वर्गीय आवश्यकताओं के लिए मानक टीईसी

22090:2025

(पूर्व सं: टीईसी 22090:2025)

STANDARD FOR GENERIC REQUIREMENTS

TEC 22090:2025

(Earlier No. TEC 22090:2025)

मोबाइल (GSM/CDMA/UMTS/EPS/IMS/5G) नेटवर्क की वैध अवरोधन

(TEC 22090:2011 मानक के सामान्य आवश्यकताओं का अधधक्रमण करता है)

LAWFUL INTERCEPTION of MOBILE (GSM/CDMA/UMTS/EPS/IMS/5G) NETWORK

(Supersede Standard for Generic Requirements TEC 22090:2011)

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

दूरसंचार विभाग, संचार मंत्रालय, भारत सरकार

खुर्शीदलाल भवन, जनपथ, नई दिल्ली – ११०००१, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

Release: , 2025

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document covers the generic requirements for Lawful Interception System (LIS) for Public Land Mobile Network (PLMN) based on GSM/GPRS, CDMA & 3GMS, IMS, EPS and 5G technologies for lawful interception of telecommunication services by authorised Central and State Government agencies in India. The document gives the general introduction, functional requirements such as access to communication content viz. circuit switched, packet switched services, other services including supplementary services which could be the subject of interception. In addition, various other requirements viz. multiple & simultaneous monitoring, encryption & encoding, identification of target, LIS equipment etc. and general requirements have also been defined.

HISTORY SHEET

Sl. No.	Standard/Document No.	Title	Remarks
1.	GR/WS/LIS- 003/01. MAR.2011	LAWFUL INTERCEPTION of MOBILE (GSM/CDMA/UMTS/EPS) NETWORK	
2.	TEC 22090:2011	Standard for Generic Requirements for a LAWFUL INTERCEPTION of MOBILE (GSM/CDMA/UMTS/EPS) NETWORK	Includes revised Numbering Scheme
3.	TEC 22090:2025	Standard for Generic Requirements for a LAWFUL INTERCEPTION of MOBILE (GSM/CDMA/UMTS/IMS/ EPS/5G) NETWORK	Includes revisions as per latest 3GPP releases and 5G requirements

Note:

1. The documents have been renumbered as per revised numbering scheme, kindly refer the Mapping-Listing Table pertaining to old and revised document number available on TEC website www.tec.gov.in/. In case of further clarification, please contact at email ID adgdoc.tec@gov.in

2. Inside the documents, General Requirements may be read as Standard for General Requirements, Interface Requirements as Standard for Interface Requirements, Several Requirements as Standard for General Requirements and Test Schedule & Test Procedure (TSTP) as TEC Test Guide.

INDEX

References

S. No.	3GPP /ETSI/ ITU-T/ TEC GR reference	Description
1.	3GPP TS 33.106	3G security Lawful Interception Requirements
2.	3GPP TS 33.107	3G security Lawful Interception architecture & Functions
3.	3GPP TS 33.108	Handover interface for Lawful Interception (LI)
4	3GPP TS 33.126	Lawful Interception requirements
5	3GPP TS 33.127	Lawful Interception (LI) architecture and functions
6	3GPP TS 33.128	3G security; Handover interface for Lawful Interception
7.	3GPP TS 26.111	Codecs for CS multimedia telephony service - Modifications to H.324
8.	3GPP TS 26.112	Codecs for CS multimedia telephony service – call set up requirements
9.	ETSI ES 201671	Handover interface for Lawful Interception (LI) Of telecommunication traffic
10.	ETSI TS 102 232-1	Service –specific details (SSD) for IP delivery - Handover specifications for IP delivery
11.	ETSI TS 102 232-5	Service –specific details (SSD) for IP delivery - IP multi-media services
12.	ITU-T H.223	Multiplexing protocol for low bit rate multimedia communication
13	ITU-T H.324 M	Terminal for low bit-rate multimedia communication
14.	TEC Standard No. TEC/EMI/TEL-001/01/FEB-09	EMC requirements
15	TEC SD: QM-333	Environment Requirements
16.	TEC/FLA/SMP-001	TEC GR on SMPS based Power Plants
17.	TEC/GR/BAT-01	TEC GR on VRLA Battery
18.	TEC/GR/GPR-01	General Packet Radio Service
19.	TEC/GR/GPR-02	GPRS for GSM, GERAN, UMTS
20.	TEC/SD/CCS-02	CCS 7 National standards for MTP & ISUP
21.	TEC/SD/ISN-01	National Standards for ISDN user network interface

Note: The latest version of the above mentioned references shall be applicable.

CHAPTER - 1
Introduction

1.1. Scope

This document covers the generic requirements for Lawful Interception System (LIS) for Public Land Mobile Network (PLMN) based on GSM/GPRS, CDMA & 3GMS, IMS, EPS and 5G technologies for lawful interception of telecommunication services by authorised Central and State Government agencies .in India. The document gives the general introduction, functional requirements such as access to communication content viz. circuit switched, packet switched services, other services including supplementary services which could be the subject of interception. In addition, various other requirements viz. multiple & simultaneous monitoring, encryption & encoding, identification of target, LIS equipment etc. and general requirements have also been defined.

1.2. Definitions

(i) Target and Target Identity: Target is the subject of interception. A target identity is a network or service identity that uniquely identifies a target for interception from all other non-targets within one or more TSP services. One target may have one or several target identities. The target identity can be a long term subscription based identity, a short term network identity, a public available identity or an internal used (private) identity.

(ii) Interception Area: Interception area is a subset of the Public Lands Mobile Network (PLMN) service area comprised of a set of cells which define a geographical zone.

(iii)

(iv) Intercept related information: Collection of information associated to telecommunication services involving the target.

(v) Location Dependent Interception: It is interception within a PLMN service area that is restricted to one or several interception areas.

(vi) Monitoring: Recording and storing of target subscribers' telecommunications and call associated data by authorised Central and State Government agencies.

(vii) Law enforcement agency: body authorised by law to carry out telecommunication interceptions.

(viii) Content of Communication (CC): Information exchanged between two or more users of a communications service, excluding intercept related information. This includes information which may, as part of some communications service, be stored by one user for subsequent retrieval by another.

(ix) Intercept Related Information (IRI): Information or data associated with communication services involving the target identity, specifically communication associated information or data (e.g. unsuccessful communication attempts), service associated information or data, and location information.

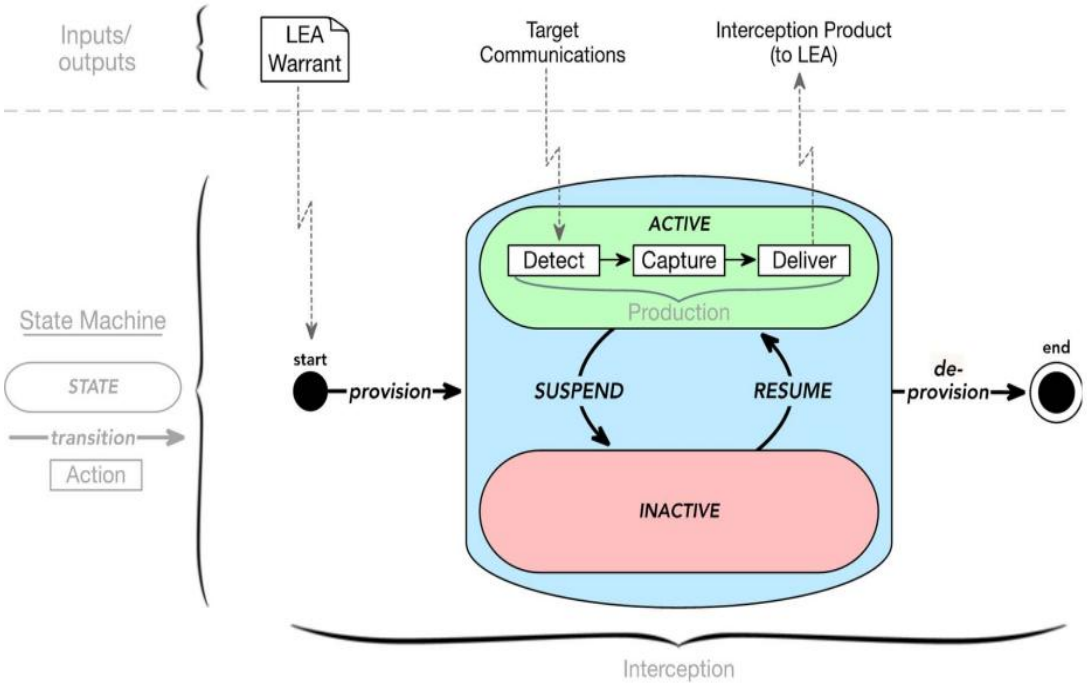
(x) Lawful Access Location Services (LALS): Action performed by a TSP of obtaining a target's location information by means of Location Services (LCS), and providing that information to an LEA.

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

(xii) Handover interface (HI): physical and logical interface across which the interception measures are requested from network operator / access provider / service provider, and the results of interception are delivered from a network operator / access provider / service provider to a law enforcement monitoring facility.

1.3. General

Figure 1 depicts the general Lawful Interception lifecycle



Source - ETSI TS 133 126 V18.2.0 (2024-09)

Figure 1- Generic Lawful Interception lifecycle

After a LEA Warrant is delivered to the TSP, the interception is provisioned. In the ACTIVE state, the Lawful Interception system elements detect, capture and deliver Interception Product to the LEA (labelled "production" in Figure 1). These three production actions occur each time a targeted communication is identified, and therefore may happen many times during the lifecycle.

Some jurisdictions may not support the INACTIVE state of the interception. In such cases, the production actions start directly upon provisioning, and stop directly upon de-provisioning.

Figure 2 depicts the general interception model. Lawful Interception (LI) is implemented in a 3GPP Telecom Service Provider (TSP) network by the logical elements shown in the figure. Detailed LI architecture and functions are found in TS 33.127, while delivery details are found in TS 33.128.

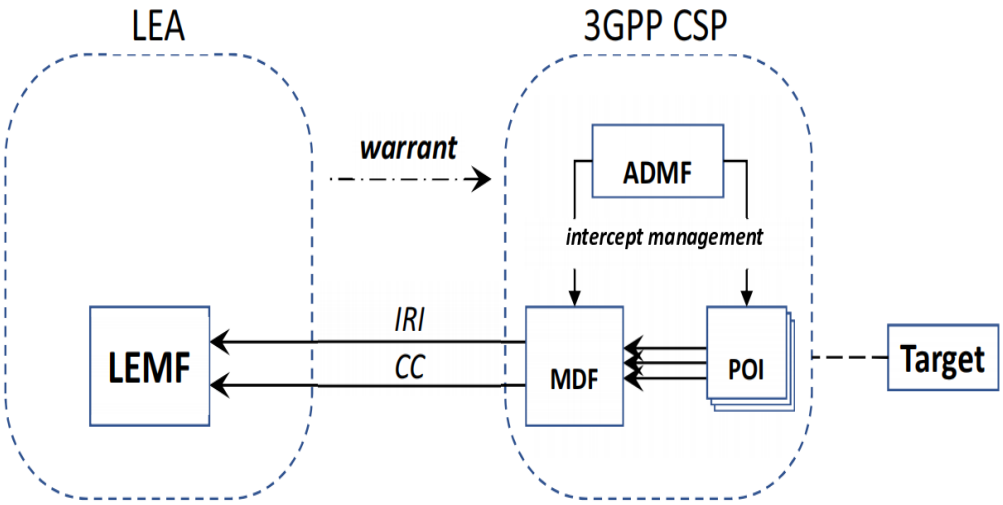


Figure2: Generic Lawful Interception Model (Source - ETSI TS 133 126 V18.2.0 (2024-09))

Figure 3 below illustrates two variations of the MDF: MDF2 and MDF3. MDF2 generates the Intercept Related Information (IRI) messages from the xIRI and sends them to one or more LEMFs. The MDF3 generates the Communication Content (CC) from the xCC and delivers it to one or more LEMFs.

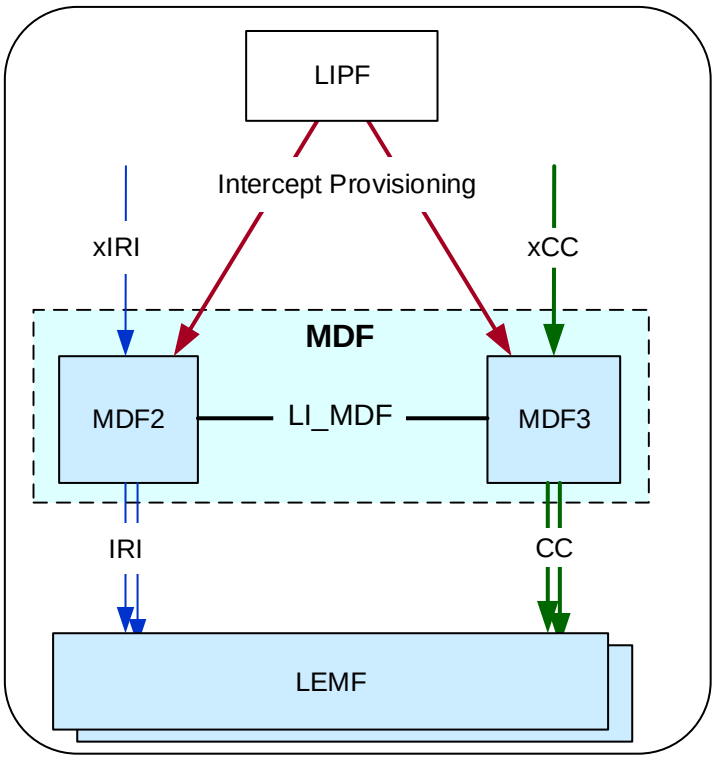


Figure3: Communication flow through MDF2 and MDF3

The Mediation and Delivery Functions (MDF2 and MDF3) are provisioned by the Lawful Interception Provisioning Function (LIPF) with the intercept information required to deliver the Intercept Related Information (IRI) and/or the Communication Content (CC) to one or more Law Enforcement Monitoring Facilities (LEMFs). The LI_MDF interface between MDF2 and MDF3 enables them to exchange information. The Points of Interception (POIs) are divided into two categories depending on the type of data they provide: the IRI-POI delivers xIRI to MDF2, while the CC-POI delivers xCC to MDF3. MDF2 processes the xIRI and generates IRI messages, which are then sent to one or more LEMFs, whereas MDF3 processes the xCC to generate CC, which is delivered to one or more LEMFs.

Public Lands Mobile Network (PLMN) provides access to the intercept product and the intercept related information of the mobile target on behalf of Law Enforcement agencies (LEAs).

A mobile target in a given PLMN can be a subscriber of that PLMN, or a subscriber of another PLMN. The intercept product and the related information can only be delivered for activities on that given PLMN in the country and delivery to the international position shall be restricted.

Location Dependent Interception allows a PLMN to serve multiple interception jurisdictions within its service area. Multiple law agencies with their own interception areas can be served by the PLMN.

The Intercept Related Information (IRI) and the Communication Content (CC) shall be delivered in as near real time as possible. The transmission of intercept request by the authorised agency to the telecom administration is by a manual/electronic approach. The interception is done by the telecom administration which extends the call content to external monitoring equipment located at the monitoring agency.

The monitoring shall not affect the basic and supplementary services of the monitored mobile subscriber i.e. the target. The interception and monitoring shall be implemented in such a way that neither the target subscriber nor any other unauthorised person is aware of it.

General Architecture for Lawful Interception and Monitoring. is shown in Figure-10 (refer Annex-1).

1.4. High Level Generic LI Architecture:

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

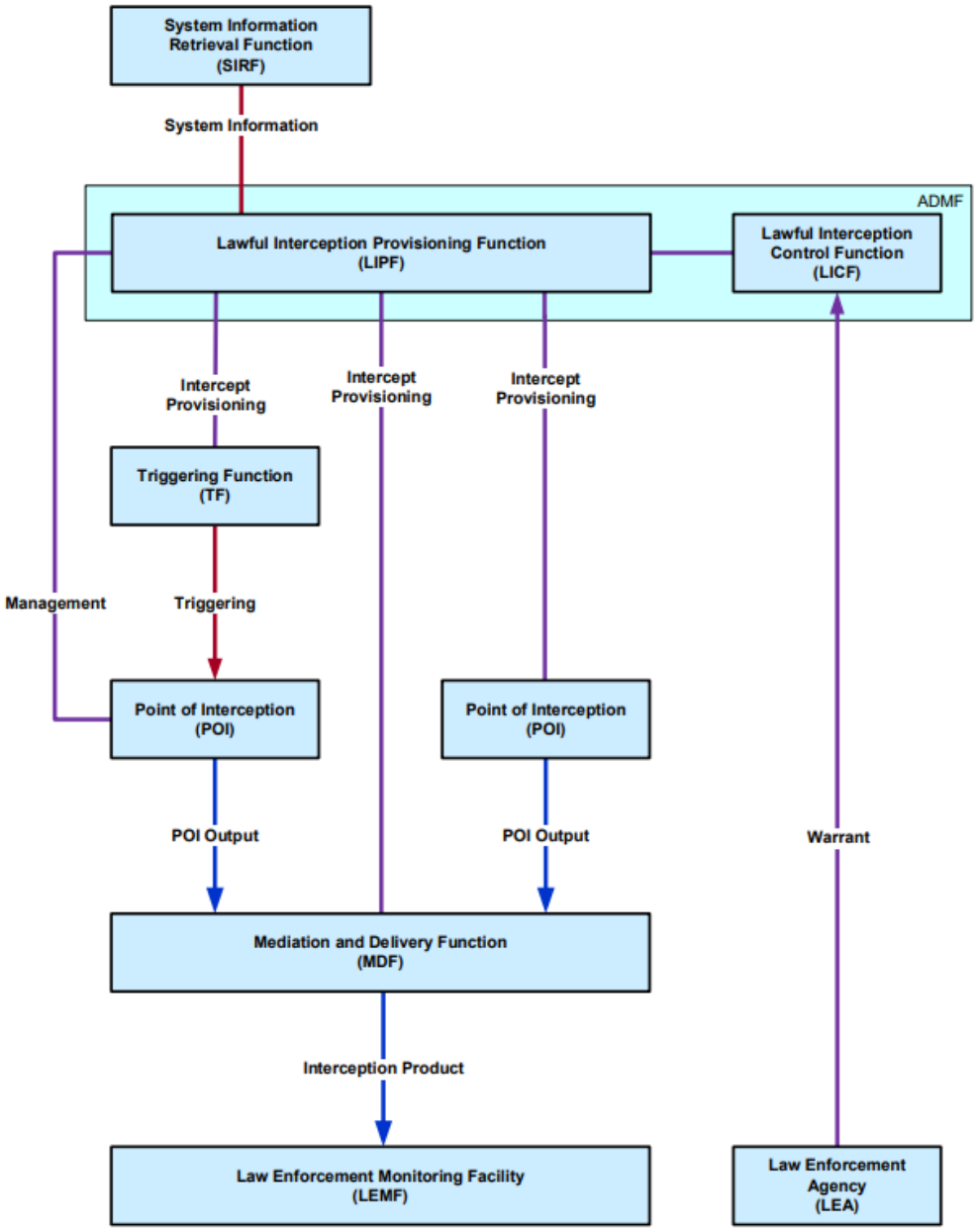


Figure 4: High Level Generic LI Architecture

1.4.1. **Functional Entities:**

1.4.1.1. **Law Enforcement Agency (LEA): I**n general the LEA is responsible for submitting the warrant to the TSPs, although in some countries the warrant may be provided by a different legal entity (e.g. judiciary).

1.4.1.2. **Point of Interception (POI):** The Point of Interception (POI) detects the target communication, derives the intercept related information or communications content from the target communications and delivers the POI output as xIRI to the MDF2 or as xCC to the MDF3. POIs are divided into two types for each category based on the type

of data they send to the MDF:

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

1.4.1.3. **Triggering Function (TF):** The Triggering Function (TF) is provisioned by the LIPF and is responsible for managing the interception state of triggered functions in response to network and service events matching the criteria provisioned by the LIPF. The Triggering Function detects the target communications and sends a trigger to the associated triggered function, and deactivates interception at the associated triggered function when required.

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

1.4.1.5. **The Administration Function (ADMF):** ADMF provides the TSP's administrative and management functions for the LI capability. This includes overall responsibility for the provisioning/activating, modifying, and de-activating/deprovisioning the Point(s) Of Interception (POI), Triggering Functions (TF), and the Mediation and Delivery Functions (MDF). The ADMF includes the following logical sub-functions:

a. Lawful Interception Control Function (LICF): The LICF controls the management of the end-to-end life cycle of a warrant. The LICF contains the master record of all sensitive information and LI configuration data. The LICF is ultimately responsible for all decisions within the overall LI system.
b. Lawful Interception Provisioning Function (LIPF): LIPF is the secure proxy used by the LICF to communicate with POIs, TFs, MDFs or other infrastructure required to operate LI within the TSP network.
c. Identifier Query Function (IQF): The IQF is the function responsible for receiving and responding to dedicated LEA real-time queries for identifier associations
d. Certificate Authority (CA)
e. Location Acquisition Function (LAF): The Location Acquisition Function (LAF) is responsible for processing the location requests received from the LEA during the location acquisition procedure

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

1.4.1.6. **System Information Retrieval Function (SIRF):** SIRF is responsible for providing the LIPF with the system related information for NFs that are known by the SIRF (e.g. service topology).

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

1.4.1.8. **Location Acquisition Requesting Function (LARF):** LARF is a function associated with the MME (for EPC) and AMF (for 5GC) responsible for handling the location requests from the LAF during the location acquisition procedure.

1.5. LI Interfaces

A high-level interception architecture diagram showing key point-to-point LI interfaces is shown in figure 5 below.

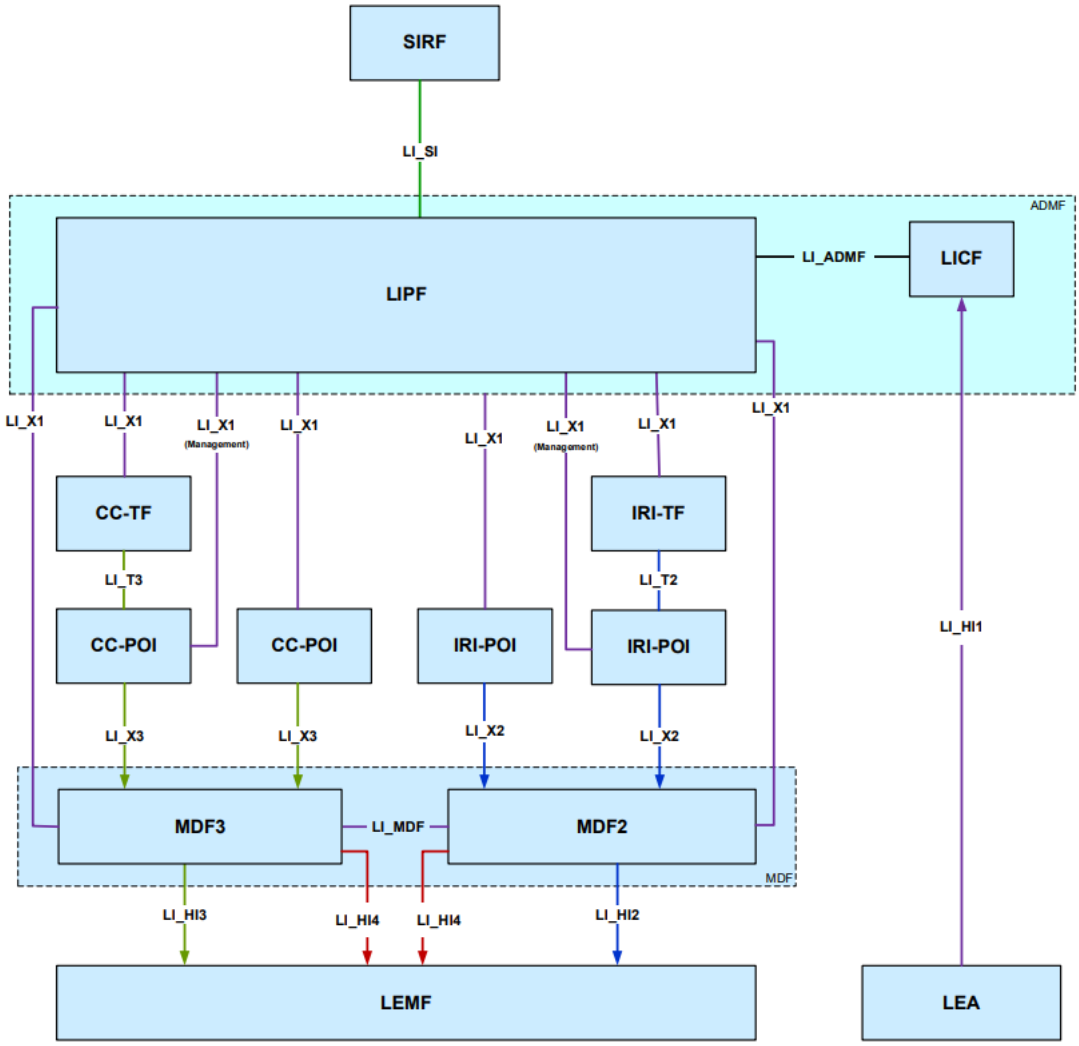


Figure 5- High-level interception architecture diagram with key point-to-point LI interfaces

Interface	Between	Purpose / Description
LI_SI	SIRF ↔ LIPF	Carries subscriber information (e.g., identity, service details) to assist in target provisioning for interception.

LI_ADMF	LIPF ↔ LICF	Used for administrative control and authorization — the LICF (Lawful Interception Control Function) receives and manages interception requests from LEA, and LIPF provisions accordingly.
LI_X1	LIPF ↔ POI (Points of Interception) / TF (Transfer Functions)	A management interface controlling activation, deactivation, and configuration of interception on network elements.
LI_X2	IRI-POI ↔ MDF2	Transfers Intercept Related Information (IRI) — metadata such as call setup, tear-down, location, IP address, etc.
LI_X3	CC-POI ↔ MDF3	Transfers Content of Communication (CC) — actual voice, message, or data payload intercepted.
LI_HI1	LEA ↔ LICF	Communication between LEA and operator's interception control — used to submit lawful warrants or interception requests.
LI_HI2	MDF2 ↔ LEMF	Transfers IRI (call metadata) to the Law Enforcement Monitoring Facility in standardized format.
LI_HI3	MDF3 ↔ LEMF	Transfers CC (content) to the LEMF for lawful monitoring.
LI_HI4	LIPF / MDF ↔ LEMF	Used for administrative or provisioning reports (e.g., acknowledgment, status of activation, synchronization).
LI_MDF	Internal link between MDF2 and MDF3	Coordinates delivery of IRI and CC streams ensuring timing and correlation between metadata and content.

1.6. LI in a virtualised environment

Figure 6 shows the necessary extensions to the basic LI architecture described in clause 1.4 required to support realtime deployment of virtualised LI functions

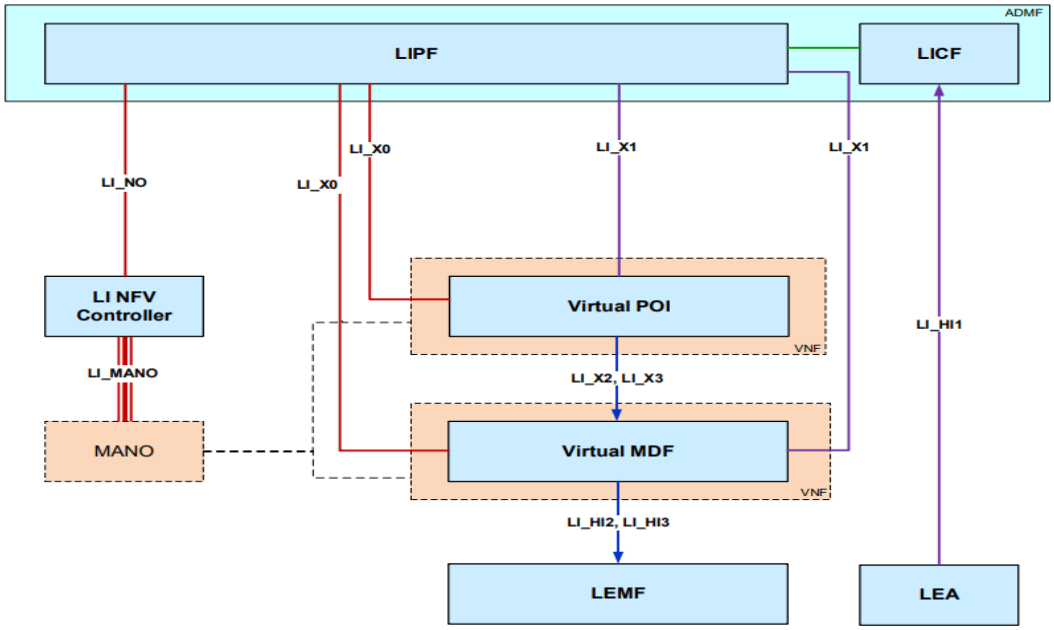


Figure 6- Simplified virtualised LI system

1.7. Handover Interface:

1.8.

The generic Handover Interface adopts a three-port structure such that administrative information (HI1), Intercept Related Information (HI2) and the Content of communication (HI3) are logically separated.

Figure -2 below shows the handover interface for Lawful Interception (LI).

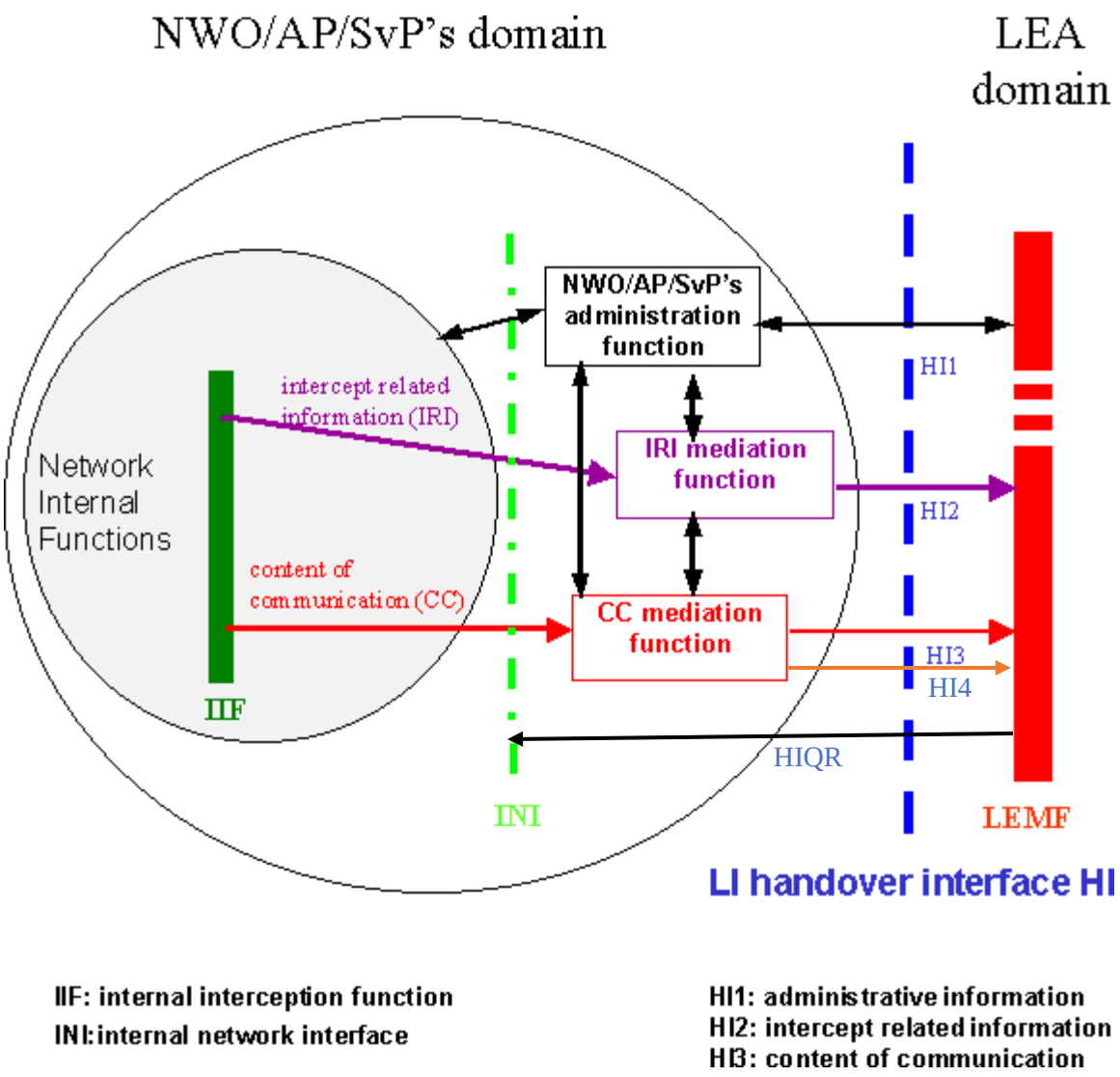


Figure: 7

(Source: ETSI ES 201671)

HI4 interface is for 5G. HI4 is explicitly referenced as an interface for *status/notification* messages (e.g., intercept activation/deactivation or delivery status) from MDF to the LEMF.

There is another interface HIQR defined in 3GPP 33.128 for LEMF to query LI system of TSP.

HIQR provides a **secure, standardized mechanism** for a **Law Enforcement Monitoring Facility (LEMF)** to **query the operator's LI system** (via the **Mediation and Delivery Function — MDF**) for:

- Interception-related information,
- Administrative status,
- Stored records,
- or to manage LI configuration parameters

1.9. Applicability to telecommunication services

The requirement for lawful interception is that all telecommunications services in the mobile network shall be capable of meeting the requirements as per 3GPP TS 33.106 and 3GPP TS 33.126.

1.9.1. Interception within the Home and Visited Network

The introduction of the Virtual Home Environment, VHE, means that significant portions of subscriber services can be executed in the home or visited network, regardless of where the target is physically located.

The visited network shall intercept only those services that the visited network provides to the target subscriber. Furthermore, the visited network shall not be required to intercept services executed by the home network.

For home subscriber visiting other network, If an event for/from a mobile subscriber occurs , the HLR/HSS sends the relevant data to the DF2/MDF2 (as defined in 3GPP TS 33.107 and 3GPP TS 33.127) and LIS shall send this info in HI2 as standard LU (location update) message to monitoring agency.

1.10. Normal operation

This section gives the expected operation for lawful interception as per 3GPP TS 33.106 and 3GPP TS 33.126.

1.10.1. Intercept administration requirements

A secure means of administrating the service by the mobile operator and intercept requesting entity is necessary. This mechanism shall provide means to activate, deactivate, show, or list targets in the mobile as quickly as possible. The function shall be policed by appropriate authentication and audit procedures. The administration function shall allow specific IAs (Interception Areas) to be associated with target subscribers when Location Dependent Interception is being used.

The LIS shall accept all administrative requests on DF1/MDF1 from monitoring agency and provide the responses through XML interface or any other standardized interfaces.

1.10.2. Activation of LI

As a result of the activation (of a warrant) it shall be possible to request for the specified target, either IRI, or both the IRI and the CC and designate the LEA destination addresses for the delivery of the CC and IRI if required.

1.10.3. Deactivation of LI

As a result of deactivation it shall be possible to stop all, or a part of, interception activities for the specified target.

1.10.4. Security of processes

The intercept function shall only be accessible by authorised personnel.

To be effective, interception must take place without the knowledge of either party to the communication. Therefore, decryption must also take place without either party being aware that it is happening.

No indication shall be given to any person except authorised personnel that the intercept function has been activated on a target. Authentication, encryption, audits, log files and other mechanisms may be used to maintain security in the system. Audit procedures should be capable of keeping accurate logs of administration commands.

NWOs/APs/SvPs shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of facilitating authorized communications interceptions and access to intercept related information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects:

1.10.4.1. the privacy and security of communications and intercept related information not authorized to be intercepted; and

1.10.4.2. information regarding the LEA's interception of communications and access to intercept related information.

A NWOs/APs/SvPs shall not be responsible for decrypting, or ensuring the LEA's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the NWOs/APs/SvPs and the NWOs/APs/SvPs possesses the information necessary to decrypt the communication or the NWOs/ APs/SvPs provides encryption keys but does not provide the encryption itself. In the case that the NWOs/ APs/SvPs provides encryption keys to the subscriber or customer but does not provide the encryption itself, the NWOs/ APs/SvPs shall provide the keys to the LEA if required by national regulations.

1.11. Intercept invocation

1.11.1. Invocation events for lawful interception

In general, Lawful interception shall be invoked when the transmission of information or an event takes place that involves the target. Examples of when Lawful interception could be invoked are when:

- A Voice / Video call is requested originated from, terminated to, or redirected by the target,
- Location information related to the target facility is modified by the subscriber attaching or detaching from the network, or if there is a change in location,
- An SMS transfer is requested - either originated from or terminated to the target,
- A data packet is transmitted to or from a target.
- Serving System Change/ Serving Evolved Packet System.
- Subscriber record change.
- Registration Termination (i.e. Cancel Location)
- Bearer activation/modification/deactivation

1.11.2. Invocation and removal of interception regarding services

The invocation of lawful interception shall not alter the operation of a target's services or

provide indication to any party involved in communication with the target. Lawful interception shall not alter the standard function of other network elements.

If lawful interception is activated during a Voice / Video service, the currently active service is not required to be intercepted. If lawful interception is deactivated during a service, all ongoing intercepted activities may continue until they are completed.

Since in 5G, data size of intercepted content will be huge so 3GPP has given provision of Service scoping in provisioning. Service Scoping is the process of defining which services, traffic types, or network functions (NFs) must be intercepted for a given target (subscriber, device, or identifier). While invoking lawful interception of a target, filter criterias to be supported by telecom service provider.

If lawful interception is activated when a packet data service is already in use, the next packets transmitted shall be intercepted. If lawful interception is deactivated during a packet data service, the next packets shall not be transmitted.

1.11.3. Correlation of information and product

When both IRI and CC are invoked, an unambiguous correlation shall be established between the two. The IRI and CC shall be delivered in ETSI or any other globally recognized format as well as readable format as per procurer requirements.

1.11.4. Exceptional procedures

When a failure occurs while establishing the connection towards the LEA to transfer the CC this shall not result in any interruption of the ongoing telecommunications service. Whenever failure occurs while trying to provide the IRI it shall be temporarily stored in the service provider/LIS and further attempts shall be made to deliver as soon as possible.

1.12. Minimum service requirements

Quality of service, capacity, integrity and reliability are the subject of bilateral agreement between the relevant authorities and the service operator. The QoS towards the delivery function provided by the network must be at least that the network provides to the target.

1.13. Functional architecture Node-wise

The following figures contain the node-wise reference configuration for the lawful interception. The circuit-switched configuration is shown in Figure 8a (for 2G/3G voice). The packet-switched configuration is shown in Figure 8b (data). Intercept configurations for 5G EPC anchored LI, 5G Core anchored LI and 4G/5G interworking LI are shown in Figure 8c, 8d and 8e respectively. Intercept configuration for Location functions, IMS in 4G/5G, non-3GPP data access in 4G/5G and Conferencing interception are shown in Figure 8f, 8g, 8h and 8i respectively.

Lawful Interception (LI) can be done at various nodes like AMF, SMF, UPF, SMSF, UDM etc. in 5G (refer 3GPP TS 33.127 for architecture diagram and interfaces), MME, P-GW/S-GW, HSS etc. in 5G (refer 3GPP TS 33.127 for architecture diagram and interfaces) and GMSC, HLR etc. (refer 3GPP TS 33.107 for architecture diagram and interfaces).

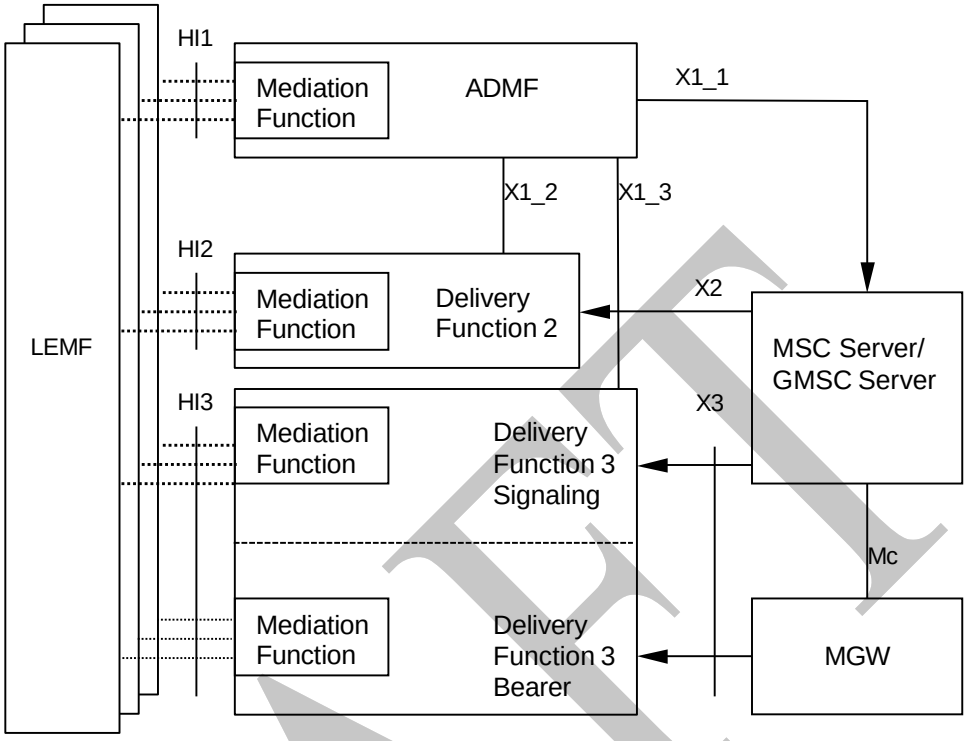


Figure 8a: Circuit switched intercept configuration

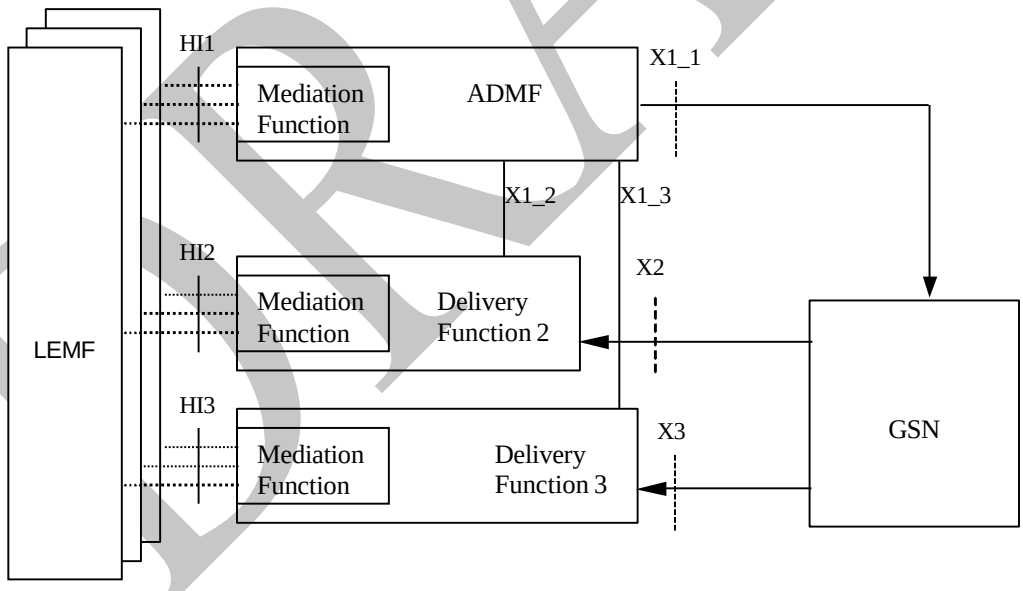


Figure 8b: Packet Switched Intercept configuration

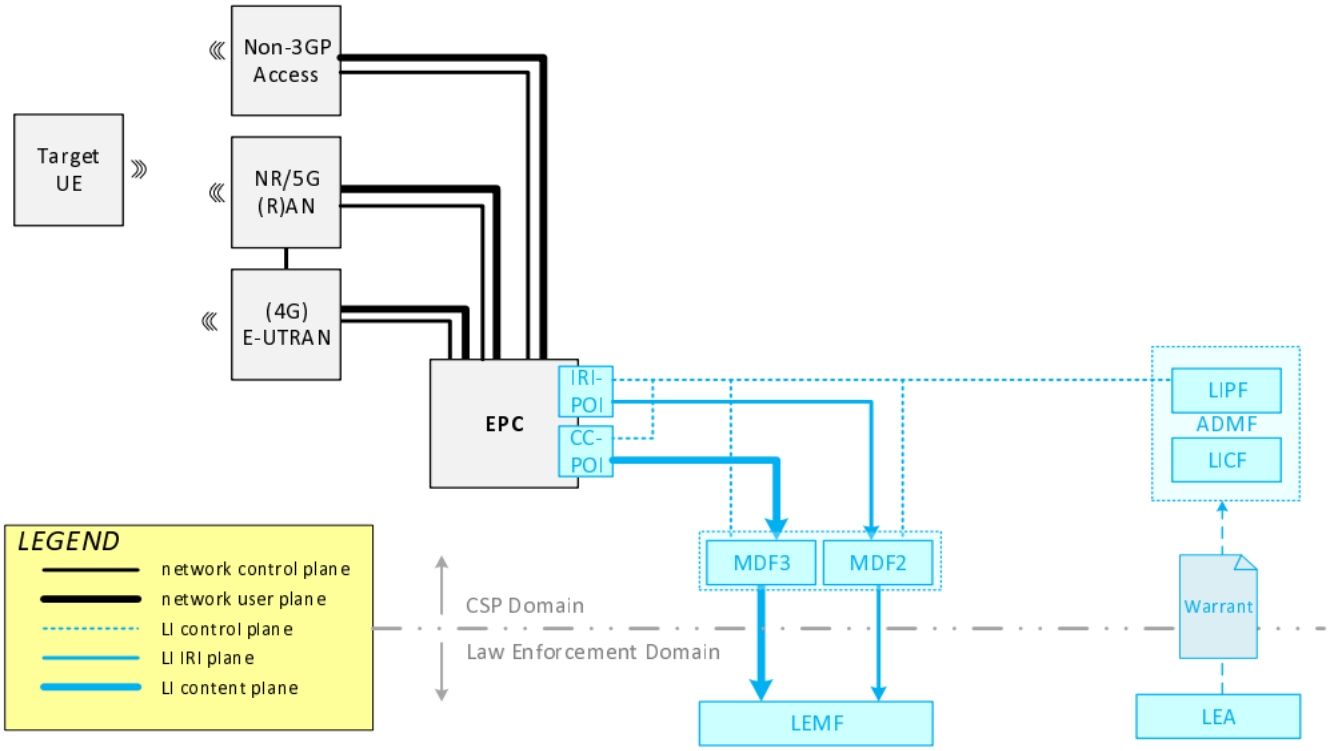


Figure 8c: 5G EPC-anchored LI architecture

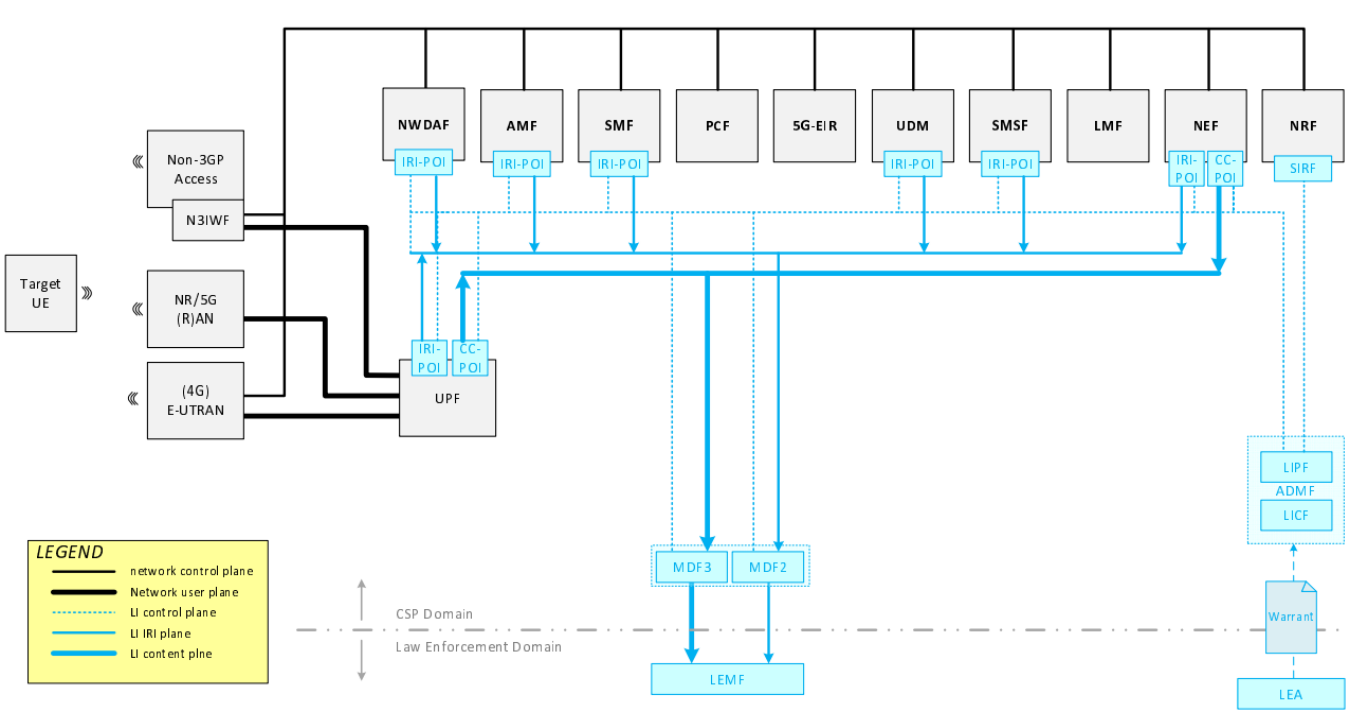


Figure 8d: 5G core-anchored LI architecture

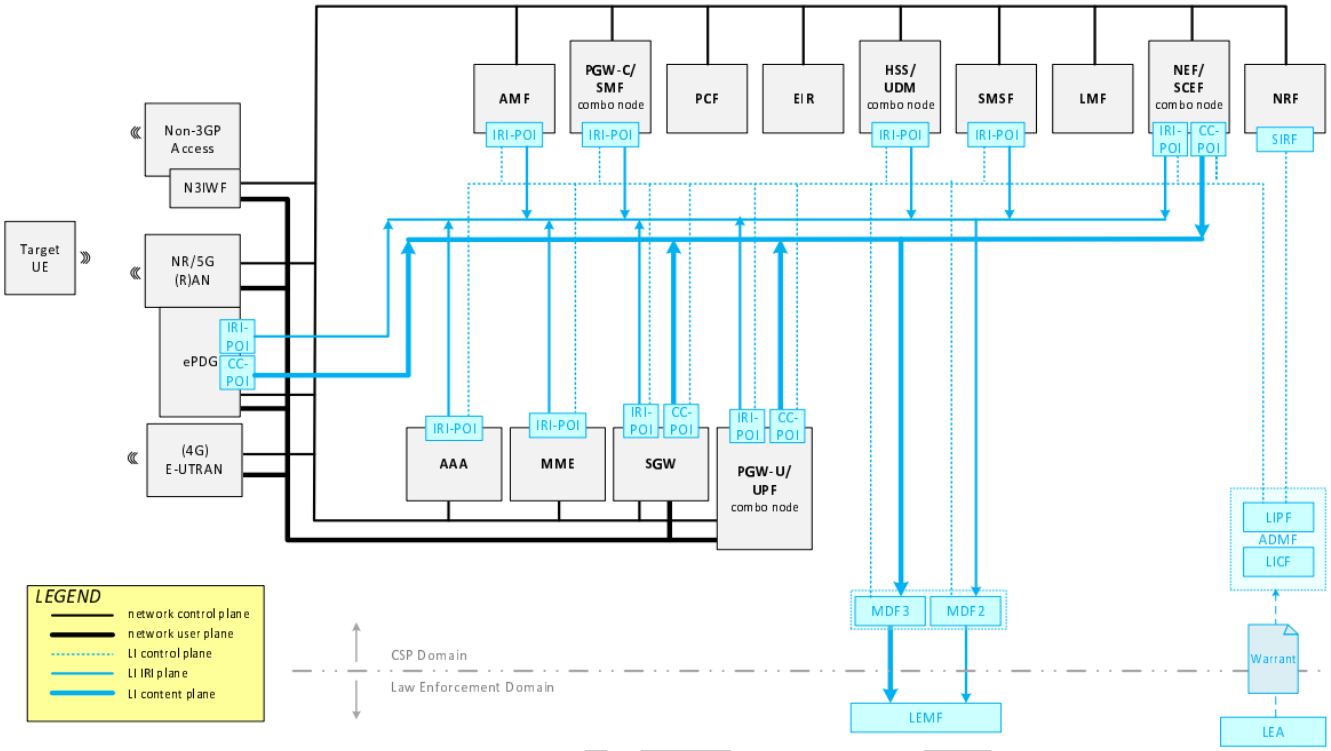


Figure 8e: EPC/5G Interworking LI architecture

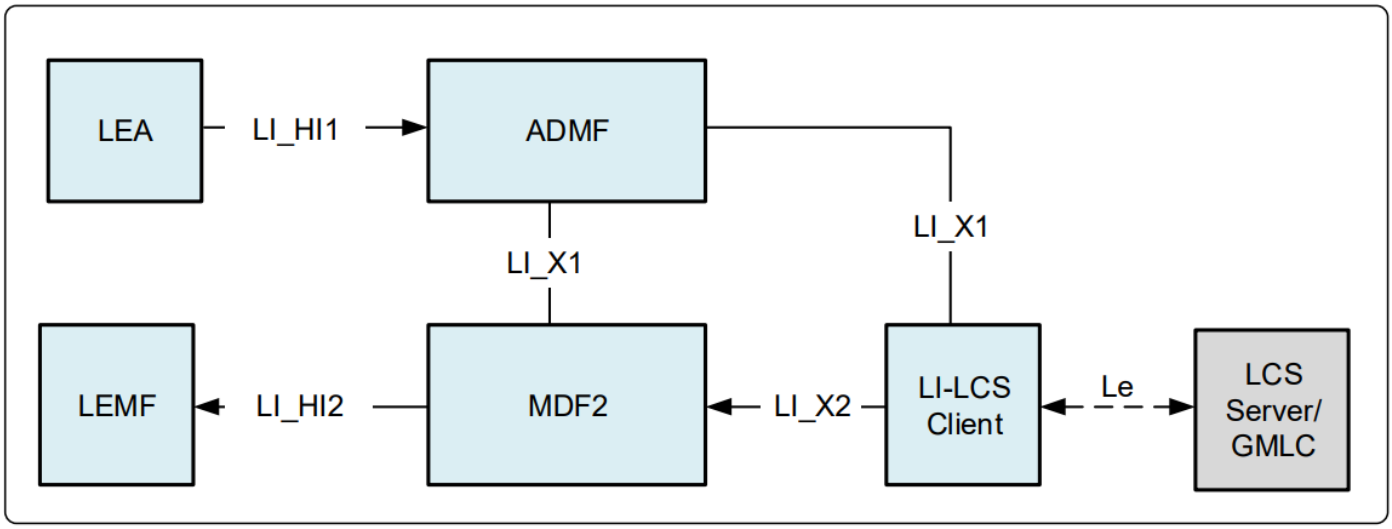


Figure 8f : LI Architecture for target positioning

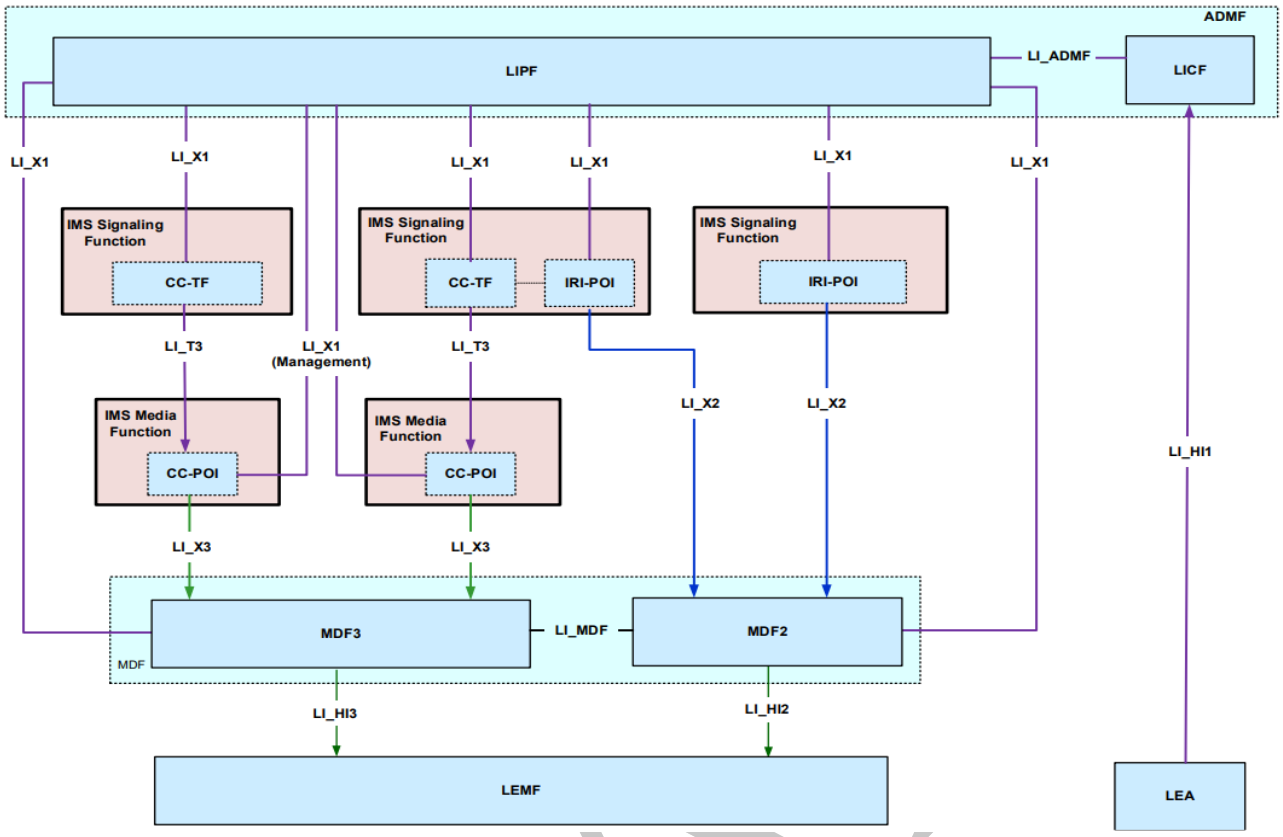


Figure 8g: IMS LI Architecture

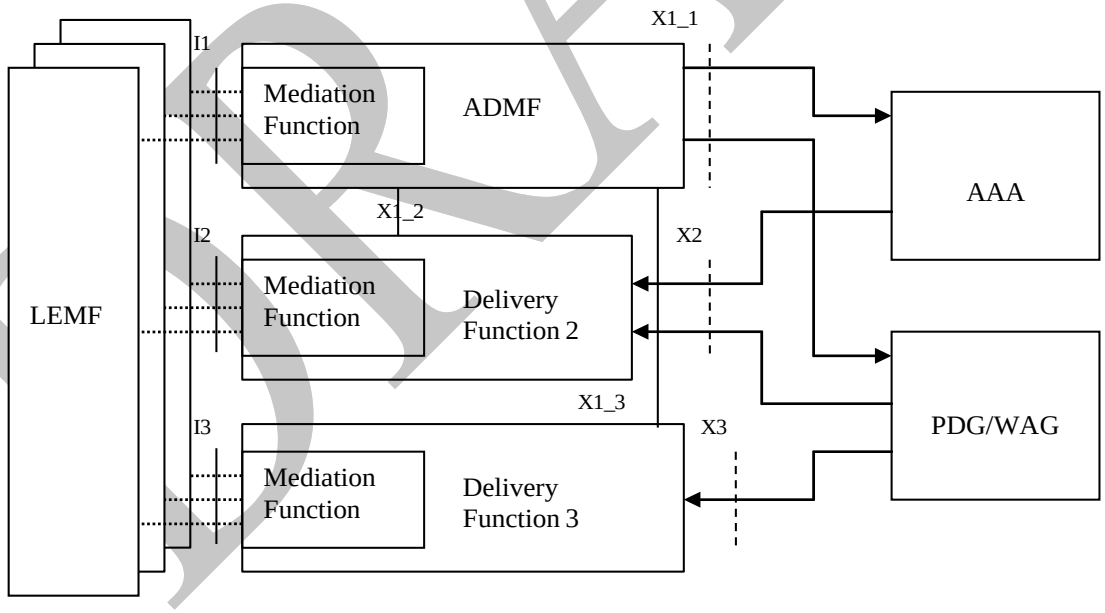


Figure 8h: WLAN Interworking Intercept configuration

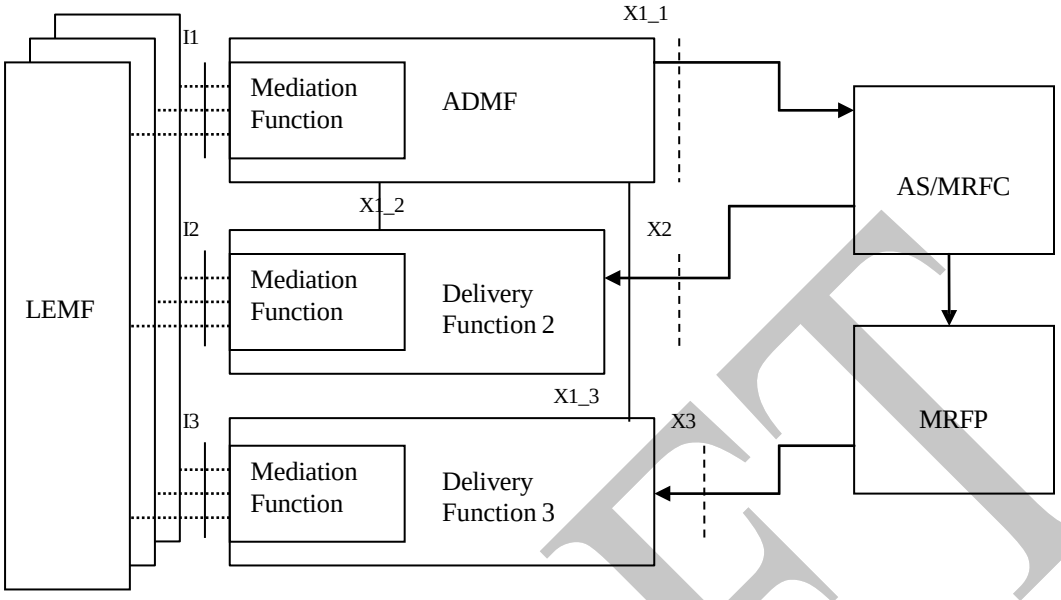


Figure 8i: IMS Conferencing Intercept configuration

1.14. Activation, deactivation and interrogation

Figure -4 is an extraction from the reference intercept configuration shown in figures 9a through to 9i which is relevant for activation, deactivation and interrogation of the lawful interception.

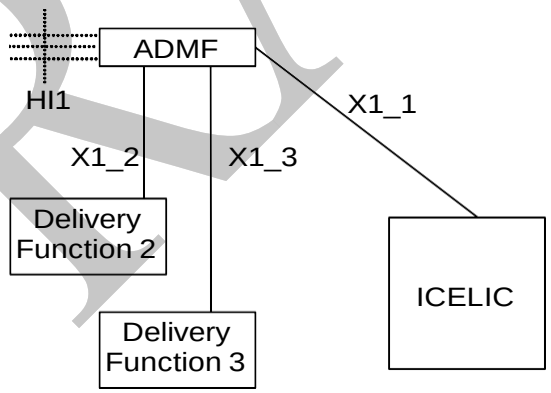


Figure -9: Functional model for Lawful Interception activation, deactivation and interrogation

In addition to the typical ICEs functional entities, a new functional entity is introduced - the ADMF - the Lawful Interception administration function. The ADMF:

- interfaces with all the LEAs that may require interception in the intercepting network;
- keeps the intercept activities of individual LEAs separate;
- interfaces to the intercepting network.

1.14.1. X1_1-interface

The messages sent from the ADMF to the ICEs (X1_1-interface) contain the:

- target identities (MSISDN, IMSI, IMEI, SIP URI or TEL URL, NAI NAI, SUPI, SUCI, GPSI, PEI, IP address)
- information whether the Content of Communication (CC) shall be provided
- address of Delivery Function 2 (DF2/MDF2) for the intercept related information
- address of Delivery Function 3 (DF3/MDF3) for the intercepted content of communications
- IA in the case of location dependent interception.
- Triggered based provisioning in case dynamic node/function invocation in 5G network using LI_T interface

1.14.2. X1_2-interface (IRI)

For the activation of IRI the message sent from the ADMF to the DF/MDF contains:

- the target identity;
- the address for delivery of IRI (= LEMF address);
- which subset of information shall be delivered;
- a DF2/MDF2 activation identity, which uniquely identifies the activation for DF2/MDF2 and is used for further interrogation or deactivation, respectively;
- the IA in case of location dependent interception;
- the warrant reference number if required by national option.

If a target is intercepted for several LEAs and/or several identities simultaneously, a single activation of delivery is necessary for each combination of LEA and identity.

1.14.3.X1_3-interface (CC)

For the activation of intercepted Content of Communications the message sent from the ADMF to the Delivery Function contains:

- the target identity;
- the address of delivery for CC (= LEMF address);
- a DF3/MDF3 activation identity, which uniquely identifies the activation for DF3/MDF3 and is used for further interrogation or deactivation, respectively;
- the IA in case of location dependent interception;
- the warrant reference number if required by national option.

If a target is intercepted by several LEAs and/or several identities simultaneously, a single activation of delivery is necessary for each combination of LEA and identity.

1.14.4.LI_T –interface

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

- LI_T2.
- LI_T3.

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

CHAPTER-2

Functional Requirements

2.1 Access to Communication Content (CC):

Access to the entire telecommunications transmitted or caused to be transmitted to and from the target subscriber shall be supported for the following forms of telecommunications:

2.1.1 Services

It shall be possible to intercept in real -time the following circuit-switched services, GSN packet-data services, Packet –data multi-media, WLAN inter-working services, MBMS, IMS conferencing services etc. used by the target as defined in 3GPP TS 33.107/ in 3GPP TS 33.127:

a) CS services

i. Voice Telephony
ii. Short message service - point to point
iii. Fax group 3
iv. Video telephony
v. CS data (9.6 Kbps/ 14.4 Kbps)

b) **GSN Packet-data services**

i. Packet Data up to 144 Kbps- (for CDMA as per IS-95, IS 707, IS 835 & IS 2000)
ii. General Packet Radio Service (GPRS): Lawful Interception of GPRS shall comply with TEC GR no. GR/ GPR-01& GR/GPR-02.
iii. SMS

c) **Packet- data multi-media Services**

i. Multimedia Messaging Services (MMS):
Lawful Interception functionality for Multimedia Messages shall comply with TEC GR No. GR/ MMS- 01. It shall be possible to record the logs of subscriber's actions (submitting, forwarding, and receiving of MMs) and saved to Lawful storage device. It shall be possible to copy-forward the submitted and received MMs for marked subscribers to multiple Lawful Interception addresses within the operator domain.

ii. Video streaming (as per ITU-T recommendations H.324 M)

iii. VoLte/ViLte interception

iv. Location Based Services (LBS):
The LBS system shall provide interfaces for provisioning, IRI and CC for the purpose of Lawful Interception. LBS system shall be able to provide location details as per the requirements of LEA, limited to the extent of capability of the

terminal and location technology used, irrespective of the state of the target (i.e. whether or not it is on an LBS call). It shall comply to TEC GR No. GR/ LBS-01 (for GSM) & TEC GR No. GR/ LBS- 02 (for CDMA). The location based information shall be available even when the target is not making a call. LIS system shall interface with LBS system over MLP (mobile location protocol) as defined by OMA (Open Mobile Alliance) as per OMA MLP v3 & above.

d) 3GPP WLAN inter-working services:

i. ePDG (Evolved Packet Data Gateway) in 4G, TNGF and N3IWF in 5G
ii. PDN-GW / UPF (User Plane Gateway functions)
iii. AAA / AUSF / SMF (for authentication and session control data)

e) IMS voice conferencing services VoIP, video, messaging, and conferencing **over IP networks (LTE or 5G).**

f) EPS

i. All packet data services over the LTE/4G network, including but not limited to web browsing, file transfer, streaming, VoIP/VoLTE, and IP application layer services.
ii. SMS over SGs and SMS over IMS.
iii. Location services specific to EPS (e.g., E-UTRAN Cell Global Identifier - ECGI).

g) 5G System (5GS) Services

i. All packet data services over the 5G network (PDU Session based), including enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), and massive IoT (mIoT) traffic.
ii. Voice over New Radio (VoNR), Video over New Radio (ViNR), and SMS over NAS.
iii. Location services, including high-accuracy positioning information where available.
iv. Services related to network slicing, where the target is using a specific network slice.
v. Services provided via Multi-access Edge Computing (MEC).

h) Other services

i. IP application layer services e.g. (e-mail, FTP,web browsing, VoIP, Push to talk etc.)
ii. MBMS
iii. WAP services (WAP 2.0)
iv. IoT / M2M Data Sessions carried over Packet-switched or 5G Core networks.
v. Over-the-top (OTT) data services, wherever interception is mandated through network-based mediation interfaces.

2.2 Supplementary Services

It shall be possible to report all activities regarding supplementary services to LEA.

2.2.1 Impact

The application of the following supplementary services shall have no impact on the interception function:

i. Calling Line Identity Presentation (CLIP)
ii. Calling Line Identity Restriction (CLIR)

iii. Connected Line Identity Presentation (COLP)
iv. Connected Line Identity Restriction (COLR)
v. Call Barring services (CB)
vi. Advice of Charge (AOC) services
vii. Closed User Group (CUG)
viii. Completion of Calls to Busy Subscribers (CCBS)
ix. Virtual Private Network (VPN)

2.3 Access to Intercept Related Information (IRI)

Access to the Intercept Related Information (IRI) for at least *3000* targets **(latest DoT administrative orders/ Instructions/ guidelines for proper provisioning and interception shall be adhered to)** per agency shall be supported. In addition to the IRI information in respect of the parameters mentioned in clause 2.7, following shall be available:

i. Type of call (originating or terminating)
ii. Date and time of answer (in case of successful call)
iii. Date and time of call origination (in case of unsuccessful call)
iv. Calling subscriber identity including Local Area Code (LAC)
v. Number dialled by the calling subscriber
vi. Indication of bearer capability for ISDN call (speech/ 3.1 kHz/ 64 kbit/s unrestricted)
vii. Duration of conversation (start time & end time)
viii. Indication of whether the call is successful or unsuccessful
ix. Co-relation information
x. All the signals emitted by the target subscriber, including post-connection dialled signals, the activation of additional facilities such as conference call, call transfer, call waiting, etc.
xi. Redirecting number (if available)
xii. Cell Global Identity (CGI)
xiii. Cell Site Information (CSI)
xiv. End Cell Global Identity
xv. Start / End Cell ID
xvi. End sector of the Cell
xvii. Call status towards monitoring agency
xviii. Activities independent of calling like power on, power off and location update.

For EPS (4G) network intercept, the following IRI information shall be delivered:
a. Target list (observed SIP-URIs and/or observed TEL-URIs, IMPU/IMPI, and/or MSISDN/IMSI)
b. Event type (e.g., *SIP Message*, *Registration*, *Session Establishment*, *Conference Event*, *Detach*, *Bearer Modification or Conference Event* or Conference Event)
c. Time stamp (date and time the event was detected)
d. Correlation number
e. SIP message (if indicated by Event type)
f. Conference Event (if indicated by Event type)

g. Call Content related
h. APN (Access Point Name) used
i. User's IP address (IPv4/IPv6)
j. Tracking Area Identity (TAI)
k. PDN connection ID / Bearer ID – identifies the specific EPS bearer associated with the session.
l. Serving Gateway (SGW) and PDN Gateway (PGW) identifiers – network element identifiers (e.g., FQDN or IP address).
m. QoS profile and bearer type – QoS Class Identifier (QCI) and ARP parameters associated with the intercepted session.
n. Serving MME identity – identifier of the MME handling the UE context at the time of interception.
o. Subscriber location information – current location estimate or service area description.
p. Operator ID / PLMN ID – identifies the operator or network domain serving the ta
q. Cell Global Identity (CGI) / E-UTRAN Cell Global Identity (ECGI)

For 5G network intercept, the following IRI information shall be delivered:

a. Target and Identity Information (*SUPI, SUCI, Generic Public Subscription Identifier (GPSI) – e.g., MSISDN, SIP URI, IMEI, Temporary identifiers – 5G-GUTI, TMSI, etc.and IMS identifiers – IMPI and IMPU (for IMS/SIP sessions*)
b. Event type (registration, authentication, session establishment, modification, release, paging, mobility event, etc.)
c. Timestamp (UTC) of event detection
d. Correlation number to link IRI with Content of Communication (CC)
e. PDU Session ID and QoS Flow Identifier (QFI)
f. Data Network Name (DNN) associated with the session
g. Slice/Service Type (SST) and Slice Differentiator (SD) – forming S-NSSAI
h. Associated SMF and UPF instance identifiers
i. Assigned IP address (IPv4 / IPv6)
j. Serving PLMN ID and operator identifier
k. Network Function identities – AMF, SMF, UPF, PCF, NEF, AUSF, UDM (by FQDN or IP)
l. Access type – 3GPP (NR / E-UTRA) or non-3GPP (trusted / untrusted WLAN)
m. User Location Information (ULI) – Tracking Area Identity (TAI), NR Cell Global Identity (NCGI), etc.
n. Roaming information – home and visited PLMN IDs
o. Quality of Service (QoS) parameters – 5QI, GBR, MBR, priority, ARP, etc.

2.4 Conditions of Access

i. Access to a target shall be supported in real time and for full time. IRI & Communication Content (CC) shall be made available at the monitoring centre in real time. In case immediate transmission is not possible for IRI, then stored IRI should be transmitted atleast once in every 5 minutes. **(latest DoT administrative orders/ Instructions/ guidelines for proper provisioning and interception shall be adhered to).**

ii. The interception and monitoring shall be implemented in such a way that neither the target subscriber nor any other unauthorised person is aware of it.

iii. The operation and services (basic & supplementary) of the target subscriber line shall not be affected in any manner.

iv. Where the target subscriber is a party to a conference call or multi-party call, access to the call content of all parties to that call and to the call associated data relevant to the target subscriber shall be supported.

v. There shall be no change in the quality of services being accessed as defined in clause 2.1.1, when the target is under interception.

Details of calls being monitored by security agencies shall not be available/accessible to anyone/anywhere in the gateway/switch except to the authorised personnel responsible for programming the number of interests. Also details of calls being monitored/number of interests programmed shall not be printed anywhere in the regularly generated traffic report/billing information. However, option should be there to generate Interception traffic (agency-wise) report separately and securely as and when requirement arises from Agency. In case of remote access to the switch/monitoring system by a service engineer or any other person, then intercepts including CC & IRI shall not be accessible to such persons.

2.5 Multiple and Simultaneous Monitoring

i. Provision shall exist to simultaneously monitor a single target subscriber simultaneously by at least ten monitoring agencies. **(latest DoT administrative orders/ Instructions/ guidelines for proper provisioning and interception shall be adhered to).**

ii. In such cases each access shall be kept separate and distinct to ensure that the interest of each agency is not known to the others.

2.6 Encryption and Encoding

i. The call content shall be transmitted in its original form without any encryption and encoding, unless otherwise asked for, to the monitoring centre.

ii. Where the call content is modified by the target subscriber, it is the responsibility of the monitoring agency to extract the intelligence from the call.

2.7 Identification of target

It shall be possible to intercept & monitor the target on the basis of any of the following:

i. MSISDN
ii. IMSI
iii. IMEI
iv. ESN
v. MIN
vi. MDN
vii. Network Access Identifier (NAI)
viii. IP address (in case of packet calls to & from terminals with fixed IP)
ix. SIP URI
x. TEL URI
xi. GUTI / 5G-GUTI / TMSI

xii. SUCI
xiii. GPSI
xiv. DNN / APN
xv. PDU Session ID / PDN Connection ID
xvi. MAC address
xvii. X.509 certificate subject / TLS client identifier
xviii. Application-level identifiers (e.g., OTT account ID, SIP To/From)

2.8 Network architecture

The system shall be based on ETSI TS 101 507 (for GSM) & 3GPP TS33.106, 33.107 & 33.108 (for WCDMA and LTE) and 3GPP TS 33.126, 33.127 and 33.128 (for 5G) and shall meet the national lawful requirements of authorised Central and State Government agencies. For IMS network, the specifications to be complied include 3GPP TS 33.108 and/or ETSI TS 102 232-1 (Part 1), ETSI TS 102232-5 (Part 5)'.

2.9 Roaming

In case a target moves to an area outside of service provider's coverage area but facilitated by roaming facility, then all calls made to and from target (when provisioned in visited PLMN), while availing roaming facility shall be intercepted and CC, IRI & other information transacted through Value Added Service shall be provided in near real time.

For proper provisioning and interception in the Inter/Intra service areas roaming latest DoT administrative orders/ Instructions/ guidelines shall be adhered to.

2.10 Incorporation of monitoring facility for new value added services:

There shall be provision to incorporate monitoring facility for Value Added Services in the network as and when a service provider starts a new Value Added Service. In addition to CC, complete details (IRI) including calling number, date, time, equipment ID / Location etc. shall also be recorded. It shall be possible to extend these details to the security agencies in real time.

2.11 Other Interception related requirements

i. Provision shall exist to simultaneously send the CC and IRI of a target subscriber to at least ten monitoring agencies. **(latest DoT administrative orders/ Instructions/ guidelines shall be adhered to).**

ii. The equipment shall support fan out of IRI simultaneously **(as per latest DoT administrative orders/ Instructions/ guidelines)** both in ETSI format and any other globally standardized format in real time and also in readable (txt, excel, xml or as specified by the tendering authority).

iii. The equipment shall be able to detect the services being accessed as defined in clause 2.1.1.

iv. The CC and IRI shall be provided in a way that allows for their accurate correlation as per ETSI standard ES 201671. The CC and IRI for WCDMA (video calls) shall be provided in a way that allows for their accurate correlation as per 3GPP TS 33.108 recommendations. For IMS network, the mediation equipment should follow

specifications 3GPP TS 33.108 and/or ETSI TS 102 232-1 (Part 1), ETSI TS 102 232-5 (Part 5) for correlation of IRI and CC.

v. The equipment shall support static as well as dynamic allocation of target on the E1 time slots.

2.12 Interfaces between LIS and equipment of monitoring agency

2.12.1 Interface for transmission of call content

i. The system shall support at least ten nos. of 30 Channel PCM links at 2048 kbit/s as per ITU-T recommendations G.703 towards monitoring agency (ies) for transmission of the CCto monitoring agencies. **(latest DoT administrative orders/ Instructions/ guidelines shall be adhered to).**

ii. The sytem shall support IP Connectivity of atleast 64 Kbps per call between MDF2 and LEMF. The BW shall be scalable as per number of intercepted targets provisioned.

iii. Each of these links may be built up to different destinations or a group of these links may be terminated on a destination (monitoring agency).

iv. The CC shall be transported using one of the channels of 2048 kbit/s PCM link. Voice shall be delivered according to ITU-T recommendations G.711, A-law encoding. The CC for video calls shall be transported as per 3GPP TS 33.108 recommendations. Video and audio data shall be multiplexed data according to the 3GPP TS 26.111 & ITU-T recommendation H.223.

v. In case same target is monitored by different agencies, the CC from the same target subscriber shall be transported to different agencies using multiple 64 kbit/s channels on the respective PCM links connected to monitoring agencies.

vi. It shall be possible to assign a time-slot (circuit) on a link to any of the subscribers under monitoring observation, through Man-machine command(s). (Optional).

vii. Signalling

The signalling between the PLMN and LIS shall be one of the following:

- CCS7 as per National standards for MTP and ISUP No. SD/CCS-02
- ISDN PRI as per TEC GR SD/ISN-01
- SIP signalling on IP (for IMS) as per 3GPP TS 33.108 and/or ETSI TS 102 232-1 (Part 1), ETSI TS 102 232-5 (Part 5)

2.12.2. Interface for Transmission of IRI

The interface between the PLMN and the equipment at the monitoring agency for transmission of IRI to monitoring agency in real-time shall be as follows:

i. ISDN dial-up

ii. TCP/IP (Transmission Control Protocol/ Internet Protocol) protocol using FTP (File Transfer Protocol) for data transfer.

iii. The IRI shall be retained in respective network elements/LIS for 2 weeks even after its successful transmission to the monitoring agency **(latest DoT administrative orders/**

Instructions/ guidelines shall be adhered to) or as per procurer requirements

iv. IRI shall also be provided in real-time. In case real time is not possible, then stored IRI shall be transmitted once in every 5 minutes' **(latest DoT administrative orders/ Instructions/ guidelines shall be adhered to)** or as per procurer requirements

2.13 Man-Machine Commands:

Following operation & management features shall be available:

i. The operations related to target interception and monitoring shall be supported by the following (minimum set) of MML commands /GUI option:

a. Add: To create a target on request from an authorised monitoring agency even with future start & end date/time.
b. Remove: To remove a target from interception on request from an authorised monitoring agency. Automatic deactivation after expiry of time and notification to monitoring agency.
c. List: Interrogation of one or all the targets with print-out of all details. It should also be possible use these commands based on electronic input from monitoring agency.

ii. It shall be possible to retrieve the IRI stored in the PLMN selected on the following criteria:

- Date
- Target
- Calling number
- Called number
- Time
- Cell Id
- Location area
- Any other criteria mentioned by procurer

iii. Access to all MML commands related to line interception and monitoring shall be controlled through a multi-level password mechanism.

iv. It shall be possible to store all the commands and responses related to interception given from the O&M terminals in the respective network elements, in a 'command log' in the system disk, which is separate from the normal 'command log'. This command log shall be a 'read only' file, which can be read by authorised personnel whenever required, using MML. System will automatically purge this read only command log after a predefined period of **time (latest DoT administrative orders/ Instructions/ guidelines shall be adhered to)** – which will be configured only at the time of system installation. Alternately, authorised personnel shall be allowed to purge these logs through MML.

v. Reports to be provided like active number of current targets,expirying targets etc. Also reports of CC & IRI counters with in period should be available

2.14 Requirements of MSC based core network for interception:

i. The switching system shall support interception of at least 480 targets per PLMN simultaneously with at least 30 simultaneous calls for each of the designated security/ law enforcement agencies. It shall be possible to define up to a maximum of 3000 targets in each MSC **(latest DoT administrative orders/ Instructions/ guidelines shall be adhered to).** All interception related elements shall be synchronized

ii. Interception and monitoring shall be possible for the entire duration of the call without losing any part of communication, and the activation of any supplementary service by the subscriber under line interception shall not affect the monitoring.

iii. The system shall indicate 'start of the call' and 'end of the call' to the monitoring equipment.

iv. Interception shall be possible for all originating and terminating calls, to and from the target subscribers. Access to the entire telecommunications transmitted or caused to be transmitted to and from the target subscriber shall be supported for the services being accessed as mentioned in clause 2.1.1.

v. No indication whatsoever should be given to any Operation & Maintenance (O&M) personnel or the target subscriber that intercept function has been invoked on the target.

vi. The line interception shall not affect the basic and supplementary services of the target subscribers.

vii. The IRI), shall be stored in a separate file (read only) in the system disk, for retrieval and printing whenever required. The IRI stored in the system shall be transferred to the monitoring agencies using interfaces specified this chapter. The data transfer mechanism shall be supported by a set of Man-Machine Commands.

viii. In case of failure to send the CC on channels towards monitoring equipment due to any reason, it shall be indicated in the IRI stored in the PLMN and sent to the monitoring equipment.

ix. Normal observations initiated on the subscriber number as part of operation and maintenance procedures shall not be affected due to interception initiated on the subscriber number.

x. In case of Mobile Switch overload, interception mechanisms shall be given priority by the MSC.

xi. It shall be possible to send only the IRI for a target, without transmission of call content.

xii. In case of circuit switched communication, it shall comply with ETSI standards ES 201 671 so as to support accurate co-relation of CC and IRI. It shall be possible to provide IRI in readily usable format. In case of packet communication, the CC and IRI shall be in readily usable format. The GUI shall support suitable options so that various fields (as applicable) such as Lawful Interception Identifier (LIID), Network Identifier (NID), Communication Identity Number (CIN), Communication Identifier CID), and CC Link Identifier (CCID) are configurable as per user requirement. It shall be possible to report all supplementary services to Law Enforcement agency (LEA) as per ETSI standard ES 201671 and it shall not have any impact on the interception function. In case of circuit switched communication for video calls, it shall comply with 3GPP TS 33.108 recommendations.

xiii. The data transfer mechanism shall be supported by a set of MML commands /GUI options.

xiv. Line Monitoring

a. The system shall provide a facility to monitor speech for the complete duration of the call for all terminating and origination calls to monitoring positions. The monitoring positions shall be defined as subscriber number in the same switch area and /or any other mobile/ PSTN number in the National Network. It shall not be possible to define international numbers as monitoring position.

b. An indication shall be given by 'ring' to the monitoring position whenever a call is made from / to the subscriber under observation.

c. It shall be possible to put subscriber under monitoring observation and created operator positions for monitoring using Man Machine Commands. It shall be possible to define a one-to-one correspondence between a subscriber under monitoring observation and an operator.

d. The monitoring shall be possible without any indication/intrusion to the calling and called subscribers.

e. The call related details for monitored subscribers shall be stored in a separate file (read only) in the system disk in a secure manner, for retrieval and printing whenever required.

f. It shall be possible to monitor the call based on Calling Number, Called Number or initial digits of these numbers.

g. It shall be possible to interrogate the list of targets and monitoring positions using man-machine commands under high level password.

h. Wherever a call is made to the monitoring positing, CCS7 messages shall support delivery of calling Number in adding to monitored number and monitoring positing number.

i. The number of lines/subscribers that can be provisioned for line monitoring for MSC, PCN, SMSC etc., shall be at least 3000 per element/node expandable as per requirement of the operator. **(latest DoT administrative orders/ Instructions/ guidelines shall be adhered to).**

2.15 Requirements for PCN for interception

a. PDSN for CDMA, PS Core for GSM/WCDMA and EPC for LTE shall support provisioning, by node console, for LI system shall support provisioning, by node console, for LI system.

b. The Packet Core Network (PCN) shall support LEAs for all packet services for both access methods, namely simple IP and Mobile IP. A duplicate stream of packets shall be sent to an authorized collection point. The packets shall be duplicated before any network level encryption is applied.

c. It shall be possible to monitor or trace communication of any subscriber served by a PDSN for CDMA ,PS Core for GSM/WCDMA and EPC for LTE.

d. be possible to monitor or trace communication of any subscriber served by a PDSN. Call content and other associated data shall be deliverable to the proper legal authorities. This information must not be available or may not be reported to unauthorized personnel.

e. The monitored packets shall be in assembled form to provide complete readable in formation transacted along with relevant header information, irrespective of routing of the information /packets.
f. Monitored information shall contain IRI like sender address, destination address, date and time of forwarding the message, notification of successful delivery of message etc.
g. Monitored packets/messages shall be transported on a (pre-defined IP address) to the user agency in sequence and with correlated data where it should be stored in separate directory.
h. The system shall provide facilities for printing, storing, transferring and concurrent/post storage analysis.
i. It shall be possible to monitor the messages transacted simultaneously by multiple monitoring agencies.
j. It shall support TCP/IP for export of CC for packet switched calls.

2.16 Requirements for MMSC for interception

a. The lawful interception functionality shall enable to mark certain subscribers for Lawful Interception and intercept the messages. In this case the logs of the subscribers' actions (submitting, forwarding, and receiving of MM's) shall be recorded and saved to Lawful storage device. It shall be possible to copy-forward the submitted and received MMs for marked subscribers to multiple Lawful Interception addresses within the operator domain. The MMS can be text, video clips etc.
b. Lawful interception functionality shall enable the lawful interception authority to set a Legal Interception (LI) flag for marked MMS subscriber. When a message is stored to the message store, a second copy shall be stored to the Legal Interception store by a hidden copy address command. The data transfer shall be in encrypted form to hide sensitive information from unauthorized users. Personnel with the appropriate access rights shall be only able to use the LI function, access, decrypt and view the messages.
c. When a message enters the MMSC a check shall be done on Legal Interception (LI) flag and an interception may take place by sending a copy of the message to the configured address (hidden copy address) of Legal Interception store. The message shall be intercepted at the earliest possible time. Even for messages that cannot be delivered to the recipients (e.g. because resolving of the recipients fails), a copy of the intercepted message shall be sent to the configured address. For intercepted messages no read-replies and/or delivery reports shall be generated. Message interception shall also take place in case a message is forwarded or diverted by or to a subscriber.
d. It shall be possible to have MSISDN level real time monitoring.
e. It shall support simultaneous monitoring by at least ten external agencies and 30 targets for each agency.

2.17 Requirements of SMSC for Interception

a. The SMSC shall have facility to query the short messages that are stored in the SMSC's relational database prior to their delivery and viewing the textual contents of a short message, identifying the SME from which the message originates and its destination, check the priority, class and status of the message and other information relating to the

message's routing and handling. This facility shall be available to super user only (to the authorized personnel in a secure manner).

b. It shall be possible to extend the intercepted messages of the target subscribers (at least 3000) to the monitoring equipment. **(latest DoT administrative orders/ Instructions/ guidelines shall be adhered to).**

c. The SMSC shall forward the monitored SMS in TCP/IP protocol to the monitoring equipment.

d. It shall have provision for lawful interception to monitor/identify all

2.18 Requirements for Location Management Function (LAF / LARF / LCS Interception): Location Accuracy Details as per Latest DoT administrative orders/ Instructions/ guidelines shall be adhered to**.**

a. The system shall support Location Acquisition requests via LAF→LARF and report accurate location based on RAT capability (NR, LTE, UMTS, GSM).

b. The LAF shall return target location regardless of subscriber activity state:

- Idle/Connected
- Paging events
- Emergency services
- Registration update
- TA/LA/RA updates

c. For EPS/5G, the system shall provide:

- TAI / ECGI / NCGI
- UE presence status
- Timestamp
- Serving MME/AMF ID
- UE RF parameters where supported
- Positioning method used (OTDOA, ECID, GNSS, NR Positioning)

d. For 5G, the system shall support high-accuracy LI positioning as per 3GPP TS 38.305/33.126, especially for indoor and IoT devices.

e. The LI system shall retrieve location information from LMF, GMLC, and AMF whenever lawful location requests are invoked.

f. LALS shall support all LEA-mandated triggers.

2.19 Requirements of MME based core network for interception:

a. The MME shall support interception of at least 3000 number of LI targets mandated by DoT and shall allow simultaneous IRI delivery and CC interception through S1-MME and S11 signalling. **(latest DoT administrative orders/ Instructions/ guidelines shall be adhered to).**

a. The MME shall generate IRI for all NAS events involving the target, including Attach, Detach, TAU, Service Request, Authentication, Session/Bearer modification, and IMS voice/SMS registration events.

b. The MME shall provide IRI whenever mobility or subscriber context changes:

i. Tracking Area changes
ii. eNodeB handovers
iii. MME relocation
iv. Serving GW relocation

c. For packet data sessions, the MME shall supply all IRI parameters listed under EPS requirements in clause 2.3, including APN, PDN connection ID, bearer ID, user IP address, QCI, ARP, SGW/PGW addresses, GUTI, TAI, CGI/ECGI.

d. The MME shall support interception activation via LI_X1 interface and shall activate POI functions for both IRI-POI and CC-POI as per provisioning from ADMF/LIPF.

e. The MME shall ensure that interception does not delay NAS procedures such as Attach/TAU or cause call setup failures.

f. The MME shall support real-time reporting to MDF2 through LI_X2, even during MME pooling or load-balancing scenarios.

g. It shall be possible to intercept IMS-based SMS (SMS over SGs) when routed through MME, and IRI shall include IMSI, MSISDN, UE IP, SGs APN, SGs events, and SMS-related NAS signalling.

h. In case S1-MME failure prevents CC delivery, the MME shall record the IRI failure reason in the IRI record.

i. Interception shall be applicable to roaming subscribers served by the MME.

2.20 Requirements of Multimedia / IMS services (VoIP, IMS SMS, IMS conferencing)

a. The IMS core (P-CSCF, I-CSCF, S-CSCF) shall support IRI and CC interception for SIP signalling and media streams as per 3GPP TS 33.108 and ETSI TS 102 232-5.

b. IMS shall generate IRI for SIP events including:
i. REGISTER
ii. INVITE / UPDATE / BYE
iii. MESSAGE (for IMS SMS)
iv. OPTIONS
v. NOTIFY / SUBSCRIBE (conferencing)
vi. REFER / transfer events

c. IMS SMS shall produce IRI including: sender URI, receiver URI, text content CC, timestamp, home/visited network, routing function used.

d. IMS conferencing (AS) shall support:
vii. Participant join/leave events
viii. Conference creation/destruction
ix. Floor control events
x. Full media CC duplication for the target

xi. IRI correlation between SIP and RTP streams

e. Recording of VoIP/IMS media shall be based on RTP duplication prior to any RTP encryption unless network-provided encryption keys exist.

f. IMS shall support lawful interception for VoLTE/ViLTE/VoNR/ViNR.

2.21 Requirements of Requirements of AMF (5G Core Access and Mobility Management Function)

a. The AMF shall support lawful interception of all NAS messages in 5GS including Registration, Deregistration, Mobility Management, Authentication, Paging, Policy update, and UE Configuration updates.

b. The AMF shall generate IRI for all 5GS identifiers: SUPI, SUCI, PEI, GPSI, 5G-GUTI, IPv4/IPv6 address, S-NSSAI (Slice identity), and UE location details (TAI, NCGI).

c. AMF shall support dynamic LI activation through LIPF using X1_1 and LI_T (triggering interface) for service-scoped 5G interception.

d. The AMF shall correlate IRI with PDU Sessions established via SMF and include:
- PDU Session ID
- QFI (QoS Flow ID)
- DNN (Data Network Name)
- Slice/Service Type

e. The AMF shall support CC interception through CC-POI at UPF or SMF as per 3GPP TS 33.127, while ensuring that IRI generation at the AMF remains accurate and synchronized.

f. The AMF shall support IRI generation for both 3GPP access (NR/NG-RAN) and non-3GPP access (WLAN/ePDG/N3IWF) when AMF is anchoring the mobility context.

g. AMF shall support location reporting for Lawful Access Location Services (LALS) through LAF and LARF procedures.

h. Network slicing must not prevent interception; AMF shall report slice-specific identifiers without impacting services.

2.22 Requirements of Non-3GPP Access (ePDG, N3IWF, TNGF, WLAN Interworking)

a. The ePDG (4G) and N3IWF/TNGF (5G) shall support LI for untrusted WLAN access and derive IRI and CC for IPsec tunnels or N3IWF PDU sessions.

b. IRI shall include:
- UE MAC address
- NAI / EAP identity
- IPsec tunnel parameters
- UE IPv4/IPv6 address
- WLAN SSID/BSSID (where applicable)
- AMF/MME identity serving the session

c. CC interception shall occur at:
- UPF (preferred)
- ePDG (for LTE Wi-Fi offload)
- N3IWF user plane
- SMF-directed UPF duplication

d. The POI shall ensure correlation between WLAN session IRI and user-plane CC.

e. Non-3GPP access interception shall continue even if the UE switches between:
   • Wi-Fi → LTE → 5G NR
   • Wi-Fi → 5G slice
   • Multi-access PDU session (ATSSS) environments

f. ATSSS (Access Traffic Steering, Switching, Splitting) shall not hinder LI. Interception shall follow all active paths.

CHAPTER - 3

General Requirements

This chapter describes the general requirements of the Lawful Interception System (LIS) viz. Documentation, Environment, EMI/EMC, Safety, Power Supply, Quality etc.

3.1 Documentation

All documents to be provided by the supplier shall be in English language.

3.1.2 The documents shall comprise of:

i. System description documents
ii. System operation documents
iii. Training documents
iv. Repair related documents

3.1.3 System description documents

The following system description documents shall be supplied along with the system.

i. Over-all system specification and description of hardware and software.
ii. Installation manuals and testing procedures.
iii. Equipment layout drawings.
iv. Cabling and wiring diagrams.
v. Schematic drawings of all circuits in the system with timing diagrams.
vi. Detailed specification and description of all Input/Output (I/O) devices.
vii. Adjustment procedures, if there are any field adjustable units.
viii. Acceptance testing schedules.
ix. Spare parts catalogue - including information on individual component values, tolerances, etc. enabling procurement from alternative sources.
x. Detailed description of software describing the principles, functions and interactions with hardware, structure of the program and data.
xi. Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware & data.
xii. Program and data listings.
xiii. Source files (if required by the user)
xiv. Planning and system engineering documents.

3.1.4 System operation documents

The following system operation documents shall be made available.

i. Operating manual of the system.
ii. Maintenance manual.
iii. Man-machine language manual.
iv. Operation & maintenance manual for all I/O devices.
v. Fault location and troubleshooting instructions including fault dictionary.
vi. Emergency action procedures and alarm dictionary.

3.1.5 Training documents

Training manuals and documents necessary for organising training in installation, operation and maintenance and repair of the system shall be supplied.

3.1.6 Repair related documents

Documents required for carrying out repairs on various types of PCBs/ sub-systems etc. shall be made available.

3.1.7 Apart from the printed documentation, documentation data-base shall be provided in electronic media.

3.1.8 At least three complete sets of documents shall be supplied.

3.1.9 The structure and scope of each document should be clearly described.

3.1.10 The documents should be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information.

3.1.11 All diagrams, illustrations and tables shall be consistent with the relevant text.

3.2 Environment Requirements:

The system shall comply with the environment requirements as specified under category 'A' of TEC standard SD: QM-333.

3.3 EMI/EMC Requirements:

The equipment shall conform to the following EMC requirements for Class A:
The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report from accredited test lab shall be furnished from a test agency.

a) Conducted and radiated emission *(applicable to telecom equipment)*:

Name of EMC Standard: "CISPR 32 (2015) with amendment - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits: -
i) To comply with Class A (to be mentioned in the GR / IR as per the specific requirement) of CISPR 32 (2015) with amendment
ii) **.**

b) Immunity to Electrostatic discharge:
Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test".

Limits: -

i) Contact discharge level 2 {± 4 kV} or higher voltage;

ii) Air discharge level 3 {± 8 kV} or higher voltage;

c) Immunity to radiated RF:
Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test"

Limits: -
For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)
i) Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and

ii) Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

For Telecom Terminal Equipment without Voice interface (s)
Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

d) Immunity to fast transients (burst):
Name of EMC Standard: IEC 61000- 4- 4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test"

Limits: -
Test Level 2 i.e.
a) 1 kV for AC/DC power lines;
b) 0. 5 kV for signal / control / data / telecom lines;

e) Immunity to surges:

Name of EMC Standard: IEC 61000-4-5 (2014) “Testing & Measurement techniques for Surge immunity test"

Limits: -

i) For mains power input ports: (a)1.0 kV peak open circuit voltage for line to ground coupling (b) 0.5 kV peak open circuit voltage for line to line coupling

ii) For telecom ports: (a) 0.5 kV peak open circuit voltage for line to ground (b) 0.5 KV peak open circuit voltage for line to line coupling.

f) Immunity to conducted disturbance induced by Radio frequency fields:

Name of EMC Standard: IEC 61000-4-6 (2013) with amendment) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields”

Limits: -

Under the test level 2 {3 V r.m.s.}in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):

Name of EMC Standard: IEC 61000-4-11 (2004) “Testing & measurement techniques-voltage dips, short interruptions and voltage variations immunity tests”

Limits: -

i) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms(i.e. 70 % supply voltage for 500 ms)

ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and

iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.

iv) a voltage interruption corresponding to a reduction of supply voltage of >95% for 10s

.

Note: For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. TEC/SD/DD/EMC221/05/OCT-16 and the referenced base standards i.e. IEC and CISPR standards and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (h) and TEC Standard No. TEC/SD/DD/EMC221/05/OCT-16. The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	**Euro Norm**
CISPR 11	EN 55011
CISPR 32	EN 55032
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11
IEC 61000-4-29	EN 61000-4-29

3.4 Safety Requirements

The equipment shall conform to relevant safety requirements as per IS/IEC 62368- 1:2018 or Latest as prescribed under Table no. 1 of the TEC document 'SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT": TEC10009: 2024. The manufacturer/supplier shall submit a certificate in respect of compliance to these requirements.

3.5 Qualitative Requirements (QR)

3.5.1 The supplier/manufacturer shall conform to ISO 9001:2015 certifications. A quality plan describing the quality assurance system followed the manufacturer shall be required to be submitted. Alternatively, the equipment shall be manufactured as per guidelines issued by Quality Assurance wing (QA) of purchaser.

3.5.2 The failure of any component/subsystem in the system shall not result in the failure of complete system.

3.5.3 List of all components for which second source is not available shall be provided.

3.5.4 **Reliability and quality of service**

For the duration of the interception, the reliability of services supporting the interception shall be at least equal to the reliability of the services provided to the target. The quality of service of the intercepted transmissions forwarded to the monitoring facility shall comply to the performance standards of the network operator.

3.6 Security Requirements

3.6.1 Secure data network arrangements shall be provided between monitoring centre and the PLMN for the intercept function commands.

3.6.2 Provision of periodic target synchronization shall be available between monitoring centre and the exchange to ensure that targets already defined have not been removed and unapproved targets have not been included in defined targets in the exchange, when target administration is done by LEA.
The authorized user of the LEA shall be able to start the target synchronization process manually, whenever necessary.

3.6.3 Secure network arrangements shall be provided between Network Element and the monitoring agency to ensure that network related data and the communication content reaches only the appropriate authorities.

3.6.4 Suitable safeguards shall be provided in the man-machine communication program to debar unauthorized persons from making any changes in the memory contents or office data. Access to system operations shall be controlled in a secure manner through multi-level password and authentication check.

3.6.5 Suitable safeguards for security of Mediation Equipment like protection from public domain, safe retention of information/data/observation shall be there.

3.6.6 It should not be possible for non-authorized personnel to read the list of target subscribers.

3.6.7 No indication whatsoever should be given to any O&M personnel or the target subscriber that intercepts function has been invoked on the target.

3.6.8 System shall be secured against computer based viruses.

3.7 Hardware Requirements

i. Compact and high-performance state-of-the-art hardware shall be used.

ii. The hardware platform shall be open-ended and modular in architecture so that the equipment can be augmented and adapted to customer requirements.

iii. The system shall have adequate redundancy so that the total system availability is 99.999% or better for the duration of the monitoring and the call content and call related information shall be stored in full without losing any part of the communications.

iv. Adequate redundancy shall be built into the design of the system so that failure of a single sub-system does not affect the performance and the features of the monitoring equipment.

v. The system shall be comprised of different units for processing sub-system, network interfaces, storage, monitoring positions and User interfaces for operation and management.

vi. Processing sub-system: The equipment shall have a redundant processor configuration working in active and hot standby mode. Each processor shall have its own hard-disk for main storage. The data in the stand-by disk should be updated periodically from the active disk. In case of failure of the active processor, the standby processor shall become active automatically with zero downtime.

3.8 Software

i. The software shall be open-ended and modular in architecture so that the entire system can be augmented and adapted to customer requirements. It shall be possible for LEA to load and integrate software for advance features related to language, speech and accent identifications.

ii. The normal operation shall not be affected while undertaking software updates, enhancement of features or correction to programs.

iii. The design of the software shall be such that the system is easy to handle both during installation and normal operations.

iv. The functional modularity of the software shall permit introduction of changes wherever necessary with least impact on other modules.

v. Adequate flexibility shall be available to easily adopt changes in technological evolution in hardware.

vi. The software shall provide sufficient checks to monitor the correct functioning of the system.

vii. Test programs shall include fault tracing for detection and localization of system faults.

viii. Facilities shall be in-built to ensure automatic system reconfiguration on detection of any major software fault.

ix. The system hardware/software shall not pose any problem due to change in date and time by events such as changeover of millennium/century, leap year etc., in normal functioning of the system.

3.9 Storage

i. Adequate capacity for the purpose of storage and playing back for the various forms of communication content i.e. voice, fax and data shall be provided. The supplier shall provide details for the calculation of disk capacity.

ii. The communication content for each target shall be stored in a separate area in the disk. It shall be possible to retrieve and present the communication contents, target-wise to an operator at a monitoring position, whenever requested through man-machine commands/GUI.

iii. **Main storage:** The equipment shall be capable of storing at least 400 hours of uncompressed signal in the duplicated system disk. **(latest DoT administrative orders/ Instructions/ guidelines shall be adhered to).**

iv. **Secondary storage**: It shall be possible to transfer the contents of the main storage to a magnetic media e.g. audio tapes, optical disk etc. It should be possible to retrieve the contents, target wise and call-wise from the secondary storage. equipment required for off-line playback presentation of the call content from the secondary storage shall be supplied as part of the monitoring equipment.

3.10 Operation and Management

3.10.1 A user-friendly GUI (Graphical-User-Interface) shall be provided for easy administration of the equipment. It shall be capable of performing all functions related to administration, management, supervision and maintenance of all kinds.

3.10.2 Adequate number of man-machine interfaces and Input/output devices shall be provided to facilitate operation and management.

3.10.3 The operation and maintenance shall be supported by a set of user-friendly man-machine commands. Man-machine language shall be in English by providing English based commands and responses.

3.10.4 (a) Suitable safeguards shall be provided in the man-machine communication programs to debar unauthorized persons from making any changes in the data contents stored in memory.

(b) Access to system operations should be controlled through multi-level password and authentication checks.

3.10.5 The man-machine language shall have facility for restricting the use of certain commands or procedures to certain staff/terminals.

3.10.6 Calendar management for operator commands shall be available (It shall be possible to execute any command at any time by attaching a time tag to command and it shall be executed when the real time marches the time tag).

3.10.7 It shall be possible to store a log of commands and responses in a read-only file in the system disk, which can be retrieved whenever, required using man-machine commands.

3.10.8 The normal operation of the equipment shall not be affected while undertaking hardware expansion or enhancement of features.

3.11 System supervision

3.11.1 Provision shall be made for continuous testing of the system to allow both system quality check and fault indication as a fault arises.

3.11.2 The equipment shall provide for print-outs and visual/audible alarms to assist in efficient administration.

3.11.3 The visual display and the devices for manual control of the different parts of the system shall preferably be centralized on a supervisory panel. Details of the displays and the control arrangement shall be provided.

3.11.4 In case a fault is detected requiring reloading of the program, this shall be carried out automatically. There shall be a provision for manual-loading of the programs/software modules.

3.12 Maintenance facilities

3.12.1 The system shall have the capability to monitor its own performance and to detect, analyze, locate, and report faults.

3.12.2 The equipment design shall be such that any special care and precautions on the part of the maintenance personnel are kept to an absolute minimum.

3.12.3 The maintenance spares supplied shall take into account the MTBF and MTTR. The supplier shall accordingly supply number of spares for a period of 3 years. At least one spare PCB of each type shall be supplied.

3.13 Diagnostic capabilities

3.13.1 The diagnostic capability of the system shall be such as to minimize the human efforts required. To this end, the supplier shall indicate how much of the diagnostic program are normally resident in the on line program. Details of the off-line diagnostic program shall be given. The procedure for invoking such program shall be described. The procedure for consulting fault dictionary for diagnostic program shall be made available.

3.13.2 All the hardware testers necessary for efficient maintenance of the system shall be provided. Details of the testers shall be indicated.

3.13.3 The test procedures, recommended for efficient maintenance of the system, shall be indicated. This shall include details of the testes, their periodicity, etc.

3.13.4 Any malfunction in the system shall initiate a fault message and/or visible and audible alarm. The fault information shall direct personal to the appropriate maintenance manual for location of the fault unit or for detailed procedures on further action to be taken for rectification of the fault conditions. The classification of alarms in the system shall be indicated.

3.13.5 A suitable alarm and display system shall be provided for a continuous indication of the system status. Provision shall be available to extend the alarm indication to centralized place.

3.14 Power Supply

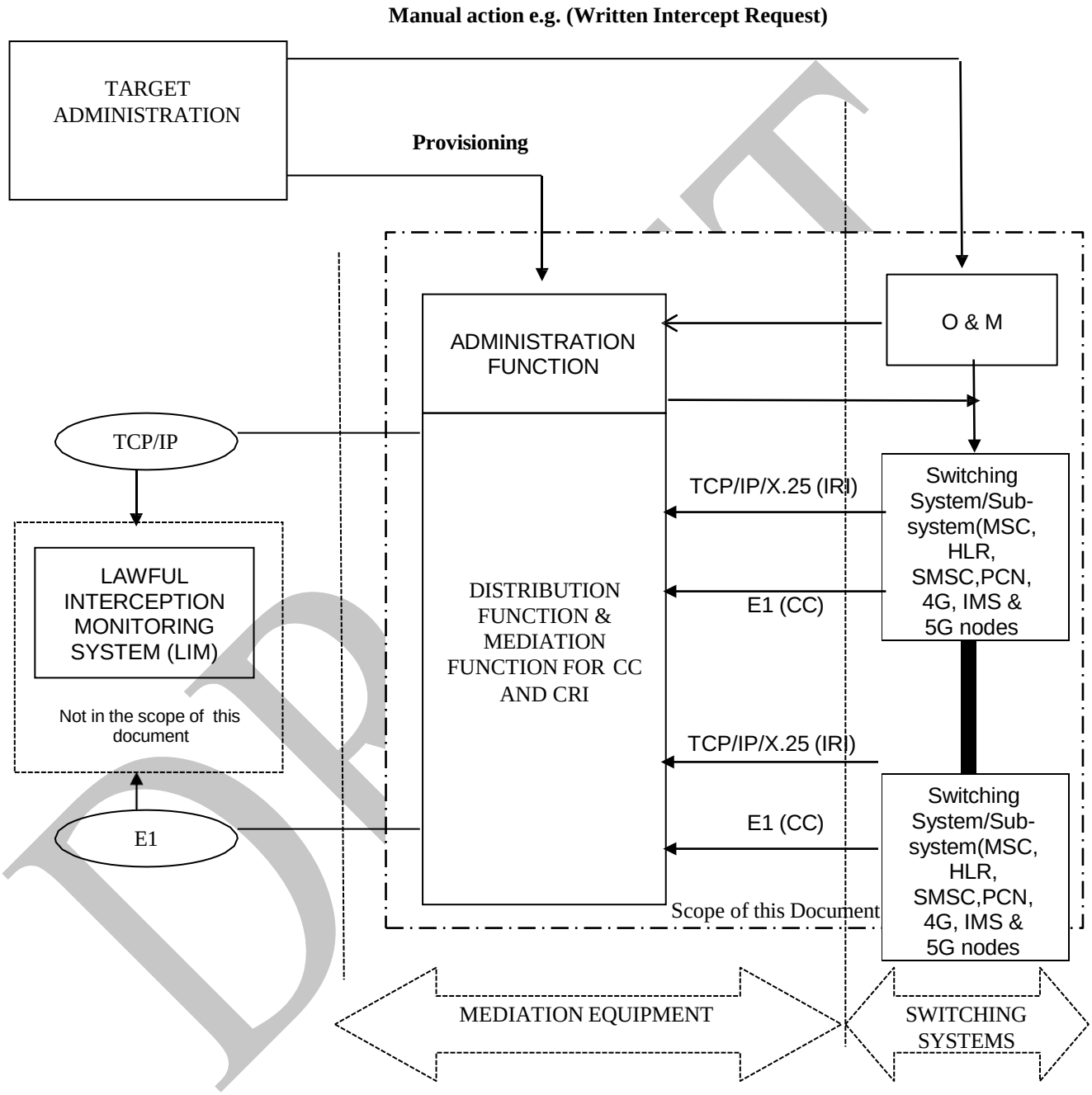
3.14.1 The equipment shall be capable of working with an input AC Mains supply of 230 Volts with a tolerance of -15% to 10 % and frequency of 50 Hz $\pm$ 2 Hz. Or DC power supply of -48V.

3.14.2 Switching Mode Power Supply (SMPS) and VRLA battery to be used shall be as per TEC Generic Requirements No. GR/FLA/SMP–001 and GR/BAT-01 respectively. Power supply and battery shall be modular and expendable to support the ultimate equipment configuration.

3.14.3 UPS and other power requirements are to be specified by the system supplier.

Annex.-1

The general architecture for Lawful Interception and Monitoring System is shown in the figure given below:



CC- COMMUNICATION CONTENT
IRI- INTERCEPT RELATED INFORMATION

Figure-10: General Architecture For Lawful Interception And Monitoring

ABBREVIATIONS

ADMF	Administrative Function
AoC	Advice of Charge
AP	Access Provider
BRI	Basic Rate Interface
CB	Call Barring
CC	Communication Content
CCS7	Common Channel Signalling
CGI	Cell Global Identity
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CS	Circuit Switched
CSCF	Call Session Control Function
CUG	Closed User Group
DF	Delivery Function
EMC	Electromagnetic Compatibility
EPS	Evolved Packet System
ESN	Equipment Serial Number
FTP	File Transfer Protocol
GPRS	General Packet Radio System
GUI	Graphical User Interface
HI	Handover Interface
HLR	Home Location Register
ICE	Interception Element
IMEI	International Mobile Equipment Identity
IMS	IP Multi-media Sub-system
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IRI	Intercept Related Information
IS	International Standard
ITU	International Telecommunication Union
LAC	Local Area Code
LBS	Location Based Services
LAP-B	Link Access protocol - B Channel
LEA	Law Enforcement Agency
LEMF	Lawful Enforcement Monitoring Facility
LIS	Lawful Interception System
LU	Location Update
MBMS	Multimedia Broadcast/Multicast Service
MDN	Mobile Directory Number
MIN	Mobile Identification Number
MMC	Man Machine Commands
MML	Man Machine Language
MMS	Multi-media Messaging service

MMSC	Multi-media Messaging Centre
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber ISDN Number
NAI	Network Access Identifier
NWO	Network Operator
OMA	Open Mobile Alliance
PCM	Pulse Code Modulation
PCN	Packet Core Network
PDSN	Packet Data Serving Node
PRI	Primary rate Interface
PS	Packet Switched
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Connection
QoS	Quality of Service
QR	Qualitative Requirements
SIP	Session Initiation Protocol
SMPS	Switch Mode Power Supply
SMSC	Short Message Service Centre
SvP	Service Provider
TCP	Transmission Control Protocol
TEC	Telecommunication Engineering Centre
UMTS	Universal Mobile Telecommunication System
UPS	Uninterrupted Power Supply
VC	Virtual connection
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRLA	Valve Regulated Lead Acid battery
WAP	Wireless Application Protocol
WLAN	Wireless Local Area Network
3GMS	3rd Generation Mobile System
3GPP	3rd Generation Partnership Project

-- END OF THE DOCUMENT --