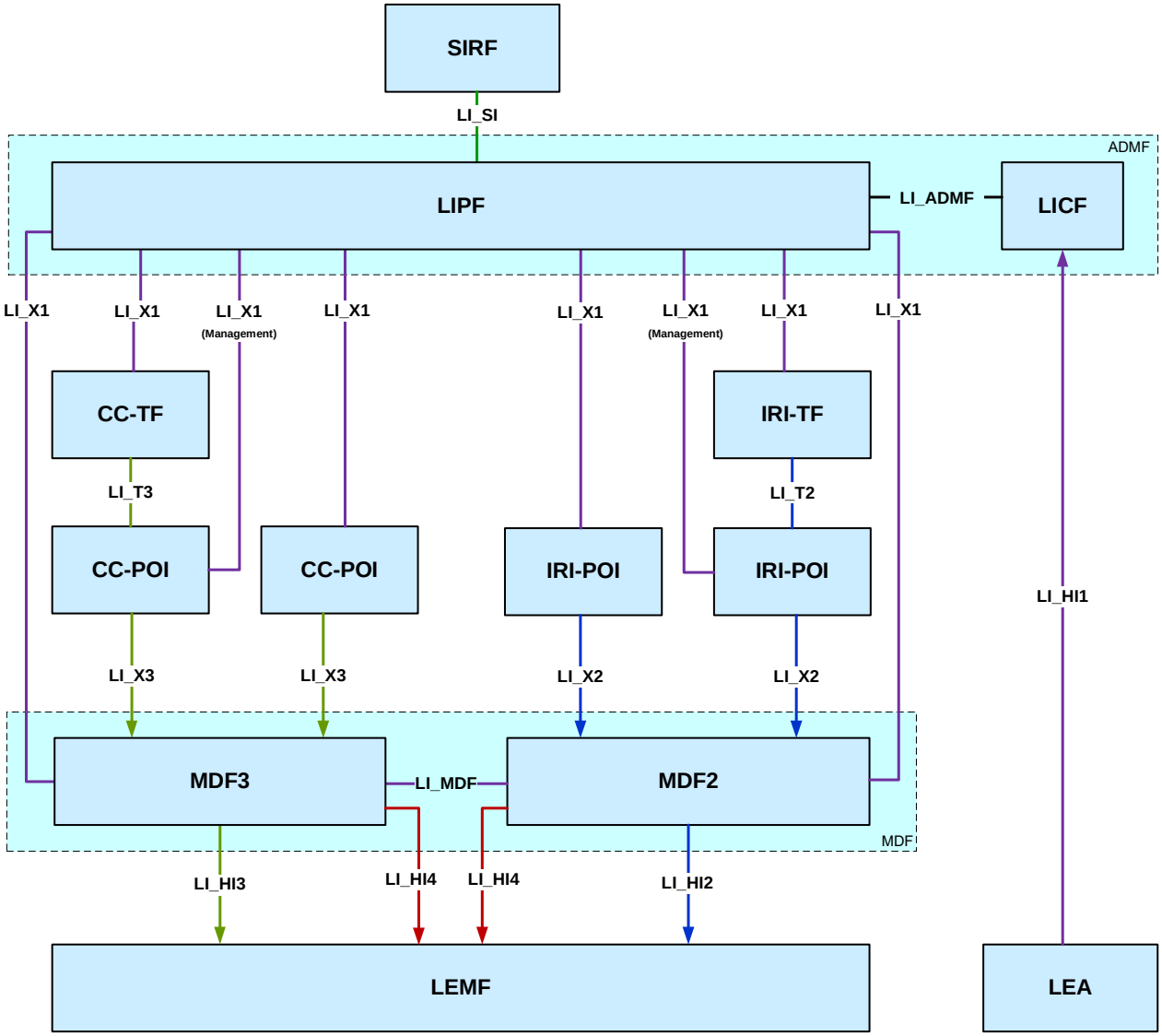
CUPS	Control and User Plane Separation
IRI	Intercept Related Information
LALS	Lawful Access Location Services
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LICF	Lawful Interception Control Function
LI_HI1	LI_Handover Interface 1
LI_HI2	LI_Handover Interface 2
LI_HI3	LI_Handover Interface 3
LI_HI4	LI_Handover Interface 4
LIPF	Lawful Interception Provisioning Function
LIR	Location Immediate Request
LI_SI	Lawful Interception System Information Interface
LI_X1	Lawful Interception Internal Interface 1
LI_X2	Lawful Interception Internal Interface 2
LI_X3	Lawful Interception Internal Interface 3
LTF	Location Triggering Function
MDF	Mediation and Delivery Function
MDF2	Mediation and Delivery Function 2
MDF3	Mediation and Delivery Function 3
NPLI	Network Provided Location Information
O&M	Operations and Management
POI	Point Of Interception
SIRF	System Information Retrieval Function
SOI	Start Of Interception
TF	Triggering Function
xCC	LI_X3 Communications Content.
xIRI	LI_X2 Intercept Related Information

4 General

4.1 Introduction

The present document provides details of the internal and external interfaces required for a network operator, access provider and/or service provider to provide the necessary information to a Law Enforcement Agency (LEA) required to meet LI requirements. LI requirements for 3GPP networks and services are given in TS 33.126 [3].

The high-level architecture that defines the necessary interfaces is specified in TS 33.127 [5]. The generic high-level architecture is as follows:



The specification of the interfaces is split into two parts:

- Internal interfaces used between an operator's network functions are described in clause 4.2.
- External interfaces used in communicating with a LEA are described in clause 4.3.

4.2 Basic principles for internal interfaces

This clause lists the internal interfaces shown in clause 4.1, indicates the protocol used to realise each interface, and gives a reference to the relevant clauses of the present document that specify how the protocol is to be used for the given interface.

Table 4.2-1: Internal interfaces and related protocols

Interface	Description	Protocol used to realise interface	Usage
LI_SI	Used to provide system information to the LIPF from the SIRF.	Out of scope of the present document.	
LI_X1	Used to configure and audit Directly-provisioned POIs, TFs and MDFs.	ETSI TS 103 221-1 [7].	See clause 5.2.2
LI_X1 (Management)	Used to audit Triggered POIs.	ETSI TS 103 221-1 [7].	See clause 5.2.3
LI_X2	Used to pass xIRI information from IRI-POIs to the MDF2.	ETSI TS 103 221-2 [8].	See clause 5.3.2
LI_X3	Used to pass xCC information from CC-POIs to the MDF3.	ETSI TS 103 221-2 [8].	See clause 5.3.3
LI_T2	Used to pass triggering information from the IRI-TF to a Triggered IRI-POI.	ETSI TS 103 221-1 [7].	See clause 5.2.4
LI_T3	Used to pass triggering information from a CC-TF to a Triggered CC-POI.	ETSI TS 103 221-1 [7].	See clause 5.2.4
LI_ADMF	Used to pass intercept provisioning information form the LICF to the LIPF.	Out of scope of the present document.	
LI_MDF	Used by MDF2 and MDF3 in interactions necessary to correctly generate CC and IRI from xCC and xIRI.	Out of scope of the present document.	

4.3 Basic principles for external handover interfaces

This clause lists the external handover interfaces shown in clause 4.1, indicates the protocol used to realise each interface, and gives a reference to the relevant clauses of the present document that specify how the protocol is to be used for the given interface.

Table 4.3-1: External handover interfaces and related protocols

Interface	Description	Protocol used to realise interface	Usage
LI_HI1	Used to send warrant and other interception request information from LEA to operator.	ETSI TS 103 120 [6] shall be supported Other methods (e.g. manual exchange) may be used depending on national regulatory requirements.	See section 5.4
LI_HI2	Used to send IRI from the MDF2 to the LEMF	ETSI TS 102 232-1 [9] and ETSI TS 102 232-7 [10] shall be supported	See section 5.5
LI_HI3	Used to send CC from the MDF3 to the LEMF	ETSI TS 102 232-1 [9] and ETSI TS 102 232-7 [10] shall be supported	See section 5.5
LI_HI4	Used to send LI notification information from MDF2/3 to LEMF	ETSI TS 102 232-1 [9] and ETSI TS 102 232-7 [10] shall be supported	See section 5.6

5 Transport and Communications Protocol

5.1 General

This clause describes the protocols used for each of the interfaces at a level which is agnostic of the subject service or network. Additional specific fields or behaviours are given in the relevant parts of clauses 6 and 7.

5.2 Protocols for LI_X1 and LI_T interfaces

5.2.1 General usage of ETSI TS 103 221-1

Functions having an LI_X1, LI_T2 or LI_T3 interface shall support the use of ETSI TS 103 221-1 [7] to realise the interface.

In the event of a conflict between ETSI TS 103 221-1 [7] and the present document, the terms of the present document shall apply.

The LIPF and MDF2/3 shall maintain a mapping between internal interception identifiers (XIDs) and external interception identifiers (LIIDs), as defined by TS 103 221-1 [7] clause 5.1.2. In case of multiple interceptions for a single target identifier, it is an implementation decision for the LIPF/TF whether multiple XIDs are used (i.e. a one-to-one mapping between XID and LIID is maintained) or whether the single XID is used and mapped to multiple LIIDs at the MDF2/3. Clauses 6 and 7 give further details for specific networks or services (e.g. minimum supported target identifier formats).

In the event that a request issued over the interface fails, or an error is reported, the LIPF should raise an alert in the appropriate LI Operations and Management (O&M) system. Further procedures (e.g. retrying a failed request) are left to CSP policy to define.

5.2.2 Usage for realising LI_X1

For the purposes of realising LI_X1 between the LIPF and a POI, MDF or TF, the LIPF plays the role of the “ADMF” as defined in ETSI TS 103 221-1 [7] reference model (clause 4.2), and the POI, MDF or TF plays the role of the “NE”.

5.2.3 Usage for realising LI_X1 (management)

For the purposes of realising LI_X1 between the LIPF and a triggered POI, the LIPF plays the role of the “ADMF” as defined in ETSI TS 103 221-1 [7] reference model (clause 4.2) , and the triggered POI plays the role of the “NE”.

5.2.4 Service scoping

5.2.4.1 General

The CSP shall support the following specified options on a per intercept (per LIID) basis, to ensure strict delivery of only the interception data that an LEA is authorised to receive. These options are not exclusive, i.e., none, one, or more than one item in any given category may be turned on for any given intercept (LIID).

5.2.4.2 CSP service type

- Voice.
- Data.
- Messaging (e.g. SMS/MMS).
- Push-to-Talk (including MCPTT).

5.2.4.3 Interception type

- IRI.
- CC.

5.2.4.4 Location

- Report location at the beginning and end of a session.
- Report location every time the network detects a change in target location (including location update with no physical change of location).
- LALS.

5.2.4.5 Roaming

- Stop interception for non HPLMN RAN.

5.2.5 Usage for realising LI_T2

For the purposes of realising LI_T2 between a TF and a Triggered POI, the TF plays the role of the “ADMF” as defined in the ETSI TS 103 221-1 [7] reference model (clause 4.2), and the triggered POI plays the role of the “NE”.

5.2.6 Usage for realising LI_T3

For the purposes of realising LI_T3 between a TF and a Triggered POI, the TF plays the role of the "ADMF" as defined in the ETSI TS 103 221-1 [7] reference model (clause 4.2), and the triggered POI plays the role of the "NE".

5.3 Protocols for LI_X2 and LI_X3

5.3.1 General usage of ETSI TS 103 221-2

Functions having an LI_X2 or LI_X3 interface shall support the use of ETSI TS 103 221-2 [8] to realise the interface.

In the event of a conflict between ETSI TS 103 221-2 [8] and the present document, the terms of the present document shall apply.

xIRI message and xCC data sent using ETSI TS 103 221-2 [8] shall contain the appropriate XID as received in the relevant LI_X1 provisioning message (or LI_T2/3 triggering message, as appropriate).

5.3.2 Usage for realising LI_X2

The POI sending xIRI messages over the LI_X2 interface shall set the PDU type field within the xIRI messages to "X2 PDU". (see ETSI TS 103 221-2 [8] clause 5.1).

The TLS transport profile (see ETSI TS 103 221-2 [8] clause 6) shall be supported and used by default.

Unless otherwise specified, xIRI messages shall include the timestamp and sequence number conditional attribute fields, with the timestamp value set to the time at which the event occurred.

5.3.3 Usage for realising LI_X3

The POI sending xCC data over the LI_X3 interface shall set the PDU type field in the xCC data to "X3 PDU".

(see ETSI TS 103 221-2 [8] clause 5.1).

NOTE: ETSI TS 103 221-2 [8] specifies in clause 6 a default profile which is mandatory to support, but allows further profiles to be defined. In scenarios where it may not be possible to achieve the necessary LI data rates based on the default profile, alternative profiles may be considered (e.g. based on UDP, multi path TCP or other protocols). Any alternative profile needs to ensure that LI reliability, security and completeness requirements as specified in TS 33.126 [3] are met.

5.4 Protocols for LI_HI1

5.4.1 General

Functions having an LI_HI1 interface shall support the use of ETSI TS 103 120 [6] to realise the interface.

In the event of a conflict between ETSI TS 103 120 [6] and the present document, the terms of the present document shall apply.

5.5 Protocols for LI_HI2 and LI_HI3

5.5.1 General

Functions having an LI_HI2 or LI_HI3 interface shall support the use of ETSI TS 102 232-1 [9] and ETSI TS 102 232-7 [10] to realise the interface.

In the event of a conflict between either specification and the present document, the terms of the present document shall apply.

5.5.2 Usage for realising LI_HI2

The IRI messages sent over LI_HI2 are structured as a header and a payload. The header contains general information like LIID, timestamp, correlation information (as for example defined in ETSI TS 102 232-1 [9]). The payload contains

intercept related information based on information that the MDF2 has received from sources in the network, such as the IRI-POI as described in clauses 6 and 7 of the present document. Details of the IRI messages can be found in Annex B of the present document. Messages defined as passing over the LI_HI2 interface shall be passed as the payload of the threeGPP33128DefinedIRI field (see TS ETSI 102 232 -7 [10] clause 15).

5.5.3 Usage for realising LI_HI3

The CC sent over LI_HI3 is structured as a header and a payload. The header contains general information like LIID, timestamp, correlation information (as for example defined in ETSI TS 102 232-1 [9]). The payload contains content of communication based on information that the MDF3 has received from sources in the network, such as the CC-POI as described in clauses 6 and 7 of the present document. Details of the CC data can be found in Annex A of the present document. CC data defined as passing over the LI_HI3 interface shall be passed as the payload of the threeGPP33128DefinedCC field (see ETSI TS 102 232-7 [10] clause 15).

NOTE: ETSI TS 102 232-1 [9] specifies in clause 6.4 a transport layer based on TCP. However, based on agreement between network operator and LEA, in scenarios where it may not be possible to achieve the necessary LI data rates based on the transport layer based on single TCP connection, alternative profiles may be considered (e.g. based on UDP, multi path TCP or other protocols). Any alternative profile needs to ensure that LI reliability, security and completeness requirements as specified in TS 33.126 [3] are met.

5.6 Protocols for LI_HI4

5.6.1 General

Functions having an LI_HI4 shall support the use of ETSI TS 102 232-1 [9] to realise the interface.

In the event of a conflict between ETSI TS 102 232-1 [9] and the present document, the terms of the present document shall apply.

5.6.2 Usage for realising LI_HI4

The LI Notification messages sent over LI_HI4 are structured as a header and a payload. The header contains general information like LIID, timestamp (as for example defined in ETSI TS 102 232-1 [9]). The payload contains the administrative information such as notification. Details of the LI Notification messages can be found in Annex B of the present document.

Where the LI_HI4 interface is present alongside an LI_HI2 interface or LI_HI3 interface, the LI Notification messages shall be transmitted along the same connection as the IRI messages or CC. Where ETSI TS 102 232-1 [9] is used for LI_HI2 or LI_HI3, messages defined as passing over the LI_HI4 interface shall be passed as the contents of the operatorLeaMessage field.

The MDF2/3 shall support generation LI Notification messages for at least the following events:

- Activation of an interception at the MDF2/3 via LI_X1.
- Modification of an interception at the MDF2/3 via LI_X1.
- Deletion of an interception at the MDF2/3 via LI_X1.

6 Network Layer Based Interception

6.1 Introduction

This clause describes any remaining fields, behaviours or details necessary to implement the required LI interfaces for specific 3GPP-defined network deployments which are not described in clauses 4 and 5.

6.2 5G

6.2.1 General

This clause describes the LI interfaces specific to LI for 5G networks.

6.2.2 LI at AMF

6.2.2.1 Provisioning over LI_X1

The IRI-POI present in the AMF is provisioned over LI_X1 by the LIPF using the X1 protocol as described in clause 5.2.2.

The POI in the AMF shall support the following target identifier formats in the ETSI TS 103 221-1 [7] messages (or equivalent if ETSI TS 103 221-1 [7] is not used):

- SUPI.
- PEI.
- GPSI.

6.2.2.2 Generation of xIRI over LI_X2

6.2.2.2.1 General

The IRI-POI present in the AMF shall send the xIRI messages over LI_X2 for each of the events described in the following clauses.

Unless otherwise specified, the LI_X2 “matched target identifier” conditional attribute shall be set to indicate what target identity was matched to generate the xIRI message (see ETSI TS 103 221-2 [8] clause 5.3.18).

6.2.2.2.2 Registration

The IRI-POI in the AMF shall generate an xIRI containing an AMFRegistration record when the IRI-POI present in the AMF detects that a UE matching one of the target identifiers provided via LI_X1 has successfully registered to the 5GS via 3GPP NG-RAN or non-3GPP access. Accordingly, the IRI-POI in the AMF generates the xIRI when one of the following events are detected:

- AMF sends a N1: REGISTRATION ACCEPT message to the target UE and the UE 5G Mobility Management (5GMM) state within the AMF is changed to 5GMM-REGISTERED.

Table 6.2.2-1: Payload for AMFRegistration record

Field name	Description	M/C/O
registrationType	Specifies the type of registration, see TS 24.501 [13] clause 9.11.3.7. This is derived from the information received from the UE in the REGISTRATION REQUEST message.	M
registrationResult	Specifies the result of registration, see TS 24.501 [13] clause 9.11.3.6.	M
slice	Provide, if available, one or more of the following: - allowed NSSAI (see TS 24.501 [13] clause 9.11.3.37). - configured NSSAI (see TS 24.501 [13] clause 9.11.3.37). - rejected NSSAI (see TS 24.501 [13] clause 9.11.3.46). This is derived from the information sent to the UE in the REGISTRATION ACCEPT message.	C
sUPI	SUPI associated with the registration (see clause 6.2.2.4).	M
sUCI	SUCI used in the registration.	C
pEI	PEI provided by the UE during the registration, if available.	C
gPSI	GPSI obtained in the registration, if available as part of the subscription profile.	C
gUTI	5G-GUTI provided as outcome of initial registration or used in other cases, see TS 24.501 [13] clause 5.5.1.2.2.	M
location	Location information determined by the network during the registration, if available.	C
non3GPPAccessEndpoint	UE's local IP address used to reach the N3IWF, if available. IP addresses are given as 4 octets (for IPv4) or 16 octets (for IPv6) with the most significant octet first (network byte order).	C

6.2.2.2.3 Deregistration

The IRI-POI in the AMF shall generate an xIRI containing an AMFDeregistration record when the IRI-POI present in the AMF detects that a UE matching one of the target identifiers provided via LI_X1 has deregistered from the 5GS. Accordingly, the IRI-POI in AMF generates the xIRI when one of the following events are detected:

- For network initiated de-registration, when the AMF receives the N1: DEREGISTRATION ACCEPT message from the target UE or when implicit deregistration timer expires; and in both cases the UE 5GMN state within the AMF is changed to 5GMM-DEREGISTERED.

- For UE initiated de-registration, when the AMF sends the N1: DEREGISTRATION ACCEPT message to the target UE or when the AMF receives the N1: DEREGISTRATION REQUEST message from the target UE with deregistration type value of “switch off”; and in both cases the UE 5GMN state within the AMF is changed to 5GMM-DEREGISTERED.

Table 6.2.2-2: Payload for AMFDeregistration record

Field name	Description	M/C/O
deregistrationDirection	Indicates whether the deregistration was initiated by the network or by the UE.	M
accessType	Indicates the access for which the deregistration is handled, see TS 24.501 [13] , clause 9.11.3.20.	M
sUPI	SUPI associated with the deregistration (see clause 6.2.2.4), if available.	C
sUCI	SUCI used in the deregistration, if available (see NOTE 1).	C
pEI	PEI used in the deregistration, if available (see NOTE 1).	C
gPSI	GPSI associated to the deregistration, if available as part of the subscription profile.	C
gUTI	5G-GUTI used in the deregistration, if available, see TS 24.501 [13], clause 5.5.2.2.1 (see NOTE 1).	C
cause	Indicates the 5GMM cause value for network-initiated deregistration, see TS 24.501 [13], clause 9.11.3.2.	C
location	Location information determined by the network during the deregistration, if available.	C
NOTE: At least one among SUCI, PEI and GUTI shall be provided.		

6.2.2.2.4 Location update

The IRI-POI in the AMF shall generate an xIRI containing an AMFLocationUpdate record each time the IRI-POI present in an AMF detects that the target’s UE location is updated due to target’s UE mobility or as a part of an AMF service procedure. The generation of such separate xIRI is not required if the updated UE location information is obtained as a part of a procedure producing some other xIRIs (e.g. mobility registration). In that case the location information is included into the respective xIRI message.

The UE mobility events resulting in an xIRI generation include the “N2 Path Switch Request” (“Xn based inter NG-RAN handover” procedure described in 3GPP TS 29.571 [4], clause 4.9.1.2) and the “N2 Handover Notify” (“Inter NG-RAN node N2 based handover” procedure described in 3GPP TS 29.571 [4], clause 4.9.1.3).

Additionally, based on regulatory requirements and operator policy, the location information obtained by AMF from NG-RAN or LMF in the course of some service operation (e.g. emergency services, LCS) may generate an xIRI containing an AMFLocationUpdate record. In the case of NG-RAN, the generation is triggered by a “Location Report” from NG-RAN induced by a “Location Report Control” from AMF, as described in 3GPP TS 29.571 [4], clause 4.10. In the case of LMF, the generation is triggered by a “Nlmf_Location_DetermineLocation Response” from LMF to AMF, as described in 3GPP TS 29.571 [4], clause 5.2.15.

Table 6.2.2-3: Payload for AMFLocationUpdate record

Field name	Description	M/C/O
sUPI	SUPI associated with the location update (see clause 6.2.2.4).	M
sUCI	SUCI associated with the location update, if available, see TS 24.501 [13].	C
pEI	PEI associated with the location update, if available.	C
gPSI	GPSI associated with the location update, if available as part of the subscription profile.	C
gUTI	5G-GUTI associated with the location update, if available, see TS 24.501 [13].	C
location	Updated location information determined by the network.	M

6.2.2.2.5 Start of interception with registered UE

The IRI-POI in the AMF shall generate an xIRI containing an AMFStartOfInterceptionWithRegisteredUE record when the IRI-POI present in the AMF detects that interception is activated on a UE that has already been registered in the 5GS (see clause 6.2.2.4 on identity privacy). A UE is considered to be already registered to the 5GS when the 5GMM state for that UE is 5GMM-REGISTERED. Therefore, the IRI-POI present in the AMF shall generate the xIRI AMFStartOfInterceptionWithRegisteredUE record when it detects that a new interception for an UE is activated (i.e. provisioned by the LIPF) and the 5G mobility management state within the AMF for that UE is 5GMM-REGISTERED.

Table 6.2.2-4: Payload for AMFStartOfInterceptionWithRegisteredUE record

Field name	Description	M/C/O
registrationResult	Specifies the result of registration, see TS 24.501 [13], clause 9.11.3.6.	M
registrationType	Specifies the type of registration, see TS 24.501 [13] clause 9.11.3.7, if available.	C
slice	Provide, if available, one or more of the following: - allowed NSSAI (see TS 24.501 [13] clause 9.11.3.37). - configured NSSAI (see TS 24.501 [13] clause 9.11.3.37). - rejected NSSAI (see TS 24.501 [13] clause 9.11.3.46). This is derived from the information that was sent to the UE in the REGISTRATION ACCEPT message. IRI-POI in AMF can include this information if and only if it retained the information that it had previously sent in the REGISTRATION ACCEPT message to the UE.	C
sUPI	SUPI associated with the registration (see clause 6.2.2.4).	M
sUCI	SUCI used in the registration.	C
pEI	PEI provided by the UE during the registration, if available.	C
gPSI	GPSI obtained in the registration, if available as part of the subscription profile.	C
gUTI	5G-GUTI provided as outcome of initial registration or used in other cases, see TS 24.501 [13], clause 5.5.1.2.2.	M
location	Location information, if available.	C
non3GPPAccessEndpoint	UE's local IP address used to reach the N3IWF, if available. IP addresses are given as 4 octets (for IPv4) or 16 octets (for IPv6) with the most significant octet first (network byte order).	C
timeOfRegistration	Time at which the last registration occurred, if available. This is the time stamp when the REGISTRATION ACCEPT message is sent to the UE or (when applicable) when the REGISTRATION COMPLETE is received from the UE. Shall be given qualified with time zone information (i.e. as UTC or offset from UTC, not as local time).	C

6.2.2.2.6 AMF unsuccessful procedure

The IRI-POI in the AMF shall generate an xIRI containing an AMFUnsuccessfulProcedure record when the IRI-POI present in the AMF detects an unsuccessful procedure for a UE matching one of the target identifiers provided via LI_X1.

Unsuccessful registration shall be reported only if the target UE has been successfully authenticated.

Accordingly, the IRI-POI in the AMF generates the AMFUnsuccessfulProcedure record when one of the following events are detected:

- AMF sends a N1: REGISTRATION REJECT message to the target UE and the UE 5G Mobility Management (5GMM) state within the AMF is changed to 5GMM-DEREGISTERED.

- AMF aborts a registration procedure before the UE 5G Mobility Management (5GMM) state within the AMF is changed to 5GMM-REGISTERED.
- AMF sends a SERVICE REJECT message to the target UE including a PDU session establishment reject message type.
- AMF aborts a UE-initiated NAS transport procedure with payload container type IE set to "SMS".

Table 6.2.2-5: Payload for AMFUnsuccessfulProcedure record

Field name	Description	M/C/O
failedprocedureType	Specifies the procedure which failed at the AMF.	M
failureCause	Provides the value of the 5GSM or 5GMM cause, see TS 24.501 [13], clauses 9.11.3.2 and 9.11.4.2.	M
requestedSlice	Slice requested for the procedure, if available, given as a NSSAI (a list of S-NSSAI values as described in TS 24.501 [13] clause 9.11.3.37).	C
sUPI	SUPI associated with the procedure, if available (see NOTE).	C
sUCI	SUCI used in the procedure, if applicable and if available (see NOTE).	C
pEI	PEI used in the procedure, if available (see NOTE).	C
gPSI	GPSI used in the procedure, if available (see NOTE).	C
gUTI	5G-GUTI used in the procedure, if available, see TS 24.501 [13], clause 9.11.3.4 (see NOTE).	C
location	Location information determined during the procedure, if available.	C
NOTE: At least one identity shall be provided, the others shall be provided if available.		

6.2.2.3 Generation of IRI over LI_HI2

When an IRI-POI in the AMF generated xIRI message is received over LI_X2, the MDF2 shall generate an IRI message over LI_HI2 without undue delay. The IRI message shall contain a copy of the relevant record received in the xIRI message from LI_X2. This record may be enriched with any additional information available at the MDF (e.g. additional location information).

The timestamp field of the psHeader structure shall be set to the time at which the AMF event was observed (i.e. the timestamp field of the X2 PDU).

The threeGPP33128DefinedIRI field in ETSI TS 102 232-7 [10] clause 15 shall be populated with the BER-encoded IRIPayload.

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 message to the LEMF associated with the additional warrants without receiving a corresponding xIRI.

6.2.2.4 Identity privacy

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 [11]. This shall be performed regardless of whether the SUPI is a target of interception, and whether the null encryption algorithm is used for the SUCI. The AMF shall maintain the SUPI to SUCI mapping for at least the lifetime of the registration in order to allow interception based on SUPI after the initial registration.

6.2.3 LI for SMF/UPF

6.2.3.1 Provisioning of SMF over LI_X1

The IRI-POI and CC-TF present in the SMF are provisioned over LI_X1 by the LIPF using the X1 protocol as described in clause 5.2.2. If an SMF and UPF are implemented as a single function, then this interface may be sufficient to provision both (see clause 6.2.3.3).

The POI in the SMF shall support the following target identifier formats in the ETSI TS 103 221-1 [7] messages (or equivalent if ETSI TS 103 221-1 [7] is not used):

- SUPI.

- PEI.
- GPSI.

If packet header reporting is required, parameters specified in table 6.2.3-9: ActivatePDHReporting Parameters shall be provided as part of the LI_X1 provisioning message.

6.2.3.2 Generation of xIRI at IRI-POI in SMF over LI_X2

6.2.3.2.1 General

The IRI-POI present in the SMF shall send the xIRI messages over LI_X2 for each of the events described in the following clauses.

6.2.3.2.2 PDU session establishment

The IRI-POI in the SMF shall generate an xIRI containing an SMFPDUSessionEstablishment record when the IRI-POI present in the SMF detects that a PDU session has been established for the target UE. The IRI-POI present in the SMF shall generate the xIRI for the following events:

- For a non-roaming scenario, the SMF (or for a roaming scenario, V-SMF in the VPLMN), sends the N1 NAS message (via AMF) PDU SESSION ESTABLISHMENT ACCEPT to the UE and the 5G Session Management (5GSM) state within the SMF is changed to PDU SESSION ACTIVE (see TS 24.501 [13]).
- For a home-routed roaming scenario, the SMF in the HPLMN (i.e. H-SMF) sends the N16: Nsmf_PDU_Session_Create response message with n1SmInfoToUe IE containing the PDU SESSION ESTABLISHMENT ACCEPT (see TS 29.502 [16]).

Table 6.2.3-1: Payload for SMFPDUSessionEstablishment record

Field name	Description	M/C/O
sUPI	SUPI associated with the PDU session (e.g. as provided by the AMF in the associated Nsmf_PDU_Session_CreateSMContext service operation). Shall be present except for PEI-only unauthenticated emergency sessions (see NOTE).	C
sUPIUnauthenticated	Shall be present if a SUPI is present in the message, and set to “true” if the SUPI has not authenticated, or “false” if it has been authenticated.	C
pEI	PEI associated with the PDU session if available (see NOTE).	C
gPSI	GPSI associated with the PDU session if available (see NOTE).	C
pDUSessionID	PDU Session ID See clause 9.4 of TS 24.501 [13].	M
gTPTunnelID	Contains the F-TEID identifying the GTP tunnel used to encapsulate the traffic, as defined in TS 29.244 [15] clause 8.2.3. Non-GTP encapsulation is for further study.	M
pDUSessionType	Identifies selected PDU session type, see TS 24.501 [13] clause 9.11.4.11.	M
sNSSAI	Slice identifiers associated with the PDU session, if available. See TS 23.003 [19] clause 28.4.2 and TS 23.501 [2] clause 5.12.2.2.	C
uEEndpoint	UE endpoint address(es) if available.	C
non3GPPAccessEndpoint	UE's local IP address used to reach the N3IWF, if available. IP addresses are given as 4 octets (for IPv4) or 16 octets (for IPv6) with the most significant octet first (network byte order).	C
location	Location information provided by the AMF, if available.	C
dNN	Data Network Name associated with the target traffic, as defined in TS 23.003[19] clause 9A and described in TS 23.501 [2] clause 4.3.2.2.	M
aMFID	Identifier of the AMF associated with the target UE, as defined in TS 23.003 [19] clause 2.10.1 when available.	C
hSMFURI	URI of the Nsmf_PDUSession service of the selected H-SMF, if available. See TS 29.502 [16] clause 6.1.6.2.2.	C
requestType	Type of request as described in TS 24.501 [13] clause 9.11.3.47 if available.	C
accessType	Access type associated with the session (i.e. 3GPP or non-3GPP access) if provided by the AMF (see TS 24.501 [13] clause 9.11.3.11).	C
rATType	RAT Type associated with the access if provided by the AMF as part of session establishment (see TS 23.502 [4] clause 4.3.2). Values given as per TS 29.571 [17] clause 5.4.3.2.	C
sMPDUDNRequest	Contents of the SM PDU DN Request container, if available, as described in TS 24.501 [13] clause 9.11.4.15.	C
NOTE: At least one of the SUPI, PEI or GPSI fields shall be present.		

6.2.3.2.3 PDU session modification

The IRI-POI in the SMF shall generate an xIRI containing an SMFPDUSessionModification record when the IRI-POI present in the SMF detects that a PDU session has been modified for the target UE. The IRI-POI present in the SMF shall generate the xIRI for the following events:

- For a non-roaming scenario, the SMF (or for a roaming scenario, V-SMF in the VPLMN), receives the N1 NAS message (via AMF) PDU SESSION MODIFICATION COMMAND COMPLETE from the UE and the 5GSM state within the SMF is returned to PDU SESSION ACTIVE (see TS 24.501 [13]). This applies to the following two cases:
  - UE initiated PDU session modification.
  - Network (VPLMN) initiated PDU session modification.
- For a non-roaming scenario, the SMF (or for a roaming scenario, V-SMF in the VPLMN), sends the N1 NAS message (via AMF) PDU SESSION ESTABLISHMENT ACCEPT to the UE and the 5GSM state within the SMF remains in the PDU SESSION ACTIVE (see TS 24.501 [13]). This applies to the following case:
  - Handover from one access type to another access type happens (e.g. 3GPP to non-3GPP).
- For a home-routed roaming scenario, the SMF in the HPLMN (i.e. H-SMF) receives the N16: Nsmf_PDU_Session_Update response message with n1SmInfoFromUe IE containing the PDU SESSION MODIFICATION COMMAND COMPLETE (see TS 29.502 [16]). This applies to the following three cases:
  - UE initiated PDU session modification.
  - Network (VPLMN) initiated PDU session modification.
  - Network (HPLMN) initiated PDU session modification.
- For a home-routed roaming scenario, the SMF in the HPLMN (i.e. H-SMF) sends the N16: Nsmf_PDU_Session_Create response message with n1SmInfoToUe IE containing the PDU SESSION ESTABLISHMENT ACCEPT (see TS 29.502 [16]) while it had received a N16 Nsmf_PDU_Session_Create request message with an existing PDU Session Id with access type being changed. This applies to the following case:
  - Handover from one access type to another access type happens (e.g. 3GPP to non-3GPP).

Table 6.2.3-2: Payload for SMFPDUSessionModification record

Field name	Description	M/C/O
sUPI	SUPI associated with the PDU session (e.g. as provided by the AMF in the associated Nsmf_PDU_Session_CreateSMContext service operation). Shall be present except for PEI-only unauthenticated emergency sessions.	C
sUPIUnauthenticated	Shall be present if a SUPI is present in the message, and set to “true” if the SUPI was not authenticated, or “false” if it has been authenticated.	C
pEI	PEI associated with the PDU session if available.	C
gPSI	GPSI associated with the PDU session if available.	C
sNSSAI	Slice identifier associated with the PDU session, if available. See TS 23.003 [19] clause 28.4.2 and TS 23.501 [2] clause 5.12.2.2.	C
non3GPPAccessEndpoint	UE's local IP address used to reach the N3IWF, if available. IP addresses are given as 4 octets (for IPv4) or 16 octets (for IPv6) with the most significant octet first (network byte order).	C
location	Location information provided by the AMF, if available.	C
accessType	Access type associated with the session (i.e. 3GPP or non-3GPP access) if provided by the AMF (see TS 24.501 [13] clause 9.11.3.11).	C
rATType	RAT type associated with the access, if available. Values given as per TS 29.571 [17] clause 5.4.3.2.	C

6.2.3.2.4 PDU session release

The IRI-POI in the SMF shall generate an xIRI containing an SMFPDUSessionRelease record when the IRI-POI present in the SMF detects that a PDU session been released. The IRI-POI present in the SMF shall generate the xIRI for the following events:

- For a non-roaming scenario, the SMF (or for a roaming scenario, V-SMF in the VPLMN), receives the N1 NAS message (via AMF) PDU SESSION RELEASE COMMAND COMPLETE from the UE and the 5GSM state within the SMF is changed to PDU SESSION INACTIVE (see TS 24.501 [13]). This applies to the following two cases:
  - UE initiated PDU session release.
  - Network initiated PDU session release.
- For a non-roaming scenario, the SMF (or for a roaming scenario, V-SMF in the VPLMN), receives the N1 NAS message (via AMF) PDU SESSION MODIFICATION COMMAND REJECT from the UE with the cause value #43 indicating an invalid PDU Session ID and the 5GSM state within the SMF is changed to PDU SESSION INACTIVE (see TS 24.501 [13]). This applies to the case where the UE rejects a PDU SESSION MODIFICATION COMMAND as it finds that the indicated PDU session ID is invalid. The 5GSM state is changed to PDU SESSION INACTIVE implicitly within the SMF.
- For a home-routed roaming scenario, the SMF in the HPLMN (i.e. H-SMF) receives the N16: Nsmf_PDU_Session_Update response message with n1SmInfoFromUe IE containing the PDU SESSION RELEASE COMMAND COMPLETE (see TS 29.502 [16]) from the V-SMF. This applies to the following three cases:
  - UE initiated PDU session release.
  - Network (VPLMN) initiated PDU session release.
  - Network (HPLMN) initiated PDU session release.
- For a home-routed roaming scenario, the SMF in the HPLMN (i.e. H-SMF) receives the N16: Nsmf_PDU_Session_Update response message with n1SmInfoFromUe IE containing the PDU SESSION MODIFICATION COMMAND REJECT (see TS 29.502 [16]) from the V-SMF with the cause value #43 indicating an Invalid PDU Session ID.

Table 6.2.3-3: Payload for SMFPDUSessionRelease record

Field name	Description	M/C/O
sUPI	SUPI associated with the PDU session.	M
pEI	PEI associated with the PDU session if available.	C
gPSI	GPSI associated with the PDU session if available.	C
pDUSessionID	PDU Session ID as assigned by the AMF.	M
timeOfFirstPacket	Time of first packet as reported in the usage report IE if available in the UPF deletion response (see TS 29.244 [15] clause 7.5.7.2).	C
timeOfLastPacket	Time of last packet as reported in the usage report IE if available (see TS 29.244 [15] clause 7.5.7.2).	C
uplinkVolume	Number of uplink octets, as reported in the volume report IE if available (see TS 29.244 [15] clause 7.5.7.2).	C
downlinkVolume	Number of downlink octets, as reporting the volume report IE if available (see TS 29.244 [15] clause 7.5.7.2).	C
location	Location information, if available.	C

6.2.3.2.5 Start of interception with an established PDU session

The IRI-POI in the SMF shall generate an xIRI containing an SMFStartOfInterceptionWithEstablishedPDUSession record when the IRI-POI present in the SMF detects that a PDU session has already been established for the target UE when interception starts.

In a non-roaming scenario, the IRI-POI in the SMF (or in a roaming scenario, the IRI-POI in the V-SMF in the VPLMN) shall generate the SMFStartOfInterceptionWithEstablishedPDUSession record when it detects that a new interception for a UE is activated (i.e. provisioned by the LIPF) for the following case:

- The 5GSM state within the SMF for that UE is 5GSM: PDU SESSION ACTIVE or PDU SESSION MODIFICATION PENDING.

NOTE: The above trigger happens when the SMF (V-SMF in VPLMN) had not sent an N1 NAS message PDU SESSION RELEASE COMMAND to the UE for a PDU session and the SMF (V-SMF in the VPLMN) had previously sent an N1 NAS message PDU SESSION ESTABLISHMENT ACCEPT to that UE for the same PDU session.

In a home-routed roaming scenario, the IRI-POI in the H-SMF shall generate the xIRI when it detects that a new interception for a UE is activated (i.e. provisioned by the LIPF) for the following case:

- The H-SMF had not sent a Nsmf_PDU_Session_Update Request (n1SmInfoToUe: PDU SESSION RELEASE COMMAND) to the V-SMF for a PDU session and H-SMF had previously sent an Nsmf_PDU_Session_Create response (n1SmInfoToUE: PDU SESSION ESTABLISHMENT ACCEPT) to the V-SMF for that PDU session.

The IRI-POI in the SMF shall generate the xIRI SMF Start Of Interception with established PDU session message or each of the PDU sessions (that meets the above criteria) associated with the newly identified target UEs.

Table 6.2.3-4: Payload for SMFStartOfInterceptionWithEstablishedPDUSession record

Field name	Description	M/C/O
sUPI	SUPI associated with the PDU session (e.g. as provided by the AMF in the associated Nsmf_PDU_Session_CreateSMContext service operation). Shall be present except for PEI-only unauthenticated emergency sessions.	C
sUPIUnauthenticated	Shall be present if a SUPI is present in the message, and set to “true” if the SUPI has not authenticated, or “false” if it has been authenticated.	C
pEI	PEI associated with the PDU session if available.	C
gPSI	GPSI associated with the PDU session if available.	C
pDUSessionID	PDU Session ID as assigned by the AMF, as defined in TS 24.007 [14] clause 11.2.3.1b.	M
gTPTunnelID	Contains the F-TEID identifying the tunnel used to encapsulate the traffic, as defined in TS 29.244 [15] clause 8.2.3. Non-GTP encapsulation is for further study.	M
pDUSessionType	Identifies selected PDU session type, see TS 24.501 [13] clause 9.11.4.11.	M
sNSSAI	Slice identifier associated with the PDU session, if available. See TS 23.003 [19] clause 28.4.2 and TS 23.501 [2] clause 5.12.2.2.	C
uEEndpoint	UE endpoint address(es) if available. IP addresses are given as 4 octets (for IPv4) or 16 octets (for IPv6) with the most significant octet first (network byte order). MAC addresses are given as 6 octets with the most significant octet first.	C
non3GPPAccessEndpoint	UE's local IP address used to reach the N3IWF, if available. IP addresses are given as 4 octets (for IPv4) or 16 octets (for IPv6) with the most significant octet first (network byte order).	C
Location	Location information provided by the AMF at session establishment, if available.	C
dNN	Data Network Name associated with the target traffic, as defined in TS 23.003 [19] clause 9A and described in TS 23.501 [2] clause 4.3.2.2.	M
aMFID	Identifier of the AMF associated with the target UE, as defined in TS 23.003 [19] clause 2.10.1.	M
hSMFURI	URI of the Nsmf_PDUSession service of the selected H-SMF, if available. See TS 29.502 [16] clause 6.1.6.2.2.	C
requestType	Type of request as described in TS 24.501 [13] clause 9.11.3.47 if available.	C
accessType	Access type associated with the session (i.e. 3GPP or non-3GPP access) if provided by the AMF (see TS 24.501 [13] clause 9.11.3.11).	C
rATType	RAT type associated with the access if provided by the AMF as part of session establishment (see TS 23.502 [4] clause 4.3.2). Values given as per TS 29.571 [17] clause 5.4.3.2.	C
sMPDUDNRequest	Contents of the SM PDU DN request container, if available, as described in TS 24.501 [13] clause 9.11.4.15.	C

6.2.3.2.6 SMF unsuccessful procedure

The IRI-POI in the SMF shall generate an SMFUnsuccessfulProcedure record when the IRI-POI present in the SMF detects an unsuccessful procedure or error condition for a UE matching one of the target identifiers provided via LI_X1.

Accordingly, the IRI-POI in the SMF generates the SMFUnsuccessfulProcedure record when one of the following events are detected:

- SMF sends a PDU SESSION ESTABLISHMENT REJECT message to the target UE.

- SMF sends a PDU SESSION MODIFICATION REJECT message to the target UE.

- SMF sends a PDU SESSION RELEASE REJECT message to the target UE.
- SMF receives a PDU SESSION MODIFICATION COMMAND REJECT message from the target UE.
- An ongoing SM procedure is aborted at the SMF, due to e.g. a 5GSM STATUS message sent from or received by the SMF.

Table 6.2.3-5: Payload for SMFUnsuccessfulProcedure record

Field name	Description	M/C/O
failedProcedureType	Specifies the procedure which failed or is aborted at the SMF.	M
failureCause	Provides the value of the 5GSM cause, see TS 24.501 [13], clause 9.11.4.2. In case the procedure is aborted due to a 5GSM STATUS message, the 5GSM cause is the one included in the 5GSM status message.	M
requestedSlice	Slice requested for the procedure, if available, given as a NSSAI (a list of S-NSSAI values as described in TS 24.501 [13] clause 9.11.3.37).	C
Initiator	Specifies whether the network (SMF) or the UE is initiating the rejection or indicating the failure.	M
sUPI	SUPI associated with the procedure, if available (see NOTE).	C
sUPIUnauthenticated	Shall be present if a SUPI is present in the message and set to “true” if the SUPI has not authenticated, or “false” if it has been authenticated.	C
pEI	PEI used in the procedure, if available (see NOTE).	C
gPSI	GPSI used in the procedure, if available (see NOTE).	C
pDUSessionID	PDU Session ID See clause 9.4 of TS 24.501 [13], if available.	C
uEEndpoint	UE endpoint address(es) if available.	C
non3GPPAccessEndpoint	UE's local IP address used to reach the N3IWF, if available.	C
Location	Location information provided by the AMF, if available.	C
dNN	Data Network Name associated with the target traffic, as defined in TS 23.003 [19] clause 9A and described in TS 23.501 [2] clause 4.3.2.2, if available.	C
aMFID	Identifier of the AMF associated with the target UE, as defined in TS 23.003 [19] clause 2.10.1 when available.	C
hSMFURI	URI of the Nsmf_PDUSession service of the selected H-SMF, if available. See TS 29.502 [16] clause 6.1.6.2.2.	C
requestType	Type of request as described in TS 24.501 [13] clause 9.11.3.47 if available.	C
accessType	Access type associated with the session (i.e. 3GPP or non-3GPP access) if provided by the AMF (see TS 24.501 [13] clause 9.11.3.11).	C
rATType	RAT Type associated with the access if provided by the AMF as part of session establishment (see TS 23.502 [4] clause 4.3.2). Values given as per TS 29.571 [17] clause 5.4.3.2.	C
sMPDUDNRequest	Contents of the SM PDU DN Request container, if available, as described in TS 24.501 [13] clause 9.11.4.15.	C
NOTE: At least one identity shall be provided, the others shall be provided if available.		

6.2.3.3 Triggering of the CC-POI from CC-TF over LI_T3

6.2.3.3.1 LI_T3 interface specifics

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.

When the CC-TF in the SMF detects that a PDU session has been established for a target UE (i.e. when the SMF sends the N4: Session Establishment Request and N4: Session Modification Request to the UPF), it shall send an activation message to the CC-POI in the UPF over the LI_T3 interface. The activation message shall contain the correlation identifiers that the CC-POI in the UPF shall use with the xCC. This can be achieved by sending an ActivateTask message as defined in ETSI TS 103 221-1 [7] clause 6.2.1 with the following details.

Table 6.2.3-6: ActivateTask message for triggering the CC-POI in the UPF

ETSI TS 103 221-1 field name	Description	M/C/O
XID	Set to the same XID associated with the interception in the SMF.	M
TargetIdentifiers	Packet detection criteria as determined by the CC-TF in the SMF, which enables the UPF to isolate target traffic. The CC-POI in the UPF shall support at least the following identifier types: - GTP Tunnel ID. - IPv4 address. - IPv6 address. NOTE: This value is the target identifier for the CC-POI in the UPF, and may be different from the target identifier specified in the warrant.	M
DeliveryType	Set to "X3Only".	M
ListOfDIDs	Delivery endpoints for LI_X3. These delivery endpoints shall be configured by the CC-TF in the SMF using the CreateDestination message as described in ETSI TS 103 221-1 [7] clause 6.3.1 prior to first use.	M
CorrelationNumber	Correlation ID to assign to X3 PDUs generated by the CC-POI in the UPF.	M

When the CC-TF in the SMF detects that a targeted PDU session has changed (i.e. when the SMF sends the N4 Session Modification Request to the UPF) in a way which requires changes to the interception by the CC-POI in the UPF, the CC-TF shall modify the interception at the CC-POI in the UPF over the LI_T3 interface. This is achieved by sending a ModifyTask message as defined in ETSI TS 103 221-1 [7] clause 6.2.2 with the following details.

Table 6.2.3-7: ModifyTask message for updating interception at the CC-POI in the UPF

ETSI TS 103 221-1 field name	Description	M/C/O
XID	Set to the XID associated with the interception.	M
TargetIdentifiers	Updated packet detection criteria as determined by the CC-TF in the SMF. NOTE: See notes on TargetIdentifiers in Table 6.2.3-6.	M

When the CC-TF in the SMF detects that the PDU session has been released (i.e. when the SMF sends the N4: Session Release Request to the UPF) for a target UE, it shall send a deactivation message to the CC-POI in the UPF over the LI_T3 interface. When using ETSI TS 103 221-1 [7] this is achieved by sending a DeactivateTask message with the XID field set to the XID associated with the interception, as described in ETSI TS 103 221-1 [7] clause 6.2.3.

6.2.3.3.2 CC interception with multi-homed PDU session

When a target UE accesses multiple Data Networks (DNs) via a multi-homed PDU session (see TS 23.501 [2] clause 5.6.4.3), multiple UPFs are involved in providing the PDU Session Anchors with one UPF providing the Branching Point functionality. The Branching Point UPF may, or may not, be a PDU Session Anchor UPF (see TS 33.127 [5] Annex A3.2). The CC-TF present in the SMF shall send the CC intercept trigger to the CC-POI present in an UPF if and only if that UPF is selected to provide the CC-POI functions.

When the target UE is involved in multi-homed PDU session, the CC-TF present in the SMF (i.e. in the SMF that establishes the PDU session) shall determine which UPF(s) is(are) more suitable to provide the CC-POI functions adhering to the following requirements specified in TS 33.127 [5]:

- All applicable user plane packets are captured and delivered.
- Duplicate delivery of CC is suppressed to the extent possible.

To meet the above requirements, the CC-TF present in the SMF shall follow the rules specified below:

NOTE 1: The below rules are based on the assumption that a PDU session has one Branching Point UPF (with N3 reference point toward the target UE) and one PDU Session Anchor UPF for each DN connection).

Scenario 1: CC Interception of all DN connections is not required.

a. CC interception at PDU Session Anchor UPF.

If the CC interception of all DN connections is not required, then the CC-TF present in the SMF shall choose one or more of the PDU Session Anchor UPFs (that are on the user plane path of DN connections that require CC interception) to provide the CC-POI functions.

In this case, the CC intercept trigger shall be sent to the CC-POIs present in the selected PDU Session Anchor UPFs and shall include the packet detection rules. Examples of the packet detection rules are:

- Generate the xCC from the user plane packets sent and received from the DN connection that requires the interception, or
- Generate the xCC from all the incoming user plane packets.

In this case, the CC-TF present in the SMF shall select the Branching Point UPF to provide the CC-POI functions unless the Branching Point UPF is also a PDU Session Anchor UPF.

b. Branching Point UPF is also a PDU Session Anchor UPF.

If the CC interception of all DN connections is not required and if the UPF playing the role of Branching Point is also a PDU Session Anchor UPF, and if the CC interception for the related DN connection is required, then SMF shall choose the Branching Point/PDU Session Anchor UPF to provide the CC-POI functions for the related DN connection. The CC interception trigger sent to CC-POI present in the Branching Point/PDU Session Anchor UPF shall include the following packet detection rule:

- Generate the xCC from the user plane packets that are sent and received from the DN network to which the Branching Point UPF is providing the PDU Session Anchor PDU function.

In this case, the user plane packets sent/received on the common path (i.e. over the N3 interface) shall not be intercepted since such an interception, if performed, will result in a duplicate delivery of CC intercepted at the CC-POIs present in the PDU Session Anchor UPFs.

Scenario 2: CC interception of all DN connections is required.

If the CC interception of all DN connections is required, then the SMF may choose either all the PDU Session Anchor UPFs or the Branching Point UPF to provide the CC-POI functions.

a) PDU Session Anchor UPFs are chosen.

With this method, to ensure that all user-plane packets are intercepted, the CC-TF present in the SMF will have to choose all PDU Session Anchor UPFs to provide the CC-POI functions and accordingly, send the CC interception trigger to CC-POIs present in all the PDU Session Anchor UPFs. The CC interception trigger shall include the packet detection rules as applicable to respective CC-POIs and the examples of those rules are the same as described under scenario 1, a.

In this case, the CC-TF present in the SMF shall select the Branching Point UPF to provide the CC-POI functions if, and only if, the Branching Point UPF is also a PDU Session Anchor UPF and the packet detection rules included within the CC interception trigger sent to the CC-POI present in the Branching Point/PDU Session Anchor UPF shall be according to scenario 1, b.

b) Branching Point UPF is chosen.

When all user plane packets pass through the Branching Point UPF, the CC-TF present SMF may choose the Branching Point UPF to provide the CC -POI function and accordingly, send the CC interception trigger to the CC-POI present in the Branching Point UPF. The CC intercept trigger shall include the packet detection rules and examples of the same are:

- Generate the xCC from all the incoming and outgoing user plane packets to the target UE, or
- Generate the xCC from all the incoming user plane packets.

In this case, the CC-TF present in the SMF shall not select any of the PDU Session Anchor UPFs to provide the CC-POI functions.

NOTE 2: When Branching Point UPF is chosen to provide the CC-POI functions, and if the Branching Point UPF is removed from the user plane path during a PDU session, then the CC POI functions will have to be moved to the PDU Session Anchor UPFs.

The xCC delivered to the MDF3 shall be correlated to the PDU session related xIRI messages. The use of Correlation Id shall be on a user-plane path basis, which means that the xCC generated at different UPFs may need to have separate Correlation Ids, each correlating to their own PDU session related xIRI messages.

6.2.3.3.3 CC Interception only at PDU Session Anchor UPFs

Another option is to intercept on the N6 (defined in TS 23.501) side of the PDU Anchor UPF (for each UL classifier in case of selective routing or Service and Session Continuity mode 3) for each DN that needs to be intercepted.

6.2.3.4 IRI-POI in UPF triggering over LI_T2

When interception of Packet Data Headers is required, the IRI-TF in the SMF sends a trigger to the IRI-POI in the UPF over the LI_T2 interface.

When the IRI-TF in the SMF detects that a PDU session has been established for a target UE, it shall send an activation message to the IRI-POI in the UPF over the LI_T2 interface. The activation message shall contain the correlation identifiers that the IRI-POI in the UPF shall use when generating xIRI. This shall be achieved by sending an ActivateTask message as defined in TS 103 221-1 [7] clause 6.2.1 with the following details:

Table 6.2.3-8: ActivateTask message for triggering the UPF IRI-POI

ETSI TS 103 221-1 field name	Description	M/C/O
XID	Set to the same XID associated with the interception in the SMF.	M
TargetIdentifiers	Packet detection criteria as determined by the IRI-TF in the SMF, which enable the UPF IRI-POI to isolate target traffic. The IRI-POI in the UPF shall support at least the following identifier types: - GTP Tunnel ID. - IPv4 address. - IPv6 address. NOTE: This value is the target identifier for the IRI-POI in the UPF, and may be different from the target identifier specified in the warrant.	M
DeliveryType	Set to “X2Only”.	M
TaskDetailsExtensions/ HeaderReporting	Header reporting-specific tag to be carried in the *TaskDetailsExtensions* field of ETSI TS 103 221-1 [7].	M
ListOfDIDs	Delivery endpoints of LI_X2. These delivery endpoints shall be configured by the IRI-TF in the SMF using the *CreateDestination* message as described in ETSI TS 103 221-1 [7] clause 6.3.1 prior to first use.	M
CorrelationNumber	Correlation ID to assign to LI_X2 xIRI messages generated by the IRI-POI in the UPF.	M

Table 6.2.3-9: ActivatePDHReporting Parameters

Field name	Description	M/C/O
pDHType	This field shall be set to either: - "PDHR," for packet-by-packet reporting. - "PDSR," for summarized reporting.	M
pDSRType	If pDHType is PDSR, this field shall be set to one of the following triggers: a) timer expiry (along with a timer value and unit). b) packet count (along with a value for the number of packets detected before a summary is to be triggered). c) byte count (along with a value for the cumulative byte size reached across all packets belonging to the summary before said summary is to be triggered). Summary reports shall not be cumulative, i.e., each summary report shall describe only the packets contained in its respective range, and each new summary shall start its count (of whichever attribute from the numbered list above applies) from zero, i.e., the information in the (n+1)'th summary report starts immediately after the end of the n'th summary report.	C

When the IRI-TF in the SMF detects that a targeted PDU session has changed in a way which requires changes to the interception by the IRI-POI in the UPF, the IRI-TF in the SMF shall modify the interception at the IRI-POI in the UPF over the LI_T2 interface. This is achieved by sending an ModifyTask message as defined in ETSI TS 103 221-1[[7] clause 6.2.2 with the following details:

Table 6.2.3-10: ModifyTask message for updating interception at the IRI-POI in the UPF

Field name	Description	M/C/O
XID	Set to the XID associated with the interception	M
TargetIdentifiers	Updated packet detection criteria as determined by the IRI-TF in the SMF. NOTE: See notes on TargetIdentifiers in Table 6.2.3-6.	M

When the IRI-POI in the SMF detects that the PDU session has been released for a target UE, it shall send a deactivation message to the IRI-POI in the UPF over the LI_T2 interface. When using ETSI TS 103 221-1 [7] this is achieved by sending a DeactivateTask message with the XID field set to the XID associated with the interception, as described in ETSI TS 103 221-1 [7] clause 6.2.3.

When a PDU session involves multiple UPFs, the selection of UPF to provide the IRI-POI functions shall be done in the same way an UPF is selected to provide the CC-POI functions as described in clauses 6.2.3.3.2 and 6.2.3.3.3.

6.2.3.5 Generation of xIRI at UPF over LI_X2

6.2.3.5.1 Packet data header reporting

The IRI-POI in the UPF generates packet data header information either in per-packet form, as Packet Data Header Reports (PDHRs), or in summary form, as Packet Data Header Summary Reports (PDSRs).

6.2.3.5.2 Fragmentation

If the IRI-POI in the UPF is placed on a link which fragmented the original IP packet (see IETF RFC 791[34] for basic fragmentation rules, and IETF RFC 815 [26] for more complex re-assembly rules), a situation may occur in which only the first fragment can be sensibly reported in a PDHR, while the subsequent fragments may be missing essential fields that are mandatory, which may cause simplistic implementations to mis-report them, or omit them altogether.

In this case, the CC-POI in the UPF shall report the first fragment of a fragmented IP packet, including the port numbers when they are included within this first fragment, using the length of the fragment to determine if the port numbers are indeed encoded within this first fragment. The subsequent fragments are reported without port information. This technique relieves the IRI-POI in the UPF from having to reassemble the original IP packet (at line speed) at the cost of accuracy of the reported fields.

6.2.3.5.3 Packet Data Header Reporting (PDHR)

If the per-packet form of packet data header reporting, i.e. PDHR, is used, the IRI-POI in the UPF extracts the following information from each packet.

Table 6.2.3-11: PDHeaderReport record

Field name	Description	M/C/O
pDUSessionID	The PDU session ID received from the IRI-TF in the SMF.	M
sourceIPAddress	Shall contain the source address of the packet from the 32-bit *"Source Address"* field in IPv4, as defined in IETF RFC 791 [34], or from the 128-bit *"Source Address"* field in IPv6, as defined in IETF RFC 2460 [27].	M
sourcePort	Shall contain the *"Source Port*" number that indicates an application or service running on top of the transport, if the *"Protocol"* IP field (see the *nextLayerProtocol* field below in this table) is one of: a) Transmission Control Protocol (**TCP**), IP "Protocol" field decimal "6"; see IETF RFC 793 [28]. b) User Datagram Protocol (**UDP**), IP "Protocol" field decimal "17"; see IETF RFC 768 [29]. c) Datagram Congestion Control Protocol (**DCCP**), IP "Protocol" field decimal "33"; see IETF RFC 4340 [30]. d) Stream Control Transmission Protocol (**SCTP**), IP "Protocol" field decimal "132"; see IETF RFC 4960 [31]. For further details on Layer four protocols, see IANA [32].	C
destinationIPAddress	Shall contain the destination address of the packet from the 32-bit *"Destination Address"* field in IPv4, as defined in IETF RFC 791 [34], or from the 128-bit *"Destination Address"* field, as defined in IETF RFC 2460 [27].	M
destinationPort	Shall contain the *"Destination Port*" number that indicates an application or service running on top of the transport, if the *"Protocol"* IP field (see the *nextLayerProtocol* field below in this table) is one of: e) Transmission Control Protocol (**TCP**), IP "Protocol" field decimal "6"; see IETF RFC 793 [28]. f) User Datagram Protocol (**UDP**), IP "Protocol" field decimal "17"; see IETF RFC 768 [29]. g) Datagram Congestion Control Protocol (**DCCP**), IP "Protocol" field decimal "33"; see IETF RFC 4340 [30]. h) Stream Control Transmission Protocol (**SCTP**), IP "Protocol" field decimal "132"; see IETF RFC 4960 [31]. For further details on Layer four protocols, see IANA [32].	C
nextLayerProtocol	Shall contain the contents of the IP *"Protocol"* field as defined in IETF RFC 791 [34] (bits 72..79 in the IP header), and is one of the assigned Internet protocol numbers defined in *IANA* [32].	M
iPv6flowLabel	If the IP addresses in the report are IPv6, this field shall contain the 20-bit IPv6 "Flow Label" as defined in: • IPv6 IETF RFC 2460 [27], and • IPV6 Flow Label Specification IETF RFC 6437 [33].	C
direction	Shall contain the direction of the intercepted packet, and it indicates either "from target" or "to target."	M
packetSize	Shall contain the value of the *"Total Length*" IP header field if IPv4 is used, as defined in IETF RFC 791 [34], or the value of the "*Payload Length*" field if IPv6 is used, as defined in IETF RFC 2460 [27].	M

6.2.3.5.4 Packet Data Summary Reporting (PDSR)

If the summary form of the packet data header reporting, i.e. PDSR, is used, the IRI-POI in the UPF extracts from each packet the following information, and aggregates it in summaries.

Table 6.2.3-12: PDSummaryReport record

Field name	Description	M/C/O
pDUSessionID	The PDU session ID received from the IRI-TF in the SMF.	M
sourceIPAddress	Shall contain the source address of the packet from the 32-bit *"Source Address"* field in IPv4, as defined in IETF RFC 791 [34], or from the 128-bit *"Source Address"* field in IPv6, as defined in IETF RFC 2460 [27].	M
sourcePort	Shall contain the *"Source Port*" number that indicates an application or service running on top of the transport, if the *"Protocol"* IP field (see the *nextLayerProtocol* field below in this table) is one of: i) Transmission Control Protocol (**TCP**), IP "Protocol" field decimal "6"; see IETF RFC 793 [28]. j) User Datagram Protocol (**UDP**), IP "Protocol" field decimal "17"; see IETF RFC 768 [29]. k) Datagram Congestion Control Protocol (**DCCP**), IP "Protocol" field decimal "33"; see IETF RFC 4340 [30]. l) Stream Control Transmission Protocol (**SCTP**), IP "Protocol" field decimal "132"; Stream Control Transmission Protocol [31]. For further details on Layer four protocols, see IANA[32].	C
destinationIPAddress	Shall contain the destination address of the packet from the 32-bit *"Destination Address"* field in IPv4, as defined in IETF RFC 791 [34], or from the 128-bit *"Destination Address"* field, as defined in IETF RFC 2460 [27].	M
destinationPort	Shall contain the *"Destination Port*" number that indicates an application or service running on top of the transport, if the *"Protocol"* IP field (see the *nextLayerProtocol* field below in this table) is one of: m) Transmission Control Protocol (**TCP**), IP "Protocol" field decimal "6"; see IETF RFC 793 [28]. n) User Datagram Protocol (**UDP**), IP "Protocol" field decimal "17"; see IETF RFC 768 [29]. o) Datagram Congestion Control Protocol (**DCCP**), IP "Protocol" field decimal "33"; see IETF RFC 4340 [30]. p) Stream Control Transmission Protocol (**SCTP**), IP "Protocol" field decimal "132"; Stream Control Transmission Protocol [31]. For further details on Layer four protocols, see IANA [32].	C
nextLayerProtocol	Shall contain the contents of the IP *"Protocol"* field as defined in IETF RFC 791 [34] (bits 72..79 in the IP header), and is one of the assigned Internet protocol numbers defined in *IANA* [32].	M
iPv6flowLabel	If the IP addresses in the report are IPv6, this field shall contain the 20-bit IPv6 "Flow Label" as defined in IPv6 IETF RFC 2460 [27] and the *IPV6 Flow Label Specification* IETF RFC 6437 [33].	C
direction	Shall contain the direction of the intercepted packet, and it indicates either "from target" or "to target."	M
pDSRSummaryTrigger	Shall contain the trigger that caused the summary report to be generated, which is one of the following: a) timer expiry. b) packet count. c) byte count.	M
firstPacketTimestamp	Shall contain the timestamp that represents the time that the IRI-POI in the UPF detected the first packet in the set represented by this summary.	M
lastPacketTimestamp	Shall contain the timestamp that represents the time that the IRI-POI in the UPF detected the last packet in the set represented by this summary.	M
packetCount	Shall contain the number of packets detected during the creation of this summary.	M
byteCount	Shall contain the number of bytes summed across all packets that belong to this summary. For IPv4 it is the sum of the *"Total Length"* fields across all packets in the summary as defined in *Internet Protocol* IETF RFC 791 [34], while for IPv6 it is the sum of the *"Payload Length*" fields across all packets in the summary as defined in *Internet Protocol, Version 6 (IPv6) Specification*, IETF RFC 2460 [27].	M

6.2.3.6 Generation of xCC at CC-POI in the UPF over LI_X3

The CC-POI present in the UPF shall send xCC data over LI_X3 for each IP packet matching the criteria specified in the Triggering message (i.e. ActivateTask message) received over LI_T3 from the CC-TF in the SMF.

NOTE: Implementers are reminded of the completeness and non-duplication requirements (see TS 33.127 [5]).

Each X3 PDU shall contain the contents of the GTP-U packet given using the GTP-U payload format.

6.2.3.7 Generation of IRI over LI_HI2

When an IRI-POI in the SMF generated xIRI message is received over LI_X2, the MDF2 shall send an IRI message over LI_HI2 without undue delay. The IRI message shall contain a copy of the relevent record received from LI_X2. The record may be enriched by other information available at the MDF (e.g. additional location information).

The timestamp field of the ETSI TS 102 232-1 [9] PSHeader structure shall be set to the time at which the SMF event was observed (i.e. the timestamp field of the xIRI message). The LIID and CID fields shall correctly reflect the target identity and communication session to which the IRI belongs.

The threeGPP33128DefinedIRI field (see ETSI TS 102 232-7 [10] clause 15) shall be populated with the BER-encoded IRIPayload.

6.2.3.8 Generation of CC over LI_HI3

When an CC-POI in the UPF generated xCC data is received over LI_X3, the MDF3 shall emit a CC over LI_HI3 without undue delay.

The timestamp field of the ETSI TS 102 232-1 [9] PSHeader structure shall be set to the time that the UPF observed the data (i.e. the timestamp field of the xCC data). The LIID and CID fields shall correctly reflect the target identity and communication session to which the CC belongs.

6.2.3.9 Packet Data Information Reporting at MDF2

As described in TS 33.127 [5] clause 6.2.3.1, the warrants that do not require the interception of communication contents may require IRI messages that require access to the user plane packets. One such service that requires such a capability is the packet data header information reporting which includes the following two IRI messages:

- Packet Data Header Reporting (PDHR).

- Packet Data Summary Reporting (PDSR).

TS 33.127 [5] provides two approaches for the generation of such IRI messages. In approach 1, the IRI-POI present in the UPF based on a trigger received from IRI-TF present in the SMF constructs the xIRI PDHR and xIRI PDSR and delivers to the MDF2. The stage 3 details of this are described in clause 6.2.3.5 of the present document.

In approach 2, the CC-TF present in the SMF triggers the CC-POI present in the UPF to deliver the xCC data to the MDF3 as described in clause 6.2.3.5 of the present document. The MDF3 forwards the xCC information to the MDF2 over the LI-MDF interface and MDF2 generates the PDHR or PDSR IRI messages from the xCC information. The payload of PDHR and PDSR IRI messages are as described in clause 6.2.3.5, table 6.2.3-11.

In approach 2, the MDF2 generates the PDHR and PDSR IRI messages without receiving the equivalent xIRI messages from an IRI-POI. The actions of MDF2, MDF3 and CC-TF in SMF are managed as part of the intercept data provisioned to them over the LI_X1 interface.

6.2.4 LI at UDM for 5G

6.2.4.1 General description

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 Provisioning over LI_X1

The IRI-POI present in the SMSF is provisioned over LI_X1 by the LIPF using the X1 protocol as described in clause 5.2.2.

The POI in the SMSF shall support the following Target Identifier Formats in the ETSI TS 103 221-1 [7] messages:

- SUPI.
- PEI.
- GPSI.

6.2.5.2 Generation of xIRI over LI_X2

The IRI-POI present in the SMSF shall send xIRI messages over LI_X2 for each of the events listed in TS 33.127 [5] clause 6.2.5.3, each of which is described in the following clauses.

6.2.5.3 SMS Message

The IRI-POI in the SMSF shall generate an xIRI containing an SMSMessage record for the following cases:

SMS-MO case:

- When a target UE originates an SMS message or when any UE originates an SMS message destined to a target non-local ID.

SMS-MT case:

- When an SMS message delivery to a target UE is attempted or when an SMS message delivery originated from a target non-local ID is attempted to any UE.
- When an SMS message is successfully delivered to a target UE or when an SMS message originated from a target non-local ID is successfully delivered to any UE.

The SMS-MT case can also apply to the scenario when a receipt of SMS delivery from the far end is delivered successfully to the target UE or when a receipt of SMS delivery from a target non-Local ID is successfully delivered to the originating UE.

The IRI-POI present in the SMSF shall generate the SMSMessage record when it detects following events:

- The SMSF receives a SMCP message CP-DATA_RPDATA [SUBMIT_SMS] from a target UE (via AMF in Nsmsf_SMService_UplinkSMS message) or from any UE with TP-DA field within the SUBMIT_SMS containing a target non-Local ID and SMSF returns the SMCP: CP-ACK to that originating UE.
- The SMSF receives a Nsmsf_SMService_UplinkSMS with SmsRecordData IE containing the SMCP message CP-DATA_RP-ACK [SMS-DELIVER-REPORT] in response to a previously sent SMCP: Namf_Communication_N1N2MessageTransfer with N1MessageContainer having the SMCP message CP-DATA_RP-DATA [SMS-DELIVER].

NOTE 1: In the above-mentioned descriptions, the requirements of target Non-Local ID do not apply when both originating and terminating users of an SMS message are served by the same CSP. The method used to identify a target non-Local ID is different from the method used to identify a local target ID.

Table 6.2.5-1: Payload for SMSMessage record

Field name	Description	M/C/O
originatingSMSParty	Identity of the originating SMS party. See NOTE 2.	M
terminatingSMSParty	Identity of the terminating SMS party. See NOTE 3.	M
Direction	Direction of the SMS with respect to the target. See NOTE 4.	M
transferStatus	Indicates whether the transfer succeeded or not. See NOTE 5.	M
otherMessage	In the event of a server-initiated transfer, indicates whether the server will send another SMS. May be omitted if the transfer is target-initiated. See NOTE 6.	M
peerNFAddress	Address of the other network function (SMS-GMSC/IWMSC/SMS-Router) involved in the communication of the SMS, if available.	C
peerNFType	Type of the other network function (SMS-GMSC/IWMSC/SMS-Router) involved in the communication of the SMS, if available.	C
Location	Location information associated with the UE sending or receiving the SMS, if available. See NOTE 7.	C
smsTPDUData	SMS TPDU, encoded as per TS 23.040 [18] clause 9. See NOTE 8.	M

NOTE 2: For the SMS-MO case, the originating party is the address of the UE from which the SMSF receives the CP-DATA_RP_DATA (SUBMIT-MS) message (via AMF in the Nsmsf_SMService_UplinkSMS). The GPSI is one of the data fields used in the Nsmsf related messages (see TS 29.540 [21]). Alternatively, the SMSF may find the originating party address in the same way it finds the address when generating charging records. For SMS-MT case, this is derived from TP-OA field (TS 23.040 [18]).

NOTE 3: For SMS-MT case, the terminating party is the address of the UE to which the SMSF sends the CP-DATA_RP_DATA (SMS-DELIVER) message (via AMF in Namf_Communications_N1N2MessageTransfer). The GPSI is one of the data fields used in the Namf related messages (TS 29.518 [22]). Alternatively, the SMSF may find the terminating party address in the same way it finds the address when generating charging records. For SMS-MO case, this is derived from the TP-DA field (TS 23.040 [18]).

NOTE 4: For the SMS-MO case, for SMS originated from the target UE, the value fromTarget is used and for SMS destined to target Non-local ID, the toTarget is used. For SMS-MT case, for SMS terminated to the target UE, the value toTarget is used and for SMS originated from a target Non-local ID, the fromTarget is used.

NOTE 5: This field is set to transferSucceeded or transferFailed as follows:

- SMS-MO case:
  - To transferSucceeded: when the IRI-POI in the SMSF detects that SMSF sends the MO-FORWARD-SHORT-MESSAGE-request [SUBMIT SMS] message to the SMS-IWMSC.
  - To transferFailed: when the IRI-POI in SMSF detects the scenarios where SMSF cannot send the MO-FORWARD-SHORT-MESSAGE-request [SMS-SUBMIT] to SMS-IWMSC, but still generates an XIRISMSMESSAGE.
- SMS-MT case:
  - To transferSucceeded: when the IRI-POI in the SMSF detects that SMSF sends the MT-FORWARD-SHORT-MESSAGE-answer [SMS-DELIVER-REPORT] message to the SMS-IWMSC.
  - To transferFailed: when the IRI-POI in SMSF detects the scenarios where SMSF cannot send the MT-FORWARD-SHORT-MESSAGE-Answer [SMS-DELIVER-REPORT] to the SMS-GMSC, but an XIRISMSMESSAGE is still generated.

NOTE 6: This is only applicable to the SMS-MT case and can be derived from the TP-MMS (More Message to Send) field present in the SMS-DELIVER sent to the UE (via AMF in the Namf_Communications_N1N2MessageTransfer).

NOTE 7: This is derived from the ueLocation field of SmsRecord IE received from the AMF in the Nsmsf_SMService_UplinkSMS message (TS 29.540 [21]). For the SMS-MO case, the SMCP message is CP-DATA_RP-DATA [SMS-SUBMIT] and for the SMS-MT case, the SMCP message is CP-DATA-RP-ACK [SMS-DELIVER-REPORT].

NOTE 8: According to the intercept related data provisioning received over the LI_X1 reference point from the LIPF, the IRI-POI present in the SMSF may discover that the Interception Product may not include the CC. In this case, the IRI-POI present in the SMSF may remove the smsTPDUDATA from the SMSMessage record sent to the MDF2. When multiple warrants are issued on a target UE, the SMSF may deliver the SMSMessage record with the smsTPDUDATA present to the MDF2. In that case, the MDF2 is expected to remove the equivalent information from the IRI message sent over the LI_HI2 reference point when it discovers from the intercept related data provisioned to it over LI_X1 reference point.

6.2.5.4 Generation of IRI over LI_HI2

When an IRI-POI in the SMSF generated xIRI message is received over LI_X2, the MDF2 shall send an IRI message over LI_HI2 without undue delay. The IRI message shall contain a copy of the SMSFEvent record received from LI_X2. The record may be enriched by other information available at the MDF (e.g. additional location information).

The threeGPP33128DefinedCC field (see ETSI TS 102 232-7 [10] clause 15) shall be populated with the BER-encoded IRIPayload.

The timestamp field of the psHeader structure shall be set to the time that the SMSF event was observed (i.e. the timestamp field of the xIRI message). The LIID and CID fields shall correctly reflect the target identity and communication session to which the IRI belongs.

National regulations may require that the MDF2 removes information regarded as content from the smsTPDUData field in case of an IRI only warrant. The details of what needs be removed, and under what circumstances this is for national regulation, are outside the scope of the present document.

6.2.6 LI support at NRF

The SIRF present within the NRF provides SBA-related information to the LIPF over the LI_SI interface. Details for this interface are not considered in the present document and are for further study.

6.3 4G

The present document does not specify details of the LI interfaces for 4G / LTE. Details for this release are specified in TS 33.108 [12].

6.4 3G

The Present document does not specify details of the LI interfaces for 3G / UMTS. Details for this release are specified in TS 33.108 [12].

7 Service Layer Based Interception

7.1 Introduction

This clause describes any remaining fields, behaviours or details necessary to implement the required LI interfaces for specific 3GPP-defined services which are not described in clauses 4 and 5.

7.2 Central Subscriber Management

7.2.1 General description

This clause describes interception at central subscriber management functions or databases (e.g. UDM and HSS).

7.2.2 LI at UDM

7.2.2.1 General description

In 3GPP 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 and subscription management related xIRI.

7.2.2.2 Provisioning over LI_X1

The IRI-POI present in the UDM is provisioned over LI_X1 by the LIPF using the X1 protocol as described in clause 5.2.2.

7.2.2.3 Generation of xIRI over LI_X2

7.2.2.3.1 General description

The IRI-POI present in the UDM shall send xIRI messages over LI_X2 for each of the events listed in TS 33.127 [5] clause 7.2.2.4, each of which is described in the following clauses.

7.2.2.3.2 Serving system

The IRI-POI in the UDM shall generate the UDMServingSystemMessage record when it detects the following events:

- When the UDM receives the amf3GPPAccessRegistration from the AMF in the Nudm_UEContextManagement_Registration message (see TS 29.503 [25], clause 5.3.2.2.2).
- When the UDM receives the amfNon3GPPAccessRegistration from the AMF in the Nudm_UEContextManagement_Registration message (see TS 29.503 [25], clause 5.3.2.2.3).

When a target UE registers to both 3GPP and non-3GPP access, two UDMServingSystemMessage record may be generated by the UDM.

Table 7.2.2.3-1: Payload for UDMServingSystemMessage record

Field name	Description	M/C/O
sUPI	SUPI associated with the target UE, see TS 29.571 [17].	M
pEI	PEI associated with the target UE, when known, see TS 29.571 17].	C
gPSI	GPSI associated with the target UE, when known, see TS 29.571 [17].	C
gUAMI	Serving AMF's GUAMI, when known. See NOTE 1.	C
gUMMEI	Serving MME's GUMMEI See NOTE 2.	C
pLMNID	Serving PLMN Id. See TS 29.571 [17]. See NOTE 3.	C
servingSystemMethod	Identifies method used to access the serving system, see NOTE 4.	M

NOTE 1: GUAMI is the global unique identifier of an AMF [2] and its format is defined in TS 29.571 [17]. As defined in TS 23.501 [2], clause 5.9.4, GUAMI consists of <MCC> <MNC> <AMF Region ID> <AMF Set ID> <AMF Pointer>. The GUAMI is reported if the UDM receives the same from the AMF.

NOTE 2: GUMMEI is the global unique identifier of an MME and its format is defined in TS 23.003 [19]. As defined in TS 23.003 [19], clause 2.8.1, GUMMEI consists of <MCC> <MNC> <MME Identifier>. The GUMMEI is reported if the UDM receives the same from the MME.

NOTE 3: PLMN Id provides the VPLMN Id when the target UE is roaming.

NOTE 4: This identifies whether the UDMServingSystemMessage record is generated due to the reception of an amf3GPPAccessRegistration, or an amfNon3GPPAccessRegistration. See TS 29.503 [25].

7.2.2.3.3 Subscriber record change

Subscriber record change is not supported in the present document.

7.2.2.3.4 Cancel location

Cancel location is not supported in the present document.

7.2.2.3.5 Location information request

Location information request is not supported in the present document.

7.2.2.4 Generation of IRI over LI_HI2

When an IRI-POI in the UDM generated xIRI message is received over LI_X2, the MDF2 shall send an IRI message over LI_HI2 without undue delay.

The timestamp field of the psHeader structure shall be set to the time that the UDM event was observed (i.e. the timestamp field of the xIRI message). The LIID and CID fields shall correctly reflect the target identity and communication session to which the IRI belongs.

7.2.3 LI at HSS

The present document does not specify details of the LI interfaces at the HSS. Details for this release are specified in TS 33.108 [12].

7.3 Location

7.3.1 Lawful Access Location Services (LALS)

7.3.1.1 General description

The LALS architecture and functionality is specified in TS 33.127 [5], clause 7.3.3.

7.3.1.2 Provisioning over LI_X1

7.3.1.2.1 Target positioning service

For the LALS target positioning service (TS 33.127 [5], clause 7.3.3.2) the IRI-POI provided by the LI-LCS client is directly provisioned over LI_X1 by the LIPF using the LI_X1 protocol as described in clause 5.2.2 with the TaskDetailsExtensions field of the ActivateTask message specifying the type of the target positioning request, immediate vs. periodic, and, in the latter case, the periodicity of the positioning requests.

Based on national regulatory requirements and CSP policy, the TaskDetailsExtensions may also include the QoS parameters (specified in OMA-TS-MLP-V3-4-20150512-A [20]) for the use on the Le interface towards the LCS Server/GMLC. Alternatively, the QoS parameters may be statically configured in the LI-LCS client.

Table 7.3.1.2-1 shows the details of the LI_X1 ActivateTask message used for the LI-LCS client provisioning for the target positioning service.

The LI_X1 DeactivateTask shall be issued by the LIPF to terminate the target positioning service and withdraw the associated provisioning data, except for the Immediate target positioning service in which case the LI_X1 DeactivateTask is not used.

Table 7.3.1.2-1: ActivateTask message for LI-LCS client target positioning provisioning

ETSI TS 103 221-1 field name	Description	M/C/O
XID	XID assigned by LIPF.	M
TargetIdentifiers	One of the following: - SUPI. - PEI. - GPSI.	M
DeliveryType	Set to “X2Only”.	M
ListOfDIDs	Delivery endpoints of LI_X2 interface or MDF2 address. These delivery endpoints are configured using the CreateDestination message as described in ETSI TS 103 221-1 [7], clause 6.3.1 prior to the task activation.	M
TaskDetailsExtensions/ PositioningServiceType	“Immediate” or “Periodic”.	M
TaskDetailsExtensions/ PositioningPeriodicity	Time interval between the positioning requests in case of Periodic positioning, in seconds.	C
TaskDetailsExtensions/ PositioningParameters	Set of optional parameters for MLP SLIR message, per OMA-TS-MLP-V3-4-20150512-A [20]: requested location type (clause 5.3.60). - requested response type (clause 5.3.112.1). - max location age (clause 5.3.65). - response timing required (clause 5.3.106). - response timer (clause 5.3.107). - horizontal accuracy with QoS class (clause 5.3.44). - altitude accuracy with QoS class (clause 5.3.6). - motion state request (clause 5.3.70).	O

7.3.1.2.2 Triggered location service

For the LALS triggered location service (TS 33.127 [5], clause 7.3.3.3) the IRI-TF (LTF) is provisioned by the LIPF using the LI_X1 protocol as described in clause 5.2.2. The “TaskDetailsExtensions” parameter of the ActivateTask message in this case will carry the address of LI-LCS client to be used for the service and, optionally, the positioning parameters for use on the Le interface, similar to the target positioning provisioning.

Table 7.3.1.2-2 defines the details of the LI_X1 ActivateTask message used for the LTF provisioning for the Triggered Location service.

Table 7.3.1.2-2: ActivateTask message for LTF triggered location service provisioning

ETSI TS 103 221-1 field name	Description	M/C/O
XID	XID assigned by LIPF.	M
TargetIdentifiers	One of the following: - SUPI. - PEI. - GPSI.	M
DeliveryType	Set to “X2Only”.	M
ListOfDIDs	Delivery endpoints for LI-LCS Client LI_X2 xIRI messages. These delivery endpoints are configured in LTF using the CreateDestination message as described in ETSI TS 103 221-1 [7], clause 6.3.1 prior to the task activation.	M
TaskDetailsExtensions/ LI-LCSClientAddress	The IP address of the LI-LCS Client for triggering.	M
TaskDetailsExtensions/ PositioningParameters	Set of optional parameters for MLP SLIR message, per OMA-TS-MLP-V3-4-20150512-A [20]: - requested location type (clause 5.3.60). - requested response type (clause 5.3.112.1). - max location age (clause 5.3.65). - response timing required (clause 5.3.106). - response timer (clause 5.3.107). - horizontal accuracy with QoS class (clause 5.3.44). - altitude accuracy with QoS class (clause 5.3.6). - motion state request (clause 5.3.70).	O

7.3.1.3 Triggering over LI_T2

An LTF, provisioned as described in clause 7.3.3.2.2, triggers the triggered IRI-POI provided by the LI-LCS client using the LI_T2 protocol as described in clause 5.2.4. The "TaskDetailsExtensions" in the LI_T2 "ActivateTask" message carries the positioning parameters mapped from the LTF provisioning over the LI_X1. The LI_T2 "ActivateTask" message header may include a correlation ID from the triggering xIRI event, if available.

Prior to issuing one or more "ActivateTask" requests towards an LI-LCS Client, the LPF shall provision the LI-LCS client with the LI_X2 destinations by using the "CreateDestination" operation(s), as per clause 5.2.2. The LI-LCS client shall implicitly deactivate the task upon issuing the final xIRI message for the trigger. There is no DeactivateTask operation on the LI_T2 for the LI-LCS client.

The Table 7.3.1.3-1 shows the details of the LI_T2 ActivateTask message used by the LTF to trigger LI-CS client for the triggered location service.

Table 7.3.1.3-1: ActivateTask message from LTF to LI-LCS client for the triggered location service triggering

ETSI TS 103 221-1 field name	Description	M/C/O
XID	The same value as in the LTF provisioning (clause 7.3.3.2.2).	M
TargetIdentifiers	One of the following, per LTF provisioning: - SUPI. - PEI. - GPSI.	M
DeliveryType	Set to "X2Only".	M
ListOfDIDs	Delivery endpoints identifiers for LI-LCS Client LI_X2 messages. These delivery endpoints are configured in LTF using the CreateDestination message as described in ETSI TS 103 221-1 [7], clause 6.3.1 prior to the task activation.	M
TaskDetailsExtensions/ PositioningParameters	Set of parameters (requested location type, requested response type (SYNC vs ASYNC) and timing, QoS (max location age, accuracy and QoS Class), mapData request, velocity request), as per OMA-TS-MLP-V3-4-20150512-A [20], as specified in the LTF provisioning message over LI_X1.	C

7.3.1.4 Generation of xIRI over LI_X2

The IRI-POI provided by the LI-LCS client shall deliver the target location reports to respective MDF(s) as xIRI messages over the LI_X2 interface.

Table 7.3.1.4-1: LALSReport record

Field name	Description	M/C/O
sUPI	SUPI of the target, if used for the service.	C
pEI	PEI of the target, if used for the service.	C
gPSI	GPSI of the target, if used for the service.	C
location	location of the target, if obtained successfully.	C

The LI_X2 header (as per clause 5.3.2) of the LALSReport record presented in Table 7.3.1.4-1, shall contain the correlation ID (if provided) from a respective LI_T2 ActivationTask message.

7.3.1.5 Generation of IRI over LI_HI2

The LALSReport payload, defined in clause 7.3.1.4, shall be used as the payload of the respective LALSReport record, no payload mediation is required.

NOTE: In some specific scenarios the amount of LALS reports data may overload the LI-HI2 and/or LI_X2 interfaces. To prevent the overload, a flow control for LALS triggered location reports may be implemented in MDF and/or LI-LCS client, e.g. by limiting the frequency of the reports for individual targets.

7.3.2 Cell database information reporting

7.3.2.1 General description

When the location information present within an xIRI message includes the cell identity, the MDF2 that receives the xIRI message may retrieve the supplemental information for that cell-site from a CSP Database and deliver the same to the LEMF either within the location field of the IRI message generated from the received xIRI message or in a separate IRI message referred to as Cell Site Report.

For each intercept, if the MDF2 reports the Cell Site Supplemental information, then it shall provide the Cell Site Supplementation information at least on initial reference of a cell identity and when any information in the Cell Site Supplementation information is changed.

The Cell Site Supplementation Information Record is sent as a part of the location field of an IRI message.

7.3.2.2 Generation Cell Site Report IRI over LI_HI2

The MDF2 uses MDFCellSiteReport record to send the Cell Site Supplemental information to the LEMF over the LI_HI2 interface, when it is not able to retrieve the Cell Site Supplemental Information Record from the CSP database in time and when it sends the IRI message that would otherwise have carried the Cell Site Supplemental Information Record.

Table 7.3.2.2-1 identifies the data sent in the MDFCellSiteReport record over the LI_HI2 interface.

Table 7.3.2.2-1: Payload of MDFCellSiteReport

Field name	Description	M/C/O
location	Location information which contains the Cell Site Supplemental information	M

Annex A (normative): Structure of the Internal Interface

```
TS33128Payloads
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) threeGPP(4)
ts33128(19) r15(15) version0(0)}

DEFINITIONS IMPLICIT TAGS EXTENSIBILITY IMPLIED ::=

BEGIN

-- =============
-- Relative OIDs
-- =============

xIRIPayloadOID RELATIVE-OID ::= {threeGPP(4) ts33128(19) r15(15) version0(0) xIRI(1)}
xCCPayloadOID RELATIVE-OID ::= {threeGPP(4) ts33128(19) r15(15) version0(0) xCC(2)}

iRIPayloadOID RELATIVE-OID ::= {threeGPP(4) ts33128(19) r15(15) version0(0) iRI(3)}
cCPayloadOID RELATIVE-OID ::= {threeGPP(4) ts33128(19) r15(15) version0(0) cC(4)}

lINotificationPayloadOID RELATIVE-OID ::= {threeGPP(4) ts33128(19) r15(15) version0(0)
lINotification(5)}

-- ===============
-- X2 xIRI payload
-- ===============

XIRIPayload ::= SEQUENCE
{
    relativeOID         [1] RELATIVE-OID,
    event               [2] XIRIEvent
}

XIRIEvent ::= CHOICE
{
    -- Access and mobility related events, see clause 6.2.2
    registration                                        [1] AMFRegistration,
    deregistration                                      [2] AMFDeregistration,
    locationUpdate                                      [3] AMFLocationUpdate,
    startOfInterceptionWithRegisteredUE                 [4] AMFStartOfInterceptionWithRegisteredUE,
    unsuccessfulAMProcedure                             [5] AMFUnsuccessfulProcedure,

    -- PDU session-related events, see clause 6.2.3
    pDUSessionEstablishment                             [6] SMFPDUSessionEstablishment,
    pDUSessionModification                              [7] SMFPDUSessionModification,
    pDUSessionRelease                                   [8] SMFPDUSessionRelease,
    startOfInterceptionWithEstablishedPDUSession        [9]
SMFStartOfInterceptionWithEstablishedPDUSession,
    unsuccessfulSMProcedure                             [10] SMFUnsuccessfulProcedure,

    -- Subscriber-management related events, see clause 7.2.2
    servingSystemMessage                                [11] UDMServingSystemMessage,

    -- SMS-related events, see clause 6.2.5
    sMSMessage                                          [12] SMSMessage,

    -- LALS-related events, see clause 7.3.3
    lALSReport                                          [13] LALSReport,

    -- PDHR/PDSR-related events, see clause 6.2.3.4.1
    pDHeaderReport                                      [14] PDHeaderReport,
    pDSummaryReport                                     [15] PDSummaryReport
}

-- ==============
-- X3 xCC payload
-- ==============

-- No explicit payload required in release 15, see clause 6.2.3.5

-- ===============
-- HI2 IRI payload
-- ===============
```

```
IRIPayload ::= SEQUENCE
{
    relativeOID         [1] RELATIVE-OID,
    event               [2] IRIEvent,
    targetIdentifiers   [3] SEQUENCE OF IRITargetIdentifier OPTIONAL
}

IRIEvent ::= CHOICE
{
    -- Registration-related events, see clause 6.2.2
    registration                                        [1] AMFRegistration,
    deregistration                                      [2] AMFDeregistration,
    locationUpdate                                      [3] AMFLocationUpdate,
    startOfInterceptionWithRegisteredUE                 [4] AMFStartOfInterceptionWithRegisteredUE,
    unsuccessfulRegistrationProcedure                   [5] AMFUnsuccessfulProcedure,

    -- PDU session-related events, see clause 6.2.3
    pDUSessionEstablishment                             [6] SMFPDUSessionEstablishment,
    pDUSessionModification                              [7] SMFPDUSessionModification,
    pDUSessionRelease                                   [8] SMFPDUSessionRelease,
    startOfInterceptionWithEstablishedPDUSession        [9]
SMFStartOfInterceptionWithEstablishedPDUSession,
    unsuccessfulSessionProcedure                        [10] SMFUnsuccessfulProcedure,

    -- Subscriber-management related events, see clause 7.2.2
    servingSystemMessage                                [11] UDMServingSystemMessage,

    -- SMS-related events, see clause 6.2.5
    sMSMessage                                          [12] SMSMessage,

    -- LALS-related events, see clause 7.3.3
    lALSReport                                          [13] LALSReport,

    -- PDHR/PDSR-related events, see clause 6.2.3.4.1
    pDHeaderReport                                      [14] PDHeaderReport,
    pDSummaryReport                                     [15] PDSummaryReport,

    -- MDF-related events, see clause 7.3.4
    mDFCellSiteReport                                   [16] MDFCellSiteReport
}

IRITargetIdentifier ::= SEQUENCE
{
    identifier                                          [1] TargetIdentifier,
    provenance                                          [2] TargetIdentifierProvenance OPTIONAL
}

-- ==============
-- HI3 CC payload
-- ==============

CCPayload ::= SEQUENCE
{
    relativeOID         [1] RELATIVE-OID,
    pDU                 [2] CCPDU
}

CCPDU ::= CHOICE
{
    uPFCCPDU            [1] UPFCCPDU
}

-- ============================
-- HI4 LI notification payload
-- ============================

LINotificationPayload ::= SEQUENCE
{
    relativeOID         [1] RELATIVE-OID,
    notification        [2] LINotificationMessage
}

LINotificationMessage ::= CHOICE
{
    lINotification      [1] LINotification
}

-- ==================
```

```
-- 5G AMF definitions
-- ==================

-- See clause 6.2.2.2.2 for details of this structure
AMFRegistration ::= SEQUENCE
{
    registrationType            [1] AMFRegistrationType,
    registrationResult          [2] AMFRegistrationResult,
    slice                       [3] Slice OPTIONAL,
    sUPI                        [4] SUPI,
    sUCI                        [5] SUCI OPTIONAL,
    pEI                         [6] PEI OPTIONAL,
    gPSI                        [7] GPSI OPTIONAL,
    gUTI                        [8] FiveGGUTI,
    location                    [9] Location OPTIONAL,
    non3GPPAccessEndpoint       [10] UEEndpointAddress OPTIONAL
}

-- See clause 6.2.2.2.3 for details of this structure
AMFDeregistration ::= SEQUENCE
{
    deregistrationDirection     [1] AMFDirection,
    accessType                  [2] AccessType,
    sUPI                        [3] SUPI OPTIONAL,
    sUCI                        [4] SUCI OPTIONAL,
    pEI                         [5] PEI OPTIONAL,
    gPSI                        [6] GPSI OPTIONAL,
    gUTI                        [7] FiveGGUTI OPTIONAL,
    cause                       [8] FiveGMMCause OPTIONAL,
    location                    [9] Location OPTIONAL
}

-- See clause 6.2.2.2.4 for details of this structure
AMFLocationUpdate ::= SEQUENCE
{
    sUPI                        [1] SUPI,
    sUCI                        [2] SUCI OPTIONAL,
    pEI                         [3] PEI OPTIONAL,
    gPSI                        [4] GPSI OPTIONAL,
    gUTI                        [5] FiveGGUTI OPTIONAL,
    location                    [6] Location
}

-- See clause 6.2.2.2.5 for details of this structure
AMFStartOfInterceptionWithRegisteredUE ::= SEQUENCE
{
    registrationResult          [1] AMFRegistrationResult,
    registrationType            [2] AMFRegistrationType OPTIONAL,
    slice                       [3] Slice OPTIONAL,
    sUPI                        [4] SUPI,
    sUCI                        [5] SUCI OPTIONAL,
    pEI                         [6] PEI OPTIONAL,
    gPSI                        [7] GPSI OPTIONAL,
    gUTI                        [8] FiveGGUTI,
    location                    [9] Location OPTIONAL,
    non3GPPAccessEndpoint       [10] UEEndpointAddress OPTIONAL,
    timeOfRegistration          [11] Timestamp OPTIONAL
}

-- See clause 6.2.2.2.6 for details of this structure
AMFUnsuccessfulProcedure ::= SEQUENCE
{
    failedProcedureType         [1] AMFFailedProcedureType,
    failureCause                [2] AMFFailureCause,
    requestedSlice              [3] NSSAI OPTIONAL,
    sUPI                        [4] SUPI OPTIONAL,
    sUCI                        [5] SUCI OPTIONAL,
    pEI                         [6] PEI OPTIONAL,
    gPSI                        [7] GPSI OPTIONAL,
    gUTI                        [8] FiveGGUTI OPTIONAL,
    location                    [9] Location OPTIONAL
}

-- =================
-- 5G AMF parameters
-- =================

AMFID ::= SEQUENCE
```

```
{
    aMFRegionID [1] AMFRegionID,
    aMFSetID    [2] AMFSetID,
    aMFPointer  [3] AMFPointer
}

AMFDirection ::= ENUMERATED
{
    networkInitiated(1),
    uEInitiated(2)
}

AMFFailedProcedureType ::= ENUMERATED
{
    registration(1),
    sMS(2),
    pDUSessionEstablishment(3)
}

AMFFailureCause ::= CHOICE
{
    fiveGMMCause        [1] FiveGMMCause,
    fiveGSMCause        [2] FiveGSMCause
}

AMFPointer ::= INTEGER (0..1023)

AMFRegistrationResult ::= ENUMERATED
{
    threeGPPAccess(1),
    nonThreeGPPAccess(2),
    threeGPPAndNonThreeGPPAccess(3)
}

AMFRegionID ::= INTEGER (0..255)

AMFRegistrationType ::= ENUMERATED
{
    initial(1),
    mobility(2),
    periodic(3),
    emergency(4)
}

AMFSetID ::= INTEGER (0..63)

-- ==================
-- 5G SMF definitions
-- ==================

-- See clause 6.2.3.2.2 for details of this structure
SMFPDUSessionEstablishment ::= SEQUENCE
{
    sUPI                        [1] SUPI OPTIONAL,
    sUPIUnauthenticated         [2] SUPIUnauthenticatedIndication OPTIONAL,
    pEI                         [3] PEI OPTIONAL,
    gPSI                        [4] GPSI OPTIONAL,
    pDUSessionID                [5] PDUSessionID,
    gTPTunnelID                 [6] FTEID,
    pDUSessionType              [7] PDUSessionType,
    sNSSAI                      [8] SNSSAI OPTIONAL,
    uEEndpoint                  [9] SEQUENCE OF UEEndpointAddress OPTIONAL,
    non3GPPAccessEndpoint       [10] UEEndpointAddress OPTIONAL,
    location                    [11] Location OPTIONAL,
    dNN                         [12] DNN,
    aMFID                       [13] AMFID OPTIONAL,
    hSMFURI                     [14] HSMFURI OPTIONAL,
    requestType                 [15] FiveGSMRequestType,
    accessType                  [16] AccessType OPTIONAL,
    rATType                     [17] RATType OPTIONAL,
    sMPDUDNRequest              [18] SMPDUDNRequest OPTIONAL
}

-- See clause 6.2.3.2.3 for details of this structure
SMFPDUSessionModification ::= SEQUENCE
{
    sUPI                        [1] SUPI OPTIONAL,
    sUPIUnauthenticated         [2] SUPIUnauthenticatedIndication OPTIONAL,
```

```
    pEI                         [3] PEI OPTIONAL,
    gPSI                        [4] GPSI OPTIONAL,
    sNSSAI                      [5] SNSSAI OPTIONAL,
    non3GPPAccessEndpoint       [6] UEEndpointAddress OPTIONAL,
    location                    [7] Location OPTIONAL,
    requestType                 [8] FiveGSMRequestType,
    accessType                  [9] AccessType OPTIONAL,
    rATType                     [10] RATType OPTIONAL
}

-- See clause 6.2.3.2.4 for details of this structure
SMFPDUSessionRelease ::= SEQUENCE
{
    sUPI                        [1] SUPI,
    pEI                         [2] PEI OPTIONAL,
    gPSI                        [3] GPSI OPTIONAL,
    pDUSessionID                [4] PDUSessionID,
    timeOfFirstPacket           [5] Timestamp OPTIONAL,
    timeOfLastPacket            [6] Timestamp OPTIONAL,
    uplinkVolume                [7] INTEGER OPTIONAL,
    downlinkVolume              [8] INTEGER OPTIONAL,
    location                    [9] Location OPTIONAL
}

-- See clause 6.2.3.2.5 for details of this structure
SMFStartOfInterceptionWithEstablishedPDUSession ::= SEQUENCE
{
    sUPI                        [1] SUPI OPTIONAL,
    sUPIUnauthenticated         [2] SUPIUnauthenticatedIndication OPTIONAL,
    pEI                         [3] PEI OPTIONAL,
    gPSI                        [4] GPSI OPTIONAL,
    pDUSessionID                [5] PDUSessionID,
    gTPTunnelID                 [6] FTEID,
    pDUSessionType              [7] PDUSessionType,
    sNSSAI                      [8] SNSSAI OPTIONAL,
    uEEndpoint                  [9] SEQUENCE OF UEEndpointAddress,
    non3GPPAccessEndpoint       [10] UEEndpointAddress OPTIONAL,
    location                    [11] Location OPTIONAL,
    dNN                         [12] DNN,
    aMFID                       [13] AMFID OPTIONAL,
    hSMFURI                     [14] HSMFURI OPTIONAL,
    requestType                 [15] FiveGSMRequestType,
    accessType                  [16] AccessType OPTIONAL,
    rATType                     [17] RATType OPTIONAL,
    sMPDUDNRequest              [18] SMPDUDNRequest OPTIONAL
}

-- See clause 6.2.3.2.6 for details of this structure
SMFUnsuccessfulProcedure ::= SEQUENCE
{
    failedProcedureType         [1] SMFFailedProcedureType,
    failureCause                [2] FiveGSMCause,
    initiator                   [3] Initiator,
    requestedSlice              [4] NSSAI OPTIONAL,
    sUPI                        [5] SUPI OPTIONAL,
    sUPIUnauthenticated         [6] SUPIUnauthenticatedIndication OPTIONAL,
    pEI                         [7] PEI OPTIONAL,
    gPSI                        [8] GPSI OPTIONAL,
    pDUSessionID                [9] PDUSessionID OPTIONAL,
    uEEndpoint                  [10] SEQUENCE OF UEEndpointAddress OPTIONAL,
    non3GPPAccessEndpoint       [11] UEEndpointAddress OPTIONAL,
    dNN                         [12] DNN OPTIONAL,
    aMFID                       [13] AMFID OPTIONAL,
    hSMFURI                     [14] HSMFURI OPTIONAL,
    requestType                 [15] FiveGSMRequestType OPTIONAL,
    accessType                  [16] AccessType OPTIONAL,
    rATType                     [17] RATType OPTIONAL,
    sMPDUDNRequest              [18] SMPDUDNRequest OPTIONAL,
    location                    [19] Location OPTIONAL
}

-- =================
-- 5G SMF parameters
-- =================

SMFFailedProcedureType ::= ENUMERATED
{
    pDUSessionEstablishment(1),
```

```
    pDUSessionModification(2),
    pDUSessionRelease(3)
}

-- =================
-- 5G UPF parameters
-- =================

UPFCCPDU ::= OCTET STRING

-- ==================
-- 5G UDM definitions
-- ==================

UDMServingSystemMessage ::= SEQUENCE
{
    sUPI                        [1] SUPI,
    pEI                         [2] PEI OPTIONAL,
    gPSI                        [3] GPSI OPTIONAL,
    gUAMI                       [4] GUAMI OPTIONAL,
    gUMMEI                      [5] GUMMEI OPTIONAL,
    pLMNID                      [6] PLMNID OPTIONAL,
    servingSystemMethod         [7] UDMServingSystemMethod
}

-- =================
-- 5G UDM parameters
-- =================

UDMServingSystemMethod ::= ENUMERATED
{
    amf3GPPAccessRegistration(0),
    amfNon3GPPAccessRegistration(1),
    unknown(2)
}

-- ===================
-- 5G SMSF definitions
-- ===================

-- See clause 6.2.5.3 for details of this structure
SMSMessage ::= SEQUENCE
{
    originatingSMSParty         [1] SMSParty,
    terminatingSMSParty         [2] SMSParty,
    direction                   [3] Direction,
    transferStatus              [4] SMSTransferStatus,
    otherMessage                [5] SMSOtherMessageIndication OPTIONAL,
    location                    [6] Location OPTIONAL,
    peerNFAddress               [7] SMSNFAddress OPTIONAL,
    peerNFType                  [8] SMSNFType OPTIONAL,
    smsTPDUData                 [9] SMSTPDUData OPTIONAL
}

-- ==================
-- 5G SMSF parameters
-- ==================

SMSParty ::= SEQUENCE
{
    sUPI        [1] SUPI OPTIONAL,
    pEI         [2] PEI OPTIONAL,
    gPSI        [3] GPSI OPTIONAL
}


SMSTransferStatus ::= ENUMERATED
{
    transferSucceeded(1),
    transferFailed(2),
    undefined(3)
}

SMSOtherMessageIndication ::= BOOLEAN

SMSNFAddress ::= CHOICE
{
    iPAddress   [1] IPAddress,
```

```
    e164Number  [2] E164Number
}

SMSNFType ::= ENUMERATED
{
    sMSGMSC(1),
    iWMSC(2),
    sMSRouter(3)
}

SMSTPDUData ::= CHOICE
{
    smsTPDU [1] SMSTPDU
}

SMSTPDU ::= OCTET STRING (SIZE(1..270))

-- ====================
-- 5G LALS definitions
-- ====================

LALSReport ::= SEQUENCE
{
    sUPI                [1] SUPI OPTIONAL,
    pEI                 [2] PEI OPTIONAL,
    gPSI                [3] GPSI OPTIONAL,
    location            [4] Location OPTIONAL
}

-- ======================
-- PDHR/PDSR definitions
-- ======================

PDHeaderReport ::= SEQUENCE
{
    pDUSessionID                [1] PDUSessionID,
    sourceIPAddress             [2] IPAddress,
    sourcePort                  [3] PortNumber OPTIONAL,
    destinationIPAddress        [4] IPAddress,
    destinationPort             [5] PortNumber OPTIONAL,
    nextLayerProtocol           [6] NextLayerProtocol,
    iPv6flowLabel               [7] IPv6FlowLabel OPTIONAL,
    direction                   [8] Direction,
    packetSize                  [9] INTEGER
}

PDSummaryReport ::= SEQUENCE
{
    pDUSessionID                [1] PDUSessionID,
    sourceIPAddress             [2] IPAddress,
    sourcePort                  [3] PortNumber OPTIONAL,
    destinationIPAddress        [4] IPAddress,
    destinationPort             [5] PortNumber OPTIONAL,
    nextLayerProtocol           [6] NextLayerProtocol,
    iPv6flowLabel               [7] IPv6FlowLabel OPTIONAL,
    direction                   [8] Direction,
    pDSRSummaryTrigger          [9] PDSRSummaryTrigger,
    firstPacketTimestamp        [10] Timestamp,
    lastPacketTimestamp         [11] Timestamp,
    packetCount                 [12] INTEGER,
    byteCount                   [13] INTEGER
}

-- ====================
-- PDHR/PDSR parameters
-- ====================

PDSRSummaryTrigger ::= ENUMERATED
{
    timerExpiry(1),
    packetCount(2),
    byteCount(3)
}

-- ============================
-- LI Notification definitions
-- ============================
```

```
LINotification ::= SEQUENCE
{
    notificationType                    [1] LINotificationType,
    appliedTargetID                     [2] TargetIdentifier OPTIONAL,
    appliedDeliveryInformation          [3] SEQUENCE OF LIAppliedDeliveryInformation OPTIONAL,
    appliedStartTime                    [4] Timestamp OPTIONAL,
    appliedEndTime                      [5] Timestamp OPTIONAL
}

-- ==========================
-- LI Notification parameters
-- ==========================

LINotificationType ::= ENUMERATED
{
    activation(1),
    deactivation(2),
    modification(3)
}

LIAppliedDeliveryInformation ::= SEQUENCE
{
    hi2DeliveryIpAddress                [1] IPAddress OPTIONAL,
    hi2DeliveryPortNumber               [2] PortNumber OPTIONAL,
    hi3DeliveryIpAddress                [3] IPAddress OPTIONAL,
    hi3DeliveryPortNumber               [4] PortNumber OPTIONAL
}

-- ===============
-- MDF definitions
-- ===============

MDFCellSiteReport ::= SEQUENCE
{
    location                            [1] Location
}

-- =================
-- Common Parameters
-- =================

AccessType ::= ENUMERATED
{
    threeGPPAccess(1),
    nonThreeGPPAccess(2),
    threeGPPandNonThreeGPPAccess(3)
}

Direction ::= ENUMERATED
{
    fromTarget(1),
    toTarget(2)
}

DNN ::= UTF8String

E164Number ::= NumericString (SIZE(1..15))

FiveGGUTI ::= SEQUENCE
{
    mCC         [1] MCC,
    mNC         [2] MNC,
    aMFRegionID [3] AMFRegionID,
    aMFSetID    [4] AMFSetID,
    aMFPointer  [5] AMFPointer,
    fiveGTMSI   [6] FiveGTMSI
}

FiveGMMCause ::= INTEGER (0..255)

FiveGSMRequestType ::= ENUMERATED
{
    initialRequest(1),
    existingPDUSession(2),
    initialEmergencyRequest(3),
    existingEmergencyPDUSession(4),
    modificationRequest(5),
    reserved(6)
```

```
}

FiveGSMCause ::= INTEGER (0..255)

FiveGTMSI ::= INTEGER (0..4294967295)

FTEID ::= SEQUENCE
{
    tEID        [1] INTEGER (0.. 4294967295),
    iPv4Address [2] IPv4Address OPTIONAL,
    iPv6Address [3] IPv6Address OPTIONAL
}

GPSI ::= CHOICE
{
    mSISDN      [1] MSISDN,
    nAI         [2] NAI
}

GUAMI ::= SEQUENCE
{
    aMFID       [1] AMFID,
    pLMNID      [2] PLMNID
}

GUMMEI ::= SEQUENCE
{
    mMEID       [1] MMEID,
    mCC         [2] MCC,
    mNC         [3] MNC
}

HomeNetworkPublicKeyID ::= OCTET STRING

HSMFURI ::= UTF8String

IMEI ::= NumericString (SIZE(14))

IMEISV ::= NumericString (SIZE(16))

IMSI ::= NumericString (SIZE(6..15))

Initiator ::= ENUMERATED
{
    uE(1),
    network(2),
    unknown(3)
}

IPAddress ::= CHOICE
{
    iPv4Address [1] IPv4Address,
    iPv6Address [2] IPv6Address
}

IPv4Address ::= OCTET STRING (SIZE(4))

IPv6Address ::= OCTET STRING (SIZE(16))

IPv6FlowLabel ::= INTEGER(0..1048575)

MACAddress ::= OCTET STRING (SIZE(6))

MCC ::= NumericString (SIZE(3))

MNC ::= NumericString (SIZE(2..3))

MMEID ::= SEQUENCE
{
    mMEGI       [1] MMEGI,
    mMEC        [2] MMEC
}

MMEC ::= NumericString

MMEGI ::= NumericString

MSISDN ::= NumericString (SIZE(1..15))
```

```
NAI ::= UTF8String

NextLayerProtocol ::= INTEGER(0..255)

NSSAI ::= SEQUENCE OF SNSSAI

PLMNID ::= SEQUENCE
{
    mcc [1] MCC,
    mnc [1] MNC
}

PDUSessionID ::= INTEGER (0..255)

PDUSessionType ::= ENUMERATED
{
    iPv4(1),
    iPv6(2),
    iPv4v6(3),
    unstructured(4),
    ethernet(5)
}

PEI ::= CHOICE
{
    iMEI        [1] IMEI,
    iMEISV      [2] IMEISV
}

PortNumber ::= INTEGER(0..65535)

ProtectionSchemeID ::= INTEGER (0..15)

RATType ::= ENUMERATED
{
    nr(1),
    eutra(2),
    wlan(3),
    virtual(4)
}

RejectedNSSAI ::= SEQUENCE OF RejectedSNSSAI

RejectedSNSSAI ::= SEQUENCE
{
    causeValue  [1] RejectedSliceCauseValue,
    sNSSAI      [2] SNSSAI
}

RejectedSliceCauseValue ::= INTEGER (0..255)

RoutingIndicator ::= INTEGER (0..9999)

SchemeOutput ::= OCTET STRING

Slice ::= SEQUENCE
{
    allowedNSSAI        [1] NSSAI OPTIONAL,
    configuredNSSAI     [2] NSSAI OPTIONAL,
    rejectedNSSAI       [3] RejectedNSSAI OPTIONAL
}

SMPDUDNRequest ::= OCTET STRING

SNSSAI ::= SEQUENCE
{
    sliceServiceType    [1] INTEGER (0..255),
    sliceDifferentiator [2] OCTET STRING (SIZE(3)) OPTIONAL
}

SUCI ::= SEQUENCE
{
    mCC                         [1] MCC,
    mNC                         [2] MNC,
    routingIndicator            [3] RoutingIndicator,
    protectionSchemeID          [4] ProtectionSchemeID,
    homeNetworkPublicKeyID      [5] HomeNetworkPublicKeyID,
```

```
    schemeOutput                [6] SchemeOutput
}

SUPI ::= CHOICE
{
    iMSI        [1] IMSI,
    nAI         [2] NAI
}

SUPIUnauthenticatedIndication ::= BOOLEAN

TargetIdentifier ::= CHOICE
{
    sUPI                [1] SUPI,
    iMSI                [2] IMSI,
    pEI                 [3] PEI,
    iMEI                [4] IMEI,
    gPSI                [5] GPSI,
    mISDN               [6] MSISDN,
    nAI                 [7] NAI,
    iPv4Address         [8] IPv4Address,
    iPv6Address         [9] IPv6Address,
    ethernetAddress     [10] MACAddress
}

TargetIdentifierProvenance ::= ENUMERATED
{
    lEAProvided(1),
    observed(2),
    matchedOn(3),
    other(4)
}

Timestamp ::= GeneralizedTime

UEEndpointAddress ::= CHOICE
{
    iPv4Address         [1] IPv4Address,
    iPv6Address         [2] IPv6Address,
    ethernetAddress     [3] MACAddress
}

-- ====================
-- Location parameters
-- ====================

Location ::= SEQUENCE
{
    locationInfo                [1] LocationInfo OPTIONAL,
    positioningInfo             [2] PositioningInfo OPTIONAL,
    locationPresenceReport      [3] LocationPresenceReport OPTIONAL
}

CellSiteInformation ::= SEQUENCE
{
    geographicalCoordinates     [1] GeographicalCoordinates,
    azimuth                     [2] INTEGER (0..359) OPTIONAL,
    operatorSpecificInformation [3] UTF8String OPTIONAL
}

-- TS 29.518 [22], clause 6.4.6.2.6
LocationInfo ::= SEQUENCE
{
    userLocation                [1] UserLocation OPTIONAL,
    currentLoc                  [2] BOOLEAN OPTIONAL,
    geoInfo                     [3] GeographicArea OPTIONAL,
    ratType                     [4] RATType OPTIONAL,
    timezone                    [5] TimeZone OPTIONAL
}

-- TS 29.571 [17], clause 5.4.4.7
UserLocation ::= SEQUENCE
{
    eutraLocation               [1] EutraLocation OPTIONAL,
    nrLocation                  [2] NrLocation OPTIONAL,
    n3gaLocation                [3] N3gaLocation OPTIONAL
}
```

```
-- TS 29.571 [17], clause 5.4.4.8
EutraLocation ::= SEQUENCE
{
    tai                         [1] Tai,
    ecgi                        [2] Ecgi,
    ageOfLocatonInfo            [3] INTEGER OPTIONAL,
    ueLocationTimestamp         [4] Timestamp OPTIONAL,
    geographicalInformation     [5] UTF8String OPTIONAL,
    geodeticInformation         [6] UTF8String OPTIONAL,
    globalNgenbId               [7] GlobalRanNodeId OPTIONAL,
    cellSiteinformation         [8] CellSiteInformation OPTIONAL
}

-- TS 29.571 [17], clause 5.4.4.9
NrLocation ::= SEQUENCE
{
    tai                         [1] Tai,
    ncgi                        [2] Ncgi,
    ageOfLocatonInfo            [3] INTEGER OPTIONAL,
    ueLocationTimestamp         [4] Timestamp OPTIONAL,
    geographicalInformation     [5] UTF8String OPTIONAL,
    geodeticInformation         [6] UTF8String OPTIONAL,
    globalGnbId                 [7] GlobalRanNodeId OPTIONAL,
    cellSiteinformation         [8] CellSiteInformation OPTIONAL
}

-- TS 29.571 [17], clause 5.4.4.10
N3gaLocation ::= SEQUENCE
{
    tai                         [1] Tai OPTIONAL,
    n3IwfId                     [2] N3IwfIdNgap OPTIONAL,
    ueIpAddr                    [3] IpAddr OPTIONAL,
    portNumber                  [5] INTEGER OPTIONAL
}

-- TS 38.413 [23], clause 9.3.2.4
IpAddr ::= SEQUENCE
{
    ipv4Addr                    [1] IPv4Address OPTIONAL,
    ipv6Addr                    [2] IPv6Address OPTIONAL
}

-- TS 29.571 [17], clause 5.4.4.28
GlobalRanNodeId ::= SEQUENCE
{
    plmnId                      [1] PlmnId,
    anNodeId                    [2] CHOICE
    {
        n3IwfId [1] N3IwfIdSbi,
        gNbId   [2] GNbId,
        ngeNbId [3] NgeNbId
    }
}

-- TS 38.413 [23], clause 9.3.1.6
GNbId ::= BIT STRING(SIZE(22..32))

-- TS 29.571 [17], clause 5.4.4.4
Tai ::= SEQUENCE
{
    plmnId                      [1] PlmnId,
    tac                         [2] Tac
}

-- TS 29.571 [17], clause 5.4.4.5
Ecgi ::= SEQUENCE
{
    plmnId                      [1] PlmnId,
    eutraCellId                 [2] EutraCellId
}

-- TS 29.571 [17], clause 5.4.4.6
Ncgi ::= SEQUENCE
{
    plmnId                      [1] PlmnId,
    nrCellId                    [2] NrCellId
}
```

```
-- TS 38.413 [23], clause 9.3.3.5
PlmnId ::= OCTET STRING (SIZE(3))

-- TS 38.413 [23], clause 9.3.1.57
N3IwfIdNgap ::= BIT STRING (SIZE(16))

-- TS 29.571 [17], clause 5.4.4.28
N3IwfIdSbi ::= UTF8String

-- TS 29.571 [17], table 5.4.2-1
Tac ::= OCTET STRING (SIZE(2..3))

-- TS 38.413 [23], clause 9.3.1.9
EutraCellId ::= BIT STRING (SIZE(28))

-- TS 38.413 [23], clause 9.3.1.7
NrCellId ::= BIT STRING (SIZE(36))

-- TS 38.413 [23], clause 9.3.1.8
NgeNbId ::= CHOICE
{
    macroNgeNbId               [1] BIT STRING (SIZE(20)),
    shortMacroNgeNbId          [2] BIT STRING (SIZE(18)),
    longMacroNgeNbId           [3] BIT STRING (SIZE(21))
}

-- TS 29.518 [22], clause 6.4.6.2.3
PositioningInfo ::= SEQUENCE
{
    positionInfo               [1] LocationData OPTIONAL,
    rawMlpResponse             [2] RawMlpResponse OPTIONAL
}

RawMlpResponse ::= CHOICE
{
    -- The following parameter contains a copy of unparsed XML code of the
    -- MLP response message, i.e. the entire XML document containing
    -- a <slia> (described in OMA-TS-MLP-V3-4-20150512-A [20], clause 5.2.3.2.2) or
    -- a <slirep> (described in OMA-TS-MLP-V3-4-20150512-A [20], clause 5.2.3.2.3) MLP message.
    mlpPositionData            [1] UTF8String,
    -- OMA MLP result id, defined in OMA-TS-MLP-V3-4-20150512-A [20], Clause 5.4
    mlpErrorCode               [2] INTEGER (1..699)
}

-- TS 29.572 [24], clause 6.1.6.2.3
LocationData ::= SEQUENCE
{
    locationEstimate           [1] GeographicArea,
    accuracyFulfilmentIndicator [2] AccuracyFulfilmentIndicator OPTIONAL,
    ageOfLocationEstimate      [3] AgeOfLocationEstimate OPTIONAL,
    velocityEstimate           [4] VelocityEstimate OPTIONAL,
    civicAddress               [5] CivicAddress OPTIONAL,
    positioningDataList        [6] SET OF PositioningMethodAndUsage OPTIONAL,
    gnssPositioningDataList    [7] SET OF GnnsPositioningMethodAndUsage OPTIONAL,
    ecgi                       [8] Ecgi OPTIONAL,
    ncgi                       [9] Ncgi OPTIONAL,
    altitude                   [10] Altitude OPTIONAL,
    barometricPressure         [11] BarometricPressure OPTIONAL
}

-- TS 29.518 [22], clause 6.2.6.2.5
LocationPresenceReport ::= SEQUENCE
{
    type                       [1] AmfEventType,
    timeStamp                  [2] Timestamp,
    areaList                   [3] SET OF AmfEventArea OPTIONAL,
    timezone                   [4] TimeZone OPTIONAL,
    accessTypes                [5] SET OF AccessType OPTIONAL,
    rmInfoList                 [6] SET OF RmInfo OPTIONAL,
    cmInfoList                 [7] SET OF CmInfo OPTIONAL,
    reachability               [8] UeReachability OPTIONAL,
    location                   [9] UserLocation OPTIONAL
}

-- TS 29.518 [22], clause 6.2.6.3.3
AmfEventType ::= ENUMERATED
{
    locationReport(1),
```

```
    presenceInAoiReport(2)
}

-- TS 29.518 [22], clause 6.2.6.2.16
AmfEventArea ::= SEQUENCE
{
    presenceInfo                [1] PresenceInfo OPTIONAL,
    ladnInfo                    [2] LadnInfo OPTIONAL
}

-- TS 29.571 [17], clause 5.4.4.27
PresenceInfo ::= SEQUENCE
{
    presenceState               [1] PresenceState OPTIONAL,
    trackingAreaList            [2] SET OF Tai OPTIONAL,
    ecgiList                    [3] SET OF Ecgi OPTIONAL,
    ncgiList                    [4] SET OF Ncgi OPTIONAL,
    globalRanNodeIdList         [5] SET OF GlobalRanNodeId OPTIONAL
}

-- TS 29.518 [22], clause 6.2.6.2.17
LadnInfo ::= SEQUENCE
{
    ladn                        [1] UTF8String,
    presence                    [2] PresenceState OPTIONAL
}

-- TS 29.571 [17], clause 5.4.3.20
PresenceState ::= ENUMERATED
{
    inArea(1),
    outOfArea(2),
    unknown(3),
    inactive(4)
}

-- TS 29.518 [22], clause 6.2.6.2.8
RmInfo ::= SEQUENCE
{
    rmState                     [1] RmState,
    accessType                  [2] AccessType
}

-- TS 29.518 [22], clause 6.2.6.2.9
CmInfo ::= SEQUENCE
{
    cmState                     [1] CmState,
    accessType                  [2] AccessType
}

-- TS 29.518 [22], clause 6.2.6.3.7
UeReachability ::= ENUMERATED
{
    unreachable(1),
    reachable(2),
    regulatoryOnly(3)
}

-- TS 29.518 [22], clause 6.2.6.3.9
RmState ::= ENUMERATED
{
    registered(1),
    deregistered(2)
}

-- TS 29.518 [22], clause 6.2.6.3.10
CmState ::= ENUMERATED
{
    idle(1),
    connected(2)
}

-- TS 29.572 [24], clause 6.1.6.2.5
GeographicArea ::= CHOICE
{
    point                       [1] Point,
    pointUncertaintyCircle      [2] PointUncertaintyCircle,
    pointUncertaintyEllipse     [3] PointUncertaintyEllipse,
```

```
    polygon                     [4] Polygon,
    pointAltitude               [5] PointAltitude,
    pointAltitudeUncertainty    [6] PointAltitudeUncertainty,
    ellipsoidArc                [7] EllipsoidArc
}

-- TS 29.572 [24], clause 6.1.6.3.12
AccuracyFulfilmentIndicator ::= ENUMERATED
{
    requestedAccuracyFulfilled(1),
    requestedAccuracyNotFulfilled(2)
}

-- TS 29.572 [24], clause
VelocityEstimate ::= CHOICE
{
    horVelocity                         [1] HorizontalVelocity,
    horWithVertVelocity                 [2] HorizontalWithVerticalVelocity,
    horVelocityWithUncertainty          [3] HorizontalVelocityWithUncertainty,
    horWithVertVelocityAndUncertainty   [4] HorizontalWithVerticalVelocityAndUncertainty
}

-- TS 29.572 [24], clause 6.1.6.2.14
CivicAddress ::= SEQUENCE
{
    country                             [1] UTF8String,
    a1                                  [2] UTF8String OPTIONAL,
    a2                                  [3] UTF8String OPTIONAL,
    a3                                  [4] UTF8String OPTIONAL,
    a4                                  [5] UTF8String OPTIONAL,
    a5                                  [6] UTF8String OPTIONAL,
    a6                                  [7] UTF8String OPTIONAL,
    prd                                 [8] UTF8String OPTIONAL,
    pod                                 [9] UTF8String OPTIONAL,
    sts                                 [10] UTF8String OPTIONAL,
    hno                                 [11] UTF8String OPTIONAL,
    hns                                 [12] UTF8String OPTIONAL,
    lmk                                 [13] UTF8String OPTIONAL,
    loc                                 [14] UTF8String OPTIONAL,
    nam                                 [15] UTF8String OPTIONAL,
    pc                                  [16] UTF8String OPTIONAL,
    bld                                 [17] UTF8String OPTIONAL,
    unit                                [18] UTF8String OPTIONAL,
    flr                                 [19] UTF8String OPTIONAL,
    room                                [20] UTF8String OPTIONAL,
    plc                                 [21] UTF8String OPTIONAL,
    pcn                                 [22] UTF8String OPTIONAL,
    pobox                               [23] UTF8String OPTIONAL,
    addcode                             [24] UTF8String OPTIONAL,
    seat                                [25] UTF8String OPTIONAL,
    rd                                  [26] UTF8String OPTIONAL,
    rdsec                               [27] UTF8String OPTIONAL,
    rdbr                                [28] UTF8String OPTIONAL,
    rdsubbr                             [29] UTF8String OPTIONAL
}

-- TS 29.572 [24], clause 6.1.6.2.15
PositioningMethodAndUsage ::= SEQUENCE
{
    method                              [1] PositioningMethod,
    mode                                [2] PositioningMode,
    usage                               [3] Usage
}

-- TS 29.572 [24], clause 6.1.6.2.16
GnnsPositioningMethodAndUsage ::= SEQUENCE
{
    mode                                [1] PositioningMode,
    gnss                                [2] GnssId,
    usage                               [3] Usage
}

-- TS 29.572 [24], clause 6.1.6.2.6
Point ::= SEQUENCE
{
    geographicalCoordinates             [1] GeographicalCoordinates
}
```

```
-- TS 29.572 [24], clause 6.1.6.2.7
PointUncertaintyCircle ::= SEQUENCE
{
    geographicalCoordinates             [1] GeographicalCoordinates,
    uncertainty                         [2] Uncertainty
}

-- TS 29.572 [24], clause 6.1.6.2.8
PointUncertaintyEllipse ::= SEQUENCE
{
    geographicalCoordinates             [1] GeographicalCoordinates,
    uncertainty                         [2] UncertaintyEllipse,
    confidence                          [3] Confidence
}

-- TS 29.572 [24], clause 6.1.6.2.9
Polygon ::= SEQUENCE
{
    pointList                           [1] SET SIZE (3..15) OF GeographicalCoordinates
}

-- TS 29.572 [24], clause 6.1.6.2.10
PointAltitude ::= SEQUENCE
{
    point                               [1] GeographicalCoordinates,
    altitude                            [2] Altitude
}

-- TS 29.572 [24], clause 6.1.6.2.11
PointAltitudeUncertainty ::= SEQUENCE
{
    point                               [1] GeographicalCoordinates,
    altitude                            [2] Altitude,
    uncertaintyEllipse                  [3] UncertaintyEllipse,
    uncertaintyAltitude                 [4] Uncertainty,
    confidence                          [5] Confidence
}

-- TS 29.572 [24], clause 6.1.6.2.12
EllipsoidArc ::= SEQUENCE
{
    point                               [1] GeographicalCoordinates,
    innerRadius                         [2] InnerRadius,
    uncertaintyRadius                   [3] Uncertainty,
    offsetAngle                         [4] Angle,
    includedAngle                       [5] Angle,
    confidence                          [6] Confidence
}

-- TS 29.572 [24], clause 6.1.6.2.4
GeographicalCoordinates ::= SEQUENCE
{
    latitude                            [1] UTF8String,
    longitude                           [2] UTF8String
}

-- TS 29.572 [24], clause 6.1.6.2.22
UncertaintyEllipse ::= SEQUENCE
{
    semiMajor                           [1] Uncertainty,
    semiMinor                           [2] Uncertainty,
    orientationMajor                    [3] Orientation
}

-- TS 29.572 [24], clause 6.1.6.2.18
HorizontalVelocity ::= SEQUENCE
{
    hSpeed                              [1] HorizontalSpeed,
    bearing                             [2] Angle
}

-- TS 29.572 [24], clause 6.1.6.2.19
HorizontalWithVerticalVelocity ::= SEQUENCE
{
    hSpeed                              [1] HorizontalSpeed,
    bearing                             [2] Angle,
    vSpeed                              [3] VerticalSpeed,
    vDirection                          [4] VerticalDirection
```

```
}

-- TS 29.572 [24], clause 6.1.6.2.20
HorizontalVelocityWithUncertainty ::= SEQUENCE
{
    hSpeed                              [1] HorizontalSpeed,
    bearing                             [2] Angle,
    uncertainty                         [3] SpeedUncertainty
}

-- TS 29.572 [24], clause 6.1.6.2.21
HorizontalWithVerticalVelocityAndUncertainty ::= SEQUENCE
{
    hspeed                              [1] HorizontalSpeed,
    bearing                             [2] Angle,
    vSpeed                              [3] VerticalSpeed,
    vDirection                          [4] VerticalDirection,
    hUncertainty                        [5] SpeedUncertainty,
    vUncertainty                        [6] SpeedUncertainty
}

--The following types are described in TS 29.572 [24], table 6.1.6.3.2-1
Altitude ::= UTF8String
Angle ::= INTEGER (0..360)
Uncertainty ::= INTEGER (0..127)
Orientation ::= INTEGER (0..180)
Confidence ::= INTEGER (0..100)
InnerRadius ::= INTEGER (0..65535)
AgeOfLocationEstimate ::= INTEGER (0..32767)
HorizontalSpeed ::= UTF8String
VerticalSpeed ::= UTF8String
SpeedUncertainty ::= UTF8String
BarometricPressure ::= INTEGER (30000..155000)

-- TS 29.572 [24], clause 6.1.6.3.13
VerticalDirection ::= ENUMERATED
{
    upward(1),
    downward(2)
}

-- TS 29.572 [24], clause 6.1.6.3.6
PositioningMethod ::= ENUMERATED
{
    cellid(1),
    ecid(2),
    otdoa(3),
    barometricPresure(4),
    wlan(5),
    bluetooth(6),
    mbs(7)
}

-- TS 29.572 [24], clause 6.1.6.3.7
PositioningMode ::= ENUMERATED
{
    ueBased(1),
    ueAssisted(2),
    conventional(3)
}

-- TS 29.572 [24], clause 6.1.6.3.8
GnssId ::= ENUMERATED
{
    gps(1),
    galileo(2),
    sbas(3),
    modernizedGps(4),
    qzss(5),
    glonass(6)
}

-- TS 29.572 [24], clause 6.1.6.3.9
Usage ::= ENUMERATED
{
    unsuccess(1),
    successResultsNotUsed(2),
    successResultsUsedToVerifyLocation(3),
```

```
    successResultsUsedToGenerateLocation(4),
    successMethodNotDetermined(5)
}

-- TS 29.571 [17], table 5.2.2-1
TimeZone ::= UTF8String

END
```

Annex B (normative): LI Notification

Based on clause 5.6 of the present document, this clause defines a system of management notification of LI system with the LI_HI4 interface.

The LI_HI4 interface shall be used to transport specific LI service O&M information (referred to as LI Notification) from the CSP to the LEMF. The individual parameters of the LI Notification message shall be coded using ASN.1 and the basic encoding rules (BER). The delivery of LI Notification shall be performed directly using the same mechanism as used for delivery of IRI messages over LI_HI2 and CC over LI_HI3.

The LI Notification shall be used to send electronic notification to the LEMF in the following cases:

1) after the activation of lawful interception;

2) after the deactivation of lawful interception;

3) after the modification of an active lawful interception.

Table B.1-1: LINotification message

Field name	Description	M/C/O
notificationType	Information on the type of notification: activation, deactivation or modification	M
deliveryInformation	Delivery Information which has been decided by the LEA in terms of delivery numbers, IP addresses for LI_HI2 and LI_HI3	O
appliedTargetID	Target Identifier applied in the ADMF for the warrant	O
appliedStartTime	Start time applied to the ADMF for the warrant	C
appliedEndTime	End time applied to the ADMF for the warrant	C

Conditional parameters shall be set as follows:

LI Activation Notification		
Field name	**Description**	**M/C/O**
notificationType	Activation	M
appliedStartTime	Always present and represents: The Start Date/Time in the warrant or, The Date/Time of the CSP activation in the ADMF or, The scheduled future Start Date/Time.	C
appliedEndTime	Absence means the interception has been activated with no predefined End Date/Time. Presence means the End time is scheduled to be applied at that (future) time.	C

LI Modification Notification		
Field name	**Description**	**M/C/O**
notificationType	Modification	M
appliedStartTime	Present and provides the new Start Date/Time if modified by the LI Modification command	C
appliedEndTime	Present and provides the new End Date/Time if modified by the LI Modification command	C

LI Deactivation Notification		
Field name	**Description**	**M/C/O**
notificationType	Deactivation	M
appliedStartTime	Absent	C
appliedEndTime	Present and provides the actual End Date/Time, e.g. timed stop as per initial warrant or as per new warrant, or as pre-emptive audited stop from the LEA, or major LI failure.	C

The individual notifications parameters shall be sent to the LEMF as soon as possible with the lowest latency at least once (if available).

The MDF2/3 will deliver the LINotification message to LEMF.

Annex C (normative): XSD Schema for LI_X1 extensions

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns="urn:3GPP:ns:li:3GPPX1Extensions"
           targetNamespace="urn:3GPP:ns:li:3GPPX1Extensions"
           elementFormDefault="qualified">

  <xs:complexType name="X1Extensions">
    <xs:sequence>
      <xs:element name="Extension" type="X1Extension" minOccurs="1"
maxOccurs="unbounded"></xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="X1Extension">
    <xs:choice>
      <xs:element name="LALSLILCSTargetProvisioning"
type="LALSLILCSTargetProvisioningExtensions"></xs:element>
      <xs:element name="LALSLTFProvisioning"
type="LALSLTFProvisioningExtensions"></xs:element>
      <xs:element name="HeaderReporting" type="PDHRReportingExtensions"></xs:element>
      <xs:element name="ServiceScopingOptions" type="ServiceScopingOptions"></xs:element>
    </xs:choice>
  </xs:complexType>

  <xs:complexType name="LALSLILCSTargetProvisioningExtensions">
    <xs:sequence>
      <xs:element name="PositioningServiceType" type="PositioningServiceType"></xs:element>
      <xs:element name="PositioningPeriodicity" type="PositioningPeriodicity"
minOccurs="0"></xs:element>
      <xs:element name="PositioningParameters" type="PositioningParameters"
minOccurs="0"></xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="PositioningServiceType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="Immediate"></xs:enumeration>
      <xs:enumeration value="Periodic"></xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="PositioningPeriodicity">
    <xs:restriction base="xs:nonNegativeInteger">
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="PositioningParameters">
    <xs:sequence>
      <xs:element name="RequestedLocationType" type="RequestedLocationType"
minOccurs="0"></xs:element>
      <xs:element name="RequestedResponseType" type="RequestedResponseType"
minOccurs="0"></xs:element>
      <xs:element name="MaxLocationAge" type="xs:nonNegativeInteger"
minOccurs="0"></xs:element>
      <xs:element name="ResponseTimingRequired" type="ResponseTimingRequired"
minOccurs="0"></xs:element>
      <xs:element name="ResponseTimer" type="xs:nonNegativeInteger"
minOccurs="0"></xs:element>
      <xs:element name="HorizontalAccuracy" type="NumberWithQOSClass"
minOccurs="0"></xs:element>
```

```
      <xs:element name="AltitudeAccuracy" type="NumberWithQOSClass"
minOccurs="0"></xs:element>
      <xs:element name="MotionStateRequest" type="EmptyElement" minOccurs="0"></xs:element>
    </xs:sequence>
  </xs:complexType>
  <xs:simpleType name="RequestedLocationType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="CURRENT"></xs:enumeration>
      <xs:enumeration value="CURRENT_OR_LAST"></xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="RequestedResponseType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="SYNC"></xs:enumeration>
      <xs:enumeration value="ASYNC"></xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="ResponseTimingRequired">
    <xs:restriction base="xs:string">
      <xs:enumeration value="NO_DELAY"></xs:enumeration>
      <xs:enumeration value="LOW_DELAY"></xs:enumeration>
      <xs:enumeration value="DELAY_TOL"></xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="NumberWithQOSClass">
    <xs:simpleContent>
      <xs:extension base="xs:nonNegativeInteger">
        <xs:attribute name="qos_class" type="QOSClass"></xs:attribute>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:simpleType name="QOSClass">
    <xs:restriction base="xs:string">
      <xs:enumeration value="ASSURED"></xs:enumeration>
      <xs:enumeration value="BEST_EFFORT"></xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="EmptyElement">
    <xs:restriction base="xs:string">
      <xs:enumeration value=""></xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="LALSLTFProvisioningExtensions">
    <xs:sequence>
      <xs:element name="LILCSClientAddress" type="LILCSClientIPAddress"></xs:element>
      <xs:element name="PositioningParameters" type="PositioningParameters"
minOccurs="0"></xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="LILCSClientIPAddress">
    <xs:sequence>
      <xs:choice>
        <xs:element name="IPv4Address" type="IPv4Address"/>
        <xs:element name="IPv6Address" type="IPv6Address"/>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
```

```
  <xs:simpleType name="IPv4Address">
    <xs:restriction base="xs:token">
      <xs:pattern value="((25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])\.){3}(25[0-5]|2[0-4][0-
9]|[01]?[0-9]?[0-9])"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="IPv6Address">
    <xs:restriction base="xs:token">
      <xs:pattern value="([0-9a-f]{4}:){7}([0-9a-f]{4})"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="PDHRReportingExtensions">
    <xs:sequence>
      <xs:element name="PDHType" type="PDHType"></xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="PDHType">
    <xs:choice>
      <xs:element name="PDHR" type="EmptyElement"></xs:element>
      <xs:element name="PDSR" type="PDSRParameters"></xs:element>
    </xs:choice>
  </xs:complexType>

  <xs:complexType name="PDSRParameters">
    <xs:sequence>
      <xs:element name="PDSRTriggerType" type="PDSRTriggerType"></xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="PDSRTriggerType">
    <xs:choice>
      <xs:element name="TimerExpiry" type="TimerExpiryInSeconds"></xs:element>
      <xs:element name="PacketCount" type="xs:nonNegativeInteger"></xs:element>
      <xs:element name="ByteCount" type="xs:nonNegativeInteger"></xs:element>
    </xs:choice>
  </xs:complexType>

  <xs:simpleType name="TimerExpiryInSeconds">
    <xs:restriction base="xs:nonNegativeInteger">
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="ServiceScopingOptions">
    <xs:sequence>
      <xs:element name="ServiceTypeOptions" type="ServiceTypeOptions"></xs:element>
      <xs:element name="LocationInformationOptions"
type="LocationInformationOptions"></xs:element>
      <xs:element name="NonHPLMNRANTrafficDelivery"
type="ServiceScopeOptionValue"></xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ServiceTypeOptions">
    <xs:sequence>
      <xs:element name="Voice" type="ServiceScopeOptionValue"></xs:element>
      <xs:element name="Data" type="ServiceScopeOptionValue"></xs:element>
      <xs:element name="Messaging" type="ServiceScopeOptionValue"></xs:element>
      <xs:element name="PTT" type="ServiceScopeOptionValue"></xs:element>
    </xs:sequence>
  </xs:complexType>
```

```
  <xs:complexType name="LocationInformationOptions">
    <xs:sequence>
      <xs:element name="ReportLocationAtBeginningAndEnd"
type="ServiceScopeOptionValue"></xs:element>
      <xs:element name="ReportLocationUpdate" type="ServiceScopeOptionValue"></xs:element>
      <xs:element name="LALS" type="ServiceScopeOptionValue"></xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="ServiceScopeOptionValue">
    <xs:restriction base="xs:string">
      <xs:enumeration value="Deliver"></xs:enumeration>
      <xs:enumeration value="DoNotDeliver"></xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

Annex D (informative): Drafting Guidance

D.1 Introduction

This annex provides drafting guidance for contributors wishing to propose changes to the present document.

D.2 Drafting conventions

Table D.2-1: Drafting conventions

D.2.1	The details for each field, including a complete description of the usage, format, cardinality and conditionality of that field, are given in the prose in the main body of the document.
D.2.2	The field names used in the main body of the document match those used in the ASN.1.
D.2.3	ASN.1 comments are not used, except for to indicate where to find a description of the field or structure in the main body of the specification.
D.2.4	If a field is made conditional, the condition for its presence or absence is specified.

D.3 Naming conventions

Table D.3-1: Naming conventions

D.3.1	To meet ASN.1 syntax rules, the first character of each ASN.1 field name are lower-cased.
D.3.2	To meet ASN.1 syntax rules, the first character of an ASN.1 type name are upper-cased.
D.3.3	To meet ASN.1 syntax rules, the first character of a field or a type name is not a number.
D.3.4	Only the character ranges A-Z, a-z and 0-9 are used in names.
D.3.5	Names are be CamelCased, where the first character of each word is upper-cased (except for the first character of the name – see rule D.3.1).
D.3.6	Any acronyms in a name should be entirely upper-cased (except for the first character of the name – see rule D.3.1).

```
ExampleBadStructure ::= SEQUENCE
{
    FirstField      [1] FirstFieldType,     -- D.3.1 First letter of field is upper case
    secondField     [2] secondFieldType,    -- D.3.2 First letter of type is lower case
    3rdField        [3] 3rdFieldType,       -- D.3.3 Names starts with digit
    fourth-field    [4] Fourth_Field_Type,  -- D.3.4 Names include hyphen and underscore
    fifthfield      [5] Fifthfieldtype,     -- D.3.5 Names are not camelCased
    msisdn          [6] MSISDN,             -- D.3.6 Acronyms in field name not wholly upper-cased
    mSISDN          [7] Msisdn              -- D.3.6 Acronyms in type name not wholly upper-cased
}
```

Figure 1 – Naming convention counter-examples

D.4 ASN.1 Syntax conventions

Table D.4-1: ASN.1 Syntax conventions

D.4.1	Modules are be defined with EXTENSIBILITY IMPLIED unless there is a specific reason to limit extensibility.
D.4.2	The AUTOMATIC TAGS module directive are not be used.
D.4.3	SEQUENCE and CHOICE tag numbers start at one.
D.4.4	ENUMERATED tag numbers start at one.
D.4.5	Anonymous types are not be used. Non-trivial fields should be assigned their own named type.
D.4.6	Consideration should be given to making types re-usable and independent of a particular release. Res-using or extending an existing type, where the intent is the similar, is preferable to creating a new type.
D.4.7	Consideration should be given to making types extensible by declaring them as a SEQUENCE or CHOICE where possible.
D.4.8	Multiple smaller messages or structures with fewer OPTONAL fields are preferred to larger structures with many OPTIONAL fields, as this increases the ability of the ASN.1 schema to enforce the intent of the specification.
D.4.9	Field names, tag numbers, field types and optional flags are be space-aligned where possible.
D.4.10	Field and type names (when defining a type) are not in bold.
D.4.11	Braces are given their own line.

```
ConformatModule
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) ... }

DEFINITIONS EXTENSIBILITY IMPLIED ::=

BEGIN


Structure1 ::= SEQUENCE
{
    field1  [1] Field1,
    field2  [2] Field2
}

Field1 ::= ENUMERATED
{
    choice1(1),
    choice2(2),
    choice3(3)
}

Field2 ::= OCTET STRING

END
```

Figure 2 – Syntax convention example

```
NonconformantModule
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) ... }

DEFINITIONS AUTOMATIC TAGS ::=          -- D.4.1 Not declared with EXTENSIBILITY IMPLIED
                                        -- D.4.2 Declared AUTOMATIC TAGS
BEGIN

Structure1 ::= SEQUENCE {               -- D.4.11 Braces not given their own line
    field1  [0] ::= ENUMERATED          -- D.4.3 SEQUENCE tags don't start at 1
    {                                   -- D.4.5 Anonymous type used
        choice1(0),                     -- D.4.4 ENUMERATED tag numbers don't start at 1
        choice2(2),
        choice3(3)
    },
    field2  [2] Field2                  -- D.4.10 Field name is bold
}

Field2 ::= OCTET STRING                 -- D.4.10 Type names in definitions is bold


END
```

Figure 3 – Syntax convention counter-examples

Annex Z (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2019-03	SA#83	SP-190044				Release 15 draft Approved at TSG SA#83	15.0.0

History

Document history		
V15.0.0	April 2019	Publication