ChatGPT

# Comprehensive Summary of Lawful Interception (ETSI Standards Overview)

## Introduction

**Lawful Interception (LI)** refers to the legally authorized surveillance of telecommunications by law enforcement. ETSI and 3GPP have developed detailed technical specifications to standardize how communication service providers implement LI. These specifications define the **technical requirements**, **system architecture**, **interfaces and procedures**, and **service-specific interception details** for various communication services (IP-based services, messaging, internet access, layer-2 access, and mobile networks). The goal is to ensure that intercepted **Intercept Related Information (IRI)** (metadata/events) and **Content of Communication (CC)** (actual communications content) are delivered reliably and transparently to Law Enforcement Monitoring Facilities (LEMFs) without detection by the target [1]. All interception must meet strict requirements for timeliness, completeness, security, and privacy protection as outlined in the standards.

This report summarizes the key points from the ETSI LI deliverables: **TS 103 280** (common LI parameters dictionary), **3GPP TS 33.108** (handover interfaces for LI in GSM/UMTS/LTE, with versions 12.8.0 and 15.3.0 compared), and ETSI **TS 102 232** parts 1, 2, 3, 4, 7 (covering IP delivery, messaging, internet access, layer 2, and mobile service interception respectively). We outline general technical requirements and architecture, describe the standardized LI interfaces and procedures, detail interception for each service category, and note major changes introduced in newer document versions.

## 1. Technical Requirements for Lawful Interception

ETSI's LI standards set forth clear requirements to ensure that interceptions are effective, reliable, and legally compliant. **Identification of target communications** is paramount: the network must be able to intercept communications **based on various target identifiers** appropriate to the service [2] [3]. For example, an internet access target might be identified by username (Network Access Identifier), IP address, MAC address, dial-in number, cable modem ID, etc., as available in that service context [3]. All such identifiers **must uniquely match the target** and be determinable "without unreasonable effort" by the provider [2]. (In mobile networks, targets may be identified by MSISDN, IMSI, IMEI or other subscriber IDs [1]. Each call or session leg is associated with these IDs for interception purposes.)

**Completeness of intercept:** The provider must ensure **all relevant communications and events are captured** for the target's services. This means the LI system should **monitor all simultaneous communications** initiated or received by the target across the provider's network, at each relevant intercept access point [4] [5]. For each target service under interception, the network must provide *Intercept Related Information* (IRI) records for significant events *and* the *Content of Communication* (CC) where authorized [6] [7]. For example, in an Internet Access Service (IAS) context, IRI must be generated when the target attempts to access the network, when access is granted or denied, on status changes (e.g. logon/logoff), and on location changes [6]. The IRI should contain details like identities used (e.g. calling line number, access device ID), service parameters, status info, and timestamps for each event [7]. Likewise, **content** (such as voice call audio, email body, or IP packets) must be duplicated and delivered for each communication session once interception is activated [8] [7]. The standards emphasize that *both* IRI and CC for every intercepted communication must be forwarded to law enforcement in a timely manner.

**Timeliness and transparency:** Interception must not introduce significant delays or alterations in the target's service. The specifications require that any delays in generating IRI are only those inherent in normal protocol handling and automated forwarding by the intercept function [9]. In other words, intercept should occur in *real time*, and **no unnecessary latency** is added by the LI mechanism. Moreover, the LI process must be *covert* – undetectable to the target and other unauthorized parties. This includes not only ensuring the target's service experience is unaltered, but also maintaining strict confidentiality of intercept operations. Providers are required to implement **security measures** so that only authorized personnel/functions know of and can access intercept data. For example, ETSI TS 102 232-1 provides an option for **payload encryption** of intercepted content between the provider and LEA (using TLS or an Encryption Container) to protect confidentiality [10] [11]. Authentication and integrity checks are also mandated for the handover interfaces to prevent tampering [12] [13].

**Reliability and accuracy:** The LI system should be robust against failures that could cause loss of data or collection of extraneous data. The standards stipulate mechanisms to **detect and prevent "over-collection" or "under-collection"** of data [14]. For instance, if a system fault could lead to intercepting communications not actually belonging to the target (over-collection) or failing to capture some target communications (under-collection), the provider must detect this anomaly, take corrective action (e.g. stop the intercept if needed), and report the issue to the LEA [15] [16]. An example given is if an IP address lease expires without a proper logoff event (perhaps due to a missed message), there is a risk that the IP could be reassigned to another user – the LI system must stop intercept on that IP to avoid over-collecting someone else's traffic [16]. Another example: if intercept was set on an IMEI (device identifier), there might be a delay in intercept activation at call start and inability to capture non-call events [1]; systems and law enforcement should be aware of such limitations. Overall, **system monitoring and alarms** are required so that any software, network, or hardware failures affecting interception are quickly detected and addressed [14].

**Performance and capacity:** LI systems must handle the volume of data associated with target communications. ETSI specifications like TS 101 671 (the base requirements) and TS 102 232-1 define performance metrics such as the maximum tolerable latency for delivering IRI/CC to the LEMF, buffering requirements, etc. For example, the delivery function should forward intercept data with minimal delay; any buffering should only cover transient network issues. Annex B of TS 102 232-1 outlines performance considerations (e.g. the LI system should timestamp events accurately and meet any timing constraints set by law enforcement) [17] [9].

**Common data formats:** A key requirement is use of standardized parameter formats and identifiers across all LI interfaces. ETSI **TS 103 280** (LI "Dictionary for common parameters") defines a library of common data types and fields used in intercept records [18] [19]. This includes identifiers like IMSI, MSISDN, IP addresses, email addresses, timestamps, location coordinates, etc., with consistent definitions and encoding. By using TS 103 280's dictionary, all parties ensure that (for example) a timestamp or an IMSI in an IRI record is interpreted uniformly [19]. TS 103 280 is regularly updated (v2.7.1 in 2021) to introduce new parameters (e.g. 5G identifiers like SUPI) and clarify definitions (such as date/time formats) in line with evolving services [20]. Adhering to these common parameters is part of the technical requirements, enabling interoperability between network operators' delivery functions and law enforcement systems.

In summary, the technical requirements enforce that LI must **uniquely identify the target, capture all required events/content, deliver them promptly and securely, and avoid any leakage or missed data**. These requirements are derived from high-level lawful surveillance mandates (e.g. ETSI TS 101 331 requirements) and are refined in each service-specific standard [17] for the peculiarities of that service (internet, mobile, etc.).

## 2. System Architecture for Lawful Interception

**Logical Architecture:** The lawful interception architecture is typically represented by a set of functional entities in the network, as shown in reference configurations (see *Figure 5.4* from 3GPP TS 33.108) [21] [22]. The architecture is logical – physical implementations may combine functions – allowing flexibility and integration [23]. The key elements include:

- **Administration Function (ADMF):** A dedicated function that handles LI administrative tasks, primarily the provisioning and management of interception orders (warrants). There is usually a single ADMF in the provider's network [24]. When law enforcement issues an intercept request via the secure HI1 interface, the ADMF authenticates and activates the warrant. The ADMF configures the relevant network nodes (or Intercept Access Points) to start intercepting the target's traffic. It also coordinates multiple simultaneous intercepts. For example, if multiple LEAs have warrants on the same target, the ADMF and associated delivery functions ensure each LEA receives a copy of the intercept product while the network elements (e.g. switches) remain unaware of the number of activations [24]. The ADMF thus isolates the network's service logic from the presence of multiple interception requests on a single target.

- **Intercept Access Point (IAP):** This is not a single device but rather a logical tap or function at a network element where communications can be intercepted. IAPs are implemented in network nodes like mobile switching centers, gateways, routers, email servers, etc., depending on the service. The IAP's job is to *duplicate the relevant data* — signaling and/or user traffic — for intercepted targets. For example, in a circuit-switched mobile network, the MSC (Mobile Switching Center) has an IAP function that forks call setup messages (IRI) and voice streams (CC) for targets. In an ISP's network, a broadband remote access server or packet gateway might serve as an IAP for internet traffic. There may be multiple IAPs for different services or parts of the network. Each IAP is configured by the ADMF with the target's identifiers so it knows which traffic to intercept [5] [1].

- **Mediation and Delivery Functions (MF/DF):** Raw intercepted data from IAPs is typically fed into **mediation functions** which format, encode, and deliver it to the LEA. ETSI architecture often distinguishes between *IRI Mediation Function (IRI MF)* and *CC Mediation Function (CC MF)* for handling intercept related information and content of communication, respectively [25]. These mediation functions ensure the data conforms to the standard handover formats (ASN.1, etc.) and apply any necessary encryption or filtering. The output is then passed to **Delivery Functions** DF2 (for IRI) and DF3 (for CC) which handle transport to the LEMF [25]. In practice, the mediation and delivery functions might be part of a single **Intercept Mediation System** device within the provider's network. They act as a buffer and protocol converter between internal network signals and external handover interface. Importantly, the mediation/delivery layer implements the **correlation** between IRI and CC streams. It uses a unique **correlation number and target identifier** (assigned per intercept instance) to tag intercepted packets/records, so that the LEA can re-associate the metadata with the correct content [26]. For instance, when a call is intercepted, the MSC provides a correlation number for that call along with the target's ID to DF2/DF3; the DF2/DF3 use those to ensure the call's voice packets (CC) and the call event records (IRI) both get labeled and routed to the same LEA monitoring that target [26]. This prevents mix-ups when multiple intercepts are in play.

- **Internal Network Interfaces (X1, X2, X3):** Within the provider's infrastructure, standard internal interfaces connect the above components. **X1** is the interface between the ADMF and the network's control elements (e.g. switches or service platforms) for sending intercept activation/deactivation commands. **X2** is the interface carrying IRI from network nodes (or IRI MF) to the IRI Delivery Function (DF2), and **X3** carries CC from network nodes (or CC MF) to the Content Delivery Function (DF3) [22] [27]. These X1/X2/X3 interfaces are defined in ETSI TS 102 232-5 and TS 103 221 (for internal network LI functions) and align with the 3GPP architecture (where X2/X3 correspond to the interfaces from an Intercepting Control Element or Gateway to the delivery function). The internal interfaces are often vendor-specific or implementation-specific, but recent ETSI work has aimed to standardize them (e.g. moving toward HTTP/2 and modern protocols on X1/X2) [28] [29] for consistency with 5G core networks.

- **Law Enforcement Monitoring Facility (LEMF):** On the receiving end, the LEMF is the law enforcement agency's system that collects and analyzes the intercepted data. It interfaces with the provider via the standardized **Handover Interfaces (HI)**. The LEMF receives HI2 (IRI) messages and HI3 (CC) streams, correlates them (using the provided identifiers), and presents them to investigators. It also handles the administrative interface (HI1) for warrant issuance and status messages. The ETSI standards assume the LEMF is a secure system capable of storing and processing intercept data, but its internal design is outside the scope of these documents.

Overall, this architecture ensures a **separation of concerns**: network elements generate the raw intercept data, but know little about warrants or LEA identities; the ADMF manages warrants and hides complexities like multiple LEAs; mediation/delivery functions format and forward intercept data reliably; and the LEA receives data in a standardized form. This modular approach makes it easier to update one part (e.g. adding a new delivery format) without overhauling everything.

**Correlation and identifiers:** The LI architecture makes heavy use of identifiers to manage and correlate information. A **Lawful Interception Identifier (LIID)** uniquely identifies each interception order in the system [26] [30]. Communication sessions are labeled with a **Communication Identifier** (which may be subdivided into a Network Identifier and Communication Number) to distinguish each intercepted call or session [26] [30]. These identifiers ensure that if a target is involved in multiple simultaneous communications (or if multiple targets are intercepted), the data doesn't get mixed up. For example, every IRI event and packet of CC for a given VoIP call will carry a common communication ID so the LEMF knows they belong together. In multi-party scenarios (conference calls, group chats), separate call legs may each get their own IDs, and there are provisions to link them if needed (such as a CC-Link identifier for multi-leg calls) [31] [32]. The use of these identifiers is a core aspect of the architecture enabling **traceability** of intercept data from the network to the LEA.

**Network-specific aspects:** Different network types integrate the LI architecture in different ways. In mobile/cellular networks, 3GPP defines specific **Intercepting Control Elements (ICE)** that are responsible for interception in each domain (circuit-switched ICE in MSC, packet-switched ICE in SGSN/SGW, IMS ICE in CSCF, etc.). These ICEs interface with the ADMF and delivery functions via the X2/X3 interfaces. In data networks (IP services, ISP environments), similar concepts apply: e.g., a broadband network gateway or AAA server might act as an ICE for internet sessions. In all cases, the principle is that **interception is performed as close as possible to the service logic** – so that complete metadata and content can be obtained – and then handed to a common delivery system.

**Example:** In a circuit-switched mobile call interception (see Figure 5.4 of TS 33.108), when the target makes or receives a call, the MSC/VLR (with an IAP/ICE) recognizes the target's identifiers (MSISDN/IMSI) as under interception and begins duplicating call control events (dialed number, call begin, end, etc.) as IRI and voice as CC. The MSC sends these to the operator's **Intercept Interface Function (IIF)** which comprises the IRI MF, CC MF, DF2, DF3, etc. [22] [26]. The ADMF ensures the MSC doesn't need to know *how many* LEAs will get the data – the DF2/DF3 will replicate the IRI/CC streams to each active warrant as needed [24]. The correlation number provided by the MSC links the call content with the call events, and DF2/3 route each to the correct LEA's LEMF [26]. Meanwhile, HI1 (administrative interface) is used separately to handle warrant info, delivery address setup, etc., which we cover next.

## 3. Handover Interfaces and Procedures

All communication between the service provider's LI system and the law enforcement agency's equipment is standardized through three **Handover Interfaces (HI1, HI2, HI3)** [33]. These correspond to the ETSI handover model defined in TS 101 671 (for fixed networks) and adopted in 3GPP TS 33.108 (for mobile):

- **HI1 – Administrative Interface:** This interface carries the administrative communications between the Law Enforcement Agency (LEA) and the Communication Service Provider (CSP). It covers the delivery of the interception authorization (warrant) from the LEA to the provider, as well as operational commands (activate intercept, deactivate intercept, etc.), and status reports. Essentially, HI1 is used to provision the target in the provider's LI system. For example, a warrant on a target's phone number arrives over HI1, and the ADMF acknowledges and implements it. HI1 may also carry certain **notification messages** (e.g. a notice to the LEA that a target's service has been suspended, or that an intercept can't be executed) [34]. In the standards, HI1 is largely out-of-scope regarding exact protocols – implementations historically used secure fax or email, but modern approaches use XML/HTTP-based requests. (In fact, recent ETSI work has been aligning HI1 with web technologies like HTTP/2 and adding support for new warrant parameters [35] [29].) **Important:** The content of HI1 messages (the warrant itself) is considered highly sensitive but in some architectures, certain HI1 info may be forwarded internally. For instance, ETSI TS 102 232-1 notes that HI1 warrant data might inform the delivery function which types of intercept (IRI-only or full content) to activate [36] [13]. Overall, HI1 ensures lawful authorization and management of the interception.

- **HI2 – Intercept Related Information (IRI) Interface:** This is the interface for delivering *metadata* about the target's activities to the LEA [33]. IRI encompasses signaling information, service usage data, and other events – essentially everything about the communication except the user payload. Examples include call set-up and tear-down events, numbers dialed, timestamps, IP addresses used, URLs visited, email headers, logon/logoff events, location updates, etc., depending on the service. The IRI is typically formatted into structured **IRI messages or records** and sent in near-real-time to the LEA. ETSI defines four basic types of IRI records to standardize event reporting [37]: **IRI-BEGIN** (indicating the start of a communication or session, e.g. a call attempt or session login) [38], **IRI-END** (the end of a communication, e.g. call hang-up or session logoff) [38], **IRI-CONTINUE** (any notable interim event during an ongoing session, e.g. a handover, mid-call location change, or an extended status report) [39], and **IRI-REPORT** (used for events that are not tied to a specific communication session, or general notifications) [39]. These help structure the metadata flow. For instance, when a target initiates a VoIP call, an IRI-BEGIN is sent with details of the call (caller ID, callee, time). If the call is ongoing for a long time, periodic IRI-CONTINUE records might report in-call events (like hold/resume). When the call ends, an IRI-END is sent. If the target's phone attaches to the network or performs a location update outside of a call, that could be sent as an IRI-REPORT (since it's not part of a specific call). The **procedures** for HI2 involve reliably sending these records as soon as they are generated. According to TS 102 232-1, the delay from event occurrence to IRI delivery should only be the time needed for normal protocol processing and forwarding; no intentional holdup is allowed [9]. If the network buffers IRI (due to temporary link outage to LEMF, for example), it must catch up once restored.

- **HI3 – Content of Communication (CC) Interface:** This interface carries the actual communication content of the target to the LEA [33]. This could be the live voice of a phone call, the full text and attachments of an email, the packets of an internet connection, messages sent in a chat application, etc. The CC is delivered **concurrently** with the communication (for live intercepts) or as soon as possible for stored/transient content. The procedures on HI3 depend on the service: For a traditional voice call, HI3 is a continuous media stream (voice packets or circuit audio) sent to the LEA's recording equipment. For a packet-data intercept, HI3 may consist of IP packet copies delivered in sequence. For an email intercept, the CC might be a file (the email content) delivered when available. The standards mandate that CC be delivered **in its entirety and unaltered**, except for any lawful filters (e.g. if only specific protocols are authorized to be intercepted). TS 102 232-1 specifies using an IP-based delivery for HI3 in modern systems – for example, intercepted circuit-switched voice can be packetized and sent over an IP network to the LEA using an ASN.1-defined format [40]. In practice, HI3 often uses protocols like RTP or file transfer over TCP, depending on content type, encapsulated within the standardized LI format. An important procedure is **synchronization**: the LI system correlates each CC stream with the corresponding IRI messages via identifiers (as discussed, e.g. Communication ID) so that, for example, the LEA can tell which call a given voice stream belongs to [41]. If multiple CC streams are active (say the target is in two calls or a call and a data session), they are delivered over separate channels each identified by the intercept identifiers.

To support these interfaces, ETSI TS 102 232-1 (Part 1 for IP delivery) defines a generic **transport protocol** over IP networks. This protocol uses TCP/IP connections (or TLS over TCP for security) to carry HI2 and HI3 data units to one or more LEMFs [10] [11]. Notably, the service provider's Delivery Function is typically the **TCP client (sender)** and the LEA's LEMF is the **TCP server (receiver)** in this setup [11] [42]. The standard recommends dynamic TCP port allocation for these sessions (source port chosen by CSP, destination port as arranged with LEA) [43]. A custom session layer rides on TCP to frame the IRI and CC "Protocol Data Units" (PDUs) along with header information, so the LEA knows what each chunk of data represents (IRI message, CC payload, keep-alive, etc.) [44] [13]. The protocol includes **acknowledgment mechanisms** to ensure reliable delivery [45]. For example, each PDU can be optionally ack'ed at the session layer to confirm the LEMF received it, beyond the protection TCP provides [45]. This is important because TCP alone doesn't guarantee the data was processed by the application – the session-layer ACK in TS 102 232-1 can provide positive confirmation at the LI application level [45]. The spec even outlines **keep-alive** messages at the session layer (instead of using TCP keep-alives) to detect link failures without interfering with congestion control [42]. Annex C of TS 102 232-1 gives guidance on TCP tuning (window sizes, selective ACK, path MTU discovery) to handle high-bandwidth intercepts with minimal packet loss or delay [46] [47]. In essence, the procedure on HI2/HI3 is akin to a client-server data feed: once an intercept is activated, the provider's system establishes secure TCP connections to the LEA, then streams IRI records (as ASN.1 encoded messages) and content (as per the specified format) in real time. If the connection breaks, the system should buffer data and retry for a defined period to prevent data loss [48] [45].

A crucial procedural aspect is the **start and stop of interception**. Upon receiving a lawful request on HI1, the provider's ADMF enables intercept for the target. This may involve provisioning filters (e.g. target's identifiers) into network nodes or packet probes. The LEA is typically notified via HI1 that intercept has been enabled (or if it failed). While active, the network will continuously generate HI2/HI3 as described. When the warrant expires or is terminated, the ADMF deactivates the intercept in all IAPs and stops the data feed, and might send an HI1 message indicating cessation. ETSI standards emphasize that deactivation must be **immediate** once authorization is gone, to avoid any unauthorized collection.

**Multi-service and roaming scenarios:** Modern procedures also handle cases like a target using multiple services or roaming to another network. If a target has several services (e.g. mobile voice, VoLTE, messaging) under intercept, typically each service is handled by the relevant service-specific intercept function, but all are tied to the same warrant (LIID) and delivered accordingly. If the target roams to another operator's network, lawful interception can become complex: 3GPP LI architecture allows either the home network or visited network (or both) to perform interception depending on agreements. For example, for a VoLTE user roaming with S8 Home Routing, the home network can intercept IMS signaling and media since they anchor at home, whereas with Local Breakout roaming, the visited network may perform intercept and deliver results independently [49] [50]. The standards ensure that in either case, intercept product includes indications of the roaming scenario (like whether it was home-routed or local breakout) so LEAs know which network provided the data [51] [52].

In summary, the HI1/HI2/HI3 interfaces and procedures are designed to cover the full lifecycle of an interception: from warrant authorization, through real-time collection of metadata and content, to termination and record-keeping. The use of standardized protocols (ASN.1 encoding, TCP/TLS transport) and message types (IRI-BEGIN/END, etc.) ensures that a LEA's monitoring system can interface with any CSP's delivery function in a consistent way.

## 4. Service-Specific Interception Details

Different communication services produce different kinds of intercept information. ETSI's TS 102 232 series is a multi-part deliverable that provides **Service-Specific Details (SSD)** for lawful interception, all built on the common framework of part 1 (the IP delivery handover spec). We summarize each relevant part and service category:

### 4.1 IP-Based Services and IP Delivery (Part 1)

**ETSI TS 102 232-1 (Handover Specification for IP Delivery)** defines the generic handover mechanism for delivering intercept information over IP networks. Rather than focusing on one user service, this part specifies how to transport intercept data (IRI and CC) in a standardized way (using IP, TCP, and ASN.1 encoding) for *any* service. Key points include:

- **IP transport and session:** As mentioned, part 1 mandates using an IP-based connection (typically TCP/IP) between the provider's Delivery Function (DF) and the LEMF for HI2 and HI3 [10] [11]. It describes how to initiate and manage these connections, including port usage and optional TLS security (for encryption and authentication) [10] [43]. The DF is the active party in opening the connection to a pre-defined LEA endpoint.

- **Encapsulation and formatting:** All intercepted IRI and CC are wrapped in ASN.1 defined "HI2/HI3 messages" as they cross the handover interface [44] [13]. Part 1 provides the base ASN.1 schema for these messages or references to them. For example, it defines header structures that indicate the type of payload (IRI or CC or administrative) and includes fields like the LIID, sequence numbers, timestamps, etc. so that the LEA can decode the stream properly [44] [13]. Annex A of TS 102 232-1 contains the ASN.1 syntax for HI2/HI3 message headers, and normative annex G covers payload encryption methods if used.

- **Session management:** The specification covers how the DF and LEMF manage the intercept session. This includes **connection establishment**, **heartbeat/keep-alive messages** at the application layer to detect dropped connections (since TCP keep-alives are discouraged) [42], and **tear-down** procedures. It also allows for **option negotiation** at startup (Annex I of part 1) where the DF and LEMF can negotiate capabilities like whether to use compression, encryption, or specific protocol options in the session. For instance, option negotiation might determine if IRI-only mode is used (for warrants that only require metadata) versus full content mode [44] [13].

- **Acknowledgments and reliability:** Part 1 introduces an optional *session-layer acknowledgment* for PDUs to ensure reliability on top of TCP [45]. The DF can be configured to consider a piece of data "successfully delivered" either when TCP ACKs it (default) or when the LEMF sends an explicit ack message back [53]. This flexibility allows tuning reliability vs. performance. The spec also sets guidelines for buffering within the DF: it must buffer enough data to handle retransmissions or temporary LEMF unavailability, but not so much as to cause undue delay. Timers (TIME3, TIME4, etc.) are specified for how long to keep data and how often to retry sending before giving up [54] [55]. The DF should log any data that ultimately could not be delivered so that the provider can inform the LEA post-fact.

- **Delivery Networks:** TS 102 232-1 discusses the types of networks over which intercept data might be delivered – e.g. dedicated private lines vs. public internet – and the security considerations for each [56] [57]. It specifies that if public networks are used, strong confidentiality and integrity (e.g. via TLS) are needed [57]. It also touches on timeliness requirements: intercept data should arrive at the LEMF with minimal delay (preferably in real-time for live monitoring) [58] [9].

In summary, Part 1 is the **technical backbone** that all other service-specific parts rely on. It ensures that no matter what the service (voice, email, web, etc.), the *way* the intercept gets from CSP to LEA is consistent. To illustrate, if a provider needs to deliver both a phone call recording and an email text via LI, both will be encapsulated using the Part 1 format over a single or multiple TCP connections to the LEA. This part has evolved over time to incorporate new requirements (e.g. higher bandwidth delivery, better encryption). A new version v3.22.1 (published 2021) even added support for 5G-specific notification types and network element identifiers, preparing the system for intercepting 5G traffic in a similar framework [59].

## 4.2 Messaging Services (Part 2)

**ETSI TS 102 232-2 (Service-specific details for Messaging Services)** covers interception of messaging applications, primarily focusing on **email** and related messaging (and later extended to chat/IM). The document defines what events constitute IRI for messaging, what content is captured, and any particular model for messaging systems. Key highlights:

- **E-mail interception:** Email can be intercepted at various points – when a target sends an email, when they receive an email, or when they retrieve email from a server. TS 102 232-2 lays out an *E-mail system model* with reference scenarios [60]. For instance, when a target **sends an email**, the IRI should include an *"E-mail send event"* with details such as the sender address, recipient addresses, subject (if allowed by warrant), date/time, and any delivery status [61]. The corresponding CC is the full email content (body and attachments) as it was sent [61]. Similarly, an **E-mail receive event** is generated when a target's mailbox receives a new message (if the target is under intercept, the system would produce IRI listing sender, subject, timestamp, etc., and CC being the message content). Another scenario is **E-mail access/download** – when a target downloads email from a server (e.g. via POP3/IMAP), an intercept can capture that action as an event and provide the downloaded message content [61]. TS 102 232-2 defines specific IRI record types for these: e.g., *email sent IRI*, *email received IRI*, *email download IRI*, each with fields capturing relevant metadata. The document ensures that **both successes and failures** are reported – e.g., if an email send fails (SMTP bounce), that can be an event.

- **Unified Messaging:** The spec also addresses *unified messaging (UM)* services – systems where voicemail, fax, SMS, etc. are integrated into one mailbox. Unified messaging events might include a **message deposit** (e.g. someone leaves a voicemail in the target's mailbox) or a **message retrieval** (target listens to a voicemail or views a fax from their inbox) [62] [63]. TS 102 232-2 indicates that such events, when they occur after intercept activation, should trigger appropriate IRI and CC delivery. For example, if a target under intercept receives a voicemail in a UM system, the intercept would generate a "Messaging-Event deposit" IRI and deliver the voicemail audio as CC [63]. Likewise, when the target retrieves that message, a "Messaging-Event retrieve" IRI is sent [63]. The standard had to define how to hand over content like voicemail or fax – typically as file attachments or in a real-time stream depending on the system. (Change logs in the spec show numerous improvements over time to handle new UM features, like streaming multimedia attachments, new party identities, etc. [64] [65]).

- **Instant Messaging and Chat:** Initially, Part 2 was focused on "store-and-forward" messaging (email, voicemail, SMS to some extent). However, as OTT instant messaging and chat applications became prevalent, the standard was updated. **Version 3.12.1 (2020)** of TS 102 232-2 explicitly **extended coverage to Instant Messaging and chat apps** [66]. This means the standard now provides guidance on intercepting services like messaging apps that use TCP/HTTP (or other IP protocols) to exchange messages in near-real-time. The extension likely includes defining IRI events such as *chat message sent/received*, *group chat events*, etc., analogously to email. Since these are delivered over the same IP/TCP ASN.1 mechanism, the messages from such apps can be treated similarly to email in terms of handover format. The update was significant because many such services are provided by OTT (over-the-top) providers rather than traditional telecom operators. ETSI also introduced a new handover specification (TS 103 707) using HTTP/XML specifically for messaging services as an alternative to the TCP/ASN.1 approach [29], but within TS 102 232-2 the classic ASN.1 format is used to carry IM/chat content as well. In summary, by 2020 Part 2 ensures that not just emails, but also modern messaging (text chat, possibly multimedia messages in apps) can be lawfully intercepted.

- **SMS/MMS:** Interestingly, SMS (Short Message Service) and MMS (Multimedia Messaging Service) in cellular networks are also messaging services. However, interception of SMS/MMS in practice has often been specified in the **mobile services** context (since SMS is delivered via mobile signaling). In 3GPP TS 33.108, SMS interception is certainly covered: when a target sends or receives an SMS, the IRI includes the sender and recipient numbers and time, and the CC is the text content [67] [68]. MMS (which involves an IP-based store-and-forward of media via an MMS server) requires capturing the MMS notification (usually via SMS) and the retrieval of content via WAP/HTTP. ETSI's documentation references OMA MMS standards [69], implying MMS intercept may have been detailed under mobile or messaging parts. If not explicitly in Part 2, the concept would be: intercept MMS similar to email (with events for *MMS submitted*, *MMS delivered*, and CC being the multimedia content). For completeness, we can say that **telecom-originated messaging like SMS/MMS** is typically addressed in Part 7 (mobile) because it ties into mobile network signaling; whereas **internet messaging (email, OTT chat)** is in Part 2.

- **Metadata specifics:** The IRI fields for messaging often include things like **message IDs**, **addresses (email addresses or MSISDNs)**, **subject lines or message types**, **attachment indicators**, **delivery status**, etc. [7] [63]. Part 2 defines these so that LEAs get comprehensive information. For example, an email IRI might have a field for "email subject" (if allowed by the interception scope) and "attachment names", while a chat message IRI might indicate group IDs or chat room names. The **content** is typically delivered in its original format (e.g., the email's RFC822 text, or the binary image of an attachment, or the text of an IM message).

To illustrate, consider a target under intercept who uses a webmail service: When they compose and send an email, the intercept system (perhaps at the SMTP relay or webmail server) generates an IRI record "Email Send Success" with the addresses and time [61], and copies the outgoing email content to CC (which is then forwarded over HI3). If the target later logs in and downloads new emails, for each downloaded message an IRI "Email Download" event is sent and the email content is delivered (if not already delivered earlier) [61]. If the target is using a chat app, each message they send could be treated like a mini-email for intercept: an IRI for message send with participants' IDs and a CC with the message text.

In summary, Part 2 ensures that **electronic messaging services of all kinds** can be intercepted in a consistent manner. Its evolution to include instant messaging reflects the need to keep pace with technology. By using Part 2 in conjunction with Part 1, a provider can deliver, say, both an email and an IM conversation over the same handover system to law enforcement.

## 4.3 Internet Access Services (Part 3)

**ETSI TS 102 232-3 (Service-specific details for Internet Access Services)** addresses the lawful interception of a target's Internet access usage. This typically applies to ISP scenarios – e.g., a person's home broadband, a dial-up account, or a wireless data service – where the goal is to capture **when and how the target accesses the Internet, and potentially what data flows occur**. Important aspects include:

- **Access session events:** Internet Access Service (IAS) interception is heavily about tracking the lifecycle of the target's online sessions. The spec defines IRI events for **logon**, **logoff**, **multi-login**, and other session state changes [9] [14]. For example, when a target establishes an internet connection (such as PPPoE dial-up, or obtaining an IP on a DSL/cable modem, or attaching to a cellular PDN), an IRI "Logon" event is generated with details like the time, the network access server

(NAS) used, the IP address assigned to the target, and any authenticator info (username, etc.) [2] [3]. Correspondingly, when the session ends or the user disconnects, an IRI "Logoff" is sent. The standard also considers **multiple simultaneous logins** (if a service allows the same user to connect from two locations) – it provides that each session would be identified and reported separately [70] [71]. If a connection is lost unexpectedly, an "unexpected connection loss" IRI event can be sent by the network [72] [73].

- **IP address and target identity:** In IAS interception, a crucial piece of information is linking the target's subscriber identity to the **IP address** they are using, since much of the internet activity will be identified by IP. Part 3 has provisions for capturing the **IP assignment** event: when the target is allocated an IPv4 or IPv6 address (or prefix), the intercept device should send an IRI record noting that address and the time bound to the target [2] [3]. It may use fields like "Target ID additional identifiers" to convey IP along with username etc. Also, any change in IP (e.g., new DHCP lease) mid-session is reported. This ensures LEAs know *where* to attribute any captured traffic. The spec explicitly lists "Target identity and IP address" as a topic, meaning the intercept configuration must accommodate intercept by various identifiers including IP [74]. Sometimes a warrant may directly specify an IP (if, say, the target is known to use a static IP) – the LI system must handle that as well.

- **Intercepted communications (CC) for internet traffic:** For Internet access, the "content of communication" could be literally *all IP packets* sent/received by the target. However, capturing and delivering an entire internet feed can be extremely data-heavy. The standards provide options and guidance. They introduce the concept of **Packet Header Information** and **Packet Data Summary**:

- **Packet Data Header Reporting (PDHR):** This refers to intercepting not full packets, but just headers of packets (or selected portions) for the target's flows [74] [71]. By reporting packet headers as IRI, LEAs get metadata like source/dest IPs, ports, protocols, without all the payload. This is useful if content interception is not authorized or to reduce volume. TS 102 232-3 defines information elements for IPv4/IPv6 header fields, TCP/UDP info, etc., as part of IRI [74].
- **Packet Data Summary Report (PDSR):** In newer versions (v3.9.1, 2020), a *PDSR* feature was added [75]. A PDSR is essentially an aggregate report of a target's data session, possibly including totals like bytes transmitted, duration, etc. Instead of overwhelming LEA with every packet, the LI system might send periodic summaries. The 2020 update indicates PDSR was introduced to meet new requirements – likely for summarizing high-volume data intercepts in 5G or broadband contexts [75].

- **Full content:** If full content capture is warranted (e.g., in a targeted collection for specific traffic), HI3 for IAS can carry entire IP packets (from layer 3 upward). TS 102 232-3 discusses filtering: you might filter to only intercept certain protocols or target certain communication (for example, intercept only VOIP packets on certain ports). If no filter is applied, all of the target's internet traffic is delivered as CC, which the LEA would then need to handle (often by reassembling flows, etc.). Given the data volumes, part 3 emphasizes efficient handover – e.g., using compression where appropriate, and possibly multiple parallel streams for content. *Security note:* content may be encrypted at the application layer (e.g. HTTPS) which LI cannot break unless additional lawful measures (like getting keys) are in play; the standards usually acknowledge that the provider delivers what it can see.

- **Scenarios covered:** TS 102 232-3 enumerates common internet access scenarios: **dial-up modem access**, **xDSL access**, **cable modem access**, **WLAN access (hotspots)**, etc., each with slightly different network topology [76] [71]. In each case, the standard explains where interception can occur.

For dial-up, the NAS (Network Access Server) is the IAP; for DSL, it could be at the Broadband Remote Access Server (BRAS) or via sniffing RADIUS AAA messages; for cable, at the CMTS or provisioning system; for Wi-Fi hotspot, at the access controller, etc. An informative Annex in part 3 shows reference topologies and how events are derived. For example, in dial-up, when the user's modem connects and authentication succeeds, the AAA (RADIUS) server can trigger an intercept event with the assigned IP [77] [78]. Part 3 cross-references part 4's annex on RADIUS interception for more detail on capturing those events [77].

- **Preventing over-collection in shared IP environments:** A challenge in IP intercept is that IP addresses can be dynamic and shared (especially IPv4 with NAT or in carrier-grade NAT scenarios). The standards take care that intercept is tied to the **target's session context**. For instance, if an IP address that was used by the target gets reassigned to another user, the LI system should detect that and stop intercepting that IP unless the target logs in again [16] [79]. This avoids capturing another user's traffic. TS 102 232-3 explicitly warns about such scenarios and says to report and halt intercept to avoid "serious over collection" [16] [79]. Likewise, if a target has multiple devices and only one is under intercept, care must be taken not to intercept the other device if it uses a different IP (unless authorized).

In summary, for Internet access, the intercept is focused on **session-level monitoring (who, when, where they access)** and optionally **traffic monitoring (what they do online)**. A simplified example: A target connects to their ISP via DSL. The LI system generates an IRI: *Target X logged in from DSL line Y at 10:00, assigned IP 1.2.3.4*. Then as the target browses, it might either (a) send all packets to LEA, or (b) send IRI records summarizing flows (e.g., *target connected to www.example.com at 10:05, downloaded 500KB*), depending on warrant. When the target disconnects at 11:00, an IRI *Logoff* event is sent with session duration and bytes used. Additionally, part 3 allows generating periodic **heartbeat IRI** if needed to indicate the session is still ongoing (perhaps using IRI-CONTINUE records).

The **2020 update (v3.9.1)** to part 3, as noted in an ETSI status report, extended it with PDSR and other features to accommodate new **5G requirements** and high data volumes [75]. 5G's equivalent (retained in 3GPP TS 33.127/128) but ETSI ensured the IAS handover can carry things like 5G subscriber IDs (SUPI) and new access types. Overall, TS 102 232-3 ensures an ISP or mobile data provider can faithfully provide law enforcement with a target's internet usage information in a standardized way.

## 4.4 Layer 2 Access Services (Part 4)

**ETSI TS 102 232-4 (Service-specific details for Layer 2 services)** deals with interception in scenarios where the service provided is a layer 2 connection (rather than a layer 3 IP service). Examples include **xDSL access, cable modem networks, and layer2 VPNs** where the user's traffic might be tunneled or bridged through the provider's network to the internet. Part 4 is somewhat related to part 3 (internet access), but it focuses on cases where interception must occur at layer 2 (e.g., PPP, ATM, Ethernet frames) rather than IP, or where one provider handles the access network and another handles the internet service.

Key considerations in Part 4:

- **Access network vs service provider split:** In many broadband deployments, the access network (Layer2 domain) may be operated by one entity (e.g., a local telco wholesaling DSL lines), and the internet service (Layer3 ISP) by another. In such cases, interception might need cooperation between the access provider and service provider. TS 102 232-4 describes scenarios like:

- **Scenario 1:** Single party provides both access and internet service – interception is straightforward at their BRAS/NAS.
- **Scenario 2:** Access network provider is separate, using a RADIUS proxy to tunnel sessions to various ISPs [80] [78]. Interception might occur at the access provider (to catch the PPP session establishment) and/or at the ISP.
- **Scenario 3 & 4:** Variations with multiple tunnels or roaming between access networks.

In any case, part 4 highlights the role of **RADIUS (AAA) messages** in layer 2 interception. When a user initiates a PPPoE or similar connection, the NAS communicates with a RADIUS server for authentication and IP assignment. To intercept layer2 events, the LI function can hook into the RADIUS exchange: - On **Access-Request/Accept**, glean the username and assigned IP (if any). - On **Accounting Start/Stop**, get session start/stop times, byte counts. Annex B of TS 102 232-4 provides details on RADIUS in the LI context [77] [78], and references that TS 102 232-3's Annex A covers general RADIUS interception methods [77].

- **Intercept events:** Similar to part 3, the events include **Layer2 session start**, **Layer2 session stop**, and **unexpected drop**. The difference is they may not have IP info if IP isn't yet assigned at start. For example, in pure layer2 (like an ATM VC or an Ethernet MAC address authentication), the target might be identified by a circuit ID, DSL line ID, or MAC address at first. The intercept IRI would record that along with timestamp and any initial credentials [2] [3]. Once an IP is assigned (which might be by the ISP after authentication), that IP becomes part of the intercept info. Part 4 addresses the need to **link the layer2 identity with layer3 identity** when the latter becomes known. This could be via a message from the ISP's RADIUS server back to the access provider's intercept system, as noted in Annex B: *the RADIUS proxy or server can be extended to forward IP assignment info to the intercept function* [81] [82].

- **Content interception:** In layer2 services, content might be at the layer2 frame level. For example, intercepting a DSL line might mean capturing all PPP frames or all ATM cells for that user's circuit. However, usually the goal is still to get to the IP content. Part 4 likely suggests that if the intercept is executed at layer2, the content can be reassembled into higher-layer PDUs for delivery. If not, the frames could be delivered as a bitstream. Historically, lawful interception on pure layer2 (like ATM networks) was handled by delivering reassembled content streams (e.g. reassembling ATM cells into IP packets or voice circuits). Given TS 102 232-4's age (v2.2.1 from 2010) [83], it was written when ATM/FR and early Ethernet wholesale models were prevalent. It ensures that even if a target's communication is just a bridged layer2 tunnel, it can be intercepted.

- **Example xDSL scenario:** A user dials into a DSLAM, their modem establishes a PPPoE session. The DSL line is identified by a circuit ID. The NAS (Network Access Server) receives a login and forwards to a RADIUS server (possibly via a RADIUS proxy if the ISP is different) [80] [78]. When interception is active, the NAS or a mediation device will generate an IRI: *Target username "foo" started PPPoE on DSLAM X, port Y at time T.* The RADIUS Accept includes an IP, say 10.1.2.3, which is then included in a follow-up IRI (or in the same one) stating *IP 10.1.2.3 assigned to target* [82] [84]. All user traffic (PPP frames) could then be copied and forwarded as CC. If the DSL provider is separate, their intercept function might forward relevant info to the ISP's intercept function. The spec probably outlines that coordination.

Overall, Part 4 is a niche but important extension to handle **cases where intercepting at IP layer is not enough or not possible**, and one must intercept the lower-layer service. With the convergence to all-IP networks, Part 4 hasn't needed frequent updates (v2.2.1 is from 2010), but it still applies to scenarios like enterprise Layer2 VPNs or certain cable architectures. It essentially says: treat the layer2 session similar to an IP session for intercept, capturing login/logoff, and ensure the data content can be handed over (possibly after converting it to IP or including instructions on how to interpret it).

## 4.5 Mobile Telephony and Data Services (Part 7)

**ETSI TS 102 232-7 (Service-specific details for Mobile Services)** provides the details for interception in **2G/3G/4G mobile networks** (and is evolving to accommodate 5G by referencing newer specs). Mobile services include circuit-switched telephony (GSM calls, UMTS CS calls), packet-switched data (GPRS, EPS/LTE data sessions), SMS, MMS, and newer IMS services (VoLTE, WiFi calling), as well as niche services like push-to-talk. Rather than duplicating 3GPP specs, Part 7 references them heavily and gives the mapping to the ETSI handover format.

Key points in Part 7:

- **Voice call interception (Circuit-Switched):** When a target makes or receives a traditional voice call on 2G/3G, the network generates standard events:
- **Call attempt/establishment:** IRI records when the call is dialed (with numbers, IMSI, cell location if available, etc.) – essentially the **CALL BEGIN** IRI. If the call is successfully connected, that might be marked in IRI (or at least the time of answer). If not, cause codes can be reported.
- **Call termination:** An IRI **CALL END** is recorded when either party hangs up, including duration and release cause.
- **Supplementary events:** Any mid-call events (like call hold, conference join, etc.) would be reported via IRI-CONTINUE records if applicable.

The CC for a circuit call is the live **audio stream**. In modern systems, even a circuit-switched call's audio can be packetized for delivery. TS 102 232-7 V3.7.1 (2019) explicitly mentions an *IP-based handover for CS voice calls* – meaning even traditional calls are delivered over the HI3 IP/TCP connection using an ASN.1 format defined for voice content [40]. (Annex B.17 in 3GPP 33.108 defines an ASN.1 for CS voice content over IP [85].) Thus, LEAs receive phone call audio usually as a stream of RTP or an A-law encoded data within the LI container.

There is also mention of location: 3GPP LI can include cell location info as part of IRI for calls or periodically if warranted (via IRI-REPORT). TS 102 232-7 likely includes parameters for Cell-ID, etc., in the IRI messages for mobile.

- **SMS interception:** SMS messages are short signaling-plane transactions in mobile networks. For an intercepted target:
- When the target sends an SMS (Mobile Originating, MO), the SMS Service Center (or MSC) will trigger an IRI event containing the sender MSISDN, recipient MSISDN, timestamp, and delivery status (e.g. "sent for delivery") [86] [67]. The CC is the **text content** of the SMS (up to 160 characters, or more if concatenated) delivered usually as part of an IRI or as a small file. Some implementations treat SMS content as "IRI extended data" since it's textual and small.

- When the target receives an SMS (MT), an IRI is generated with sender number, etc., and CC is the message text. If the SMS cannot be delivered (phone off, etc.), that can be reported too.

In CDMA networks, similar standards (like ANSI J-STD-025) apply – TS 102 232-7 v3.8.1 added references to ANSI J-STD-025-B for intercepting CDMA2000 voice and SMS [87], ensuring that Part 7 covers not just GSM/UMTS/LTE but also CDMA systems.

- **MMS interception:** An MMS (picture or multimedia message) typically involves two parts: an SMS notification to the device and an IP retrieval of content from the MMSC. For intercept:
- The SMS notification can be treated like an SMS (contains the sender and an URL or ID for the content).

- When the target retrieves the MMS content (via HTTP/WAP), that transaction's details and content should be intercepted. If the target is the sender of an MMS, the process is reversed: they upload content to MMSC (an IP transaction) and an SMS is sent to notify the recipient. Part 7 works in conjunction with Part 3 (since MMS retrieval is an IP session) to capture both the signaling (as IRI, possibly referencing the MMS-ID) and the content (the actual media file) [88] [89]. 3GPP references OMA MMS specs for how to parse the content. The end result is LEA gets the *MMS message content (images, etc.)* similar to how an email would be handed over.

- **Packet-Switched Data (GPRS/EPS):** For 2.5G/3G packet data (GPRS) and 4G LTE data, interception aligns with the Internet Access Service model (Part 3), but with mobile-specific context. The 3GPP LI architecture defines that:

- **Attach/Detach:** When a mobile data user (target) attaches to the packet network (e.g. GPRS attach or PDN connection in LTE), an IRI event is created with the IMSI, assigned IP address, APN (access point name), and possibly QoS info [49] [50]. Similarly, when they detach or the PDP context is deactivated, an IRI is sent. These are analogous to logon/logoff in Part 3.
- **Location updates (Tracking Area Updates, etc.):** These can also generate IRI if relevant (especially if location tracking is part of warrant).

- **Data content:** GPRS/LTE user plane interception means copying all or selected IP packets from the target's device. In LTE, the intercept can be done at the PDN Gateway (P-GW) or Serving Gateway depending on architecture. TS 102 232-7 v3.8.1 notes covering "data handover defined by 3GPP TS 33.108 for EPS" [87]. This implies Part 7 includes specifics on how to format mobile data intercept in ASN.1. Likely, it references 3GPP-defined IRI for PDP context events and uses the same PDHR/PDSR concepts as Part 3 for the actual IP flows. One nuance: In roaming scenarios, either home or visited network might intercept (e.g., for LTE with S8 home routing, only the home sees the traffic; with local breakout, visited network sees it). Part 7 covers both by referencing appropriate 3GPP procedures.

- **IMS-based services (VoIP, VoLTE, Wi-Fi Calling):** As mobile networks have moved toward IP multimedia (IMS), intercept had to include those. Part 7 (especially in newer versions) includes sections for:

- **IMS Voice (VoLTE) and Video calls:** These are SIP-based sessions. IRI events here include SIP REGISTER (when the target's phone registers), SIP INVITE (call attempt), call answer, BYE (call end), etc. The content (voice/video) is typically on RTP streams which are intercepted at the media gateway or eNodeB. 3GPP decided that for VoLTE roaming, if using S8HR (home routing), the home network can intercept signaling at P-CSCF and media at SGW, whereas if using LBO (local breakout), the visited network intercepts both [49] [90]. ETSI Part 7 v3.7.1/3.8.1 captures these by referencing 3GPP intercept records for IMS. It defines or points to formats for *IMS IRI* (which can include headers of SIP messages as IRI content) and *IMS CC* (the RTP streams or media content).

- **IMS Conferencing:** When multiple parties are in a conference call (or an IMS multimedia conference), intercept should provide IRI that indicate participants, join/leave events, etc. Part 7 enumerates "IMS Conference Services IRI and CC" with identifiers for each conference leg [91] [92].

- **IMS messaging (SMS over IMS, Chat):** IMS can also carry SMS (via IMS Messaging) or RCS chat. These would be treated similarly to Part 2 messaging, but Part 7 might mention them if they traverse the mobile network. For instance, SMS in LTE is often delivered via IMS (SGs interface or IP-SM-GW) – intercept must capture those as well, likely mapping them to the SMS paradigm.

- **Proximity Services (ProSe) and Mission Critical Communications:** Release 12/13 introduced ProSe (D2D communication directly between devices, used in public safety) and mission-critical push-to-talk (MCPTT) and group communication features. These are complex because they involve direct UE-to-UE links or group servers. Part 7 v3.7.1+ includes clauses for **ProSe intercept** and **Group Communication System Enablers (GCSE) intercept** [93] [94]. Essentially:

- For **ProSe direct communication**, since it bypasses network for content, the network can only intercept related signaling (like ProSe service authorization, discovery messages) unless one device relays. The standard likely says that intercept of ProSe is limited and maybe treated like an IRI-REPORT of an event (e.g., two devices established direct comm at time X) [93] [95].

- For **Group communications (e.g., MCPTT)**, there are servers that manage group calls. Intercept needs to capture when a target initiates a group call (IRI for call begin with group ID), when they speak, etc., and content (audio) needs to be captured from the group call server or the network broadcast. Part 7 provides formats for those intercept records (like *Group Call Request*, *Group Call End* records with fields for group IDs) [94] [96].

- **Legacy vs 5G:** Part 7 historically covered up to LTE. With 5G, 3GPP created new specs (TS 33.127 for architecture, TS 33.128 for protocols). ETSI responded by updating Part 7 to reference those for 5G. For example, TS 102 232-7 v3.8.1 (2020) states it covers data handover for UMTS/GPRS/EPS per 33.108, and for 5G according to 33.128 [97]. This means Part 7 now acts as a bridge until a dedicated 5G part is made. Likely, it says: for 5G NSA/SA, the intercept will have similar IRI (registration, PDU session establishment, etc.) and content (user plane intercept in 5G's UPF), and it might reuse the same HI format with new parameters (like 5G GUTI, SUPI as identifiers). Indeed, TS 102 232-1 v3.22.1 added support for 5G identifiers to HI2/HI3 headers [59].

In essence, Part 7 is very broad, covering *circuit voice, SMS, packet data, IMS services, and emerging mobile services*. It relies on 3GPP stage 2 & 3 specs for the details of what to intercept, but ensures that when handed over via the ETSI HI interfaces, everything is accounted for. Service providers implementing LI in mobile networks use Part 7 as a guide to configure their network elements and mediation devices accordingly. For example, a mobile operator's LI system when intercepting a target will configure: - MSC for CS calls & SMS (mapping to TS 102 232-7 IRI/CC). - SGSN/SGW for data sessions (mapping to TS 102 232-3 and -7). - IMS servers (P-CSCF, etc.) for VoLTE (mapping to -7 IMS intercept). - Application servers for MCPTT if needed. And all that disparate info is consolidated and delivered in a unified way to LEA. Without Part 7, one would have to juggle multiple 3GPP specs – Part 7 simplifies by offering a single point of reference aligning those with ETSI handover.

## 5. Notable Changes Between Document Versions

Many of these standards have evolved over time to accommodate new technologies and law enforcement needs. We highlight some **major changes between versions**:

- **3GPP TS 33.108 (LI Handover for GSM/UMTS/LTE):** Comparing **Version 12.8.0 (Rel-12)** and **Version 15.3.0 (Rel-15)**, we see significant expansions in scope. Release 12 of 3GPP (v12.x) covered interception for GSM, UMTS, LTE and basic IMS. By Release 15 (v15.x), new services and architectures had emerged. For example, intercept support for **IMS-based VoIP (VoLTE)** and **Wi-Fi calling** was refined in Rel-13/14, including handling of roaming scenarios (S8 Home Routing vs Local Breakout) [51] [90]. **Proximity Services (Device-to-Device)** intercept was introduced around Rel-13, reflected in added provisions for ProSe in later versions [93] [95]. **Group communications (MCPTT for public safety)** came in Rel-13/14, leading to new intercept record types for group call events as seen by Rel-15 content [94] [96]. Another big change: **5G preparation**. Release 15 was the first phase of 5G, and 3GPP chose to specify 5G LI in separate docs (TS 33.126/127/128). TS 33.108 v15.3.0 likely added references ensuring interoperability with 5G. Indeed, ETSI later reported that TS 102 232-7 v3.8.1 was updated to cover 3GPP TS 33.128 for 5G intercept [97], meaning by that time 33.108 itself might have stopped short of 5G or provided transitional support. In summary, between v12.8 and v15.3, 3GPP LI capabilities grew to handle **new network elements (e.g. LTE SGW/PGW, IMS gateways)** and **new service types (IMS conferencing, VoLTE roaming scenarios, etc.)**, and set the stage for 5G.

- **ETSI TS 102 232-2 (Messaging services):** Over its lifetime, Part 2 saw updates to keep pace with messaging trends. A notable change was in **v3.12.1 (Aug 2020)** which *"was extended to cover also Instant Messenger and Chat applications"* over the existing TCP/ASN.1 delivery format [66]. Earlier versions focused on email/unified messaging; this update acknowledged that many targets use OTT chat apps, so lawful intercept standards must accommodate those. The extension likely introduced new IRI event types and content formats for chat messages, and possibly addressed encryption issues (though if messages are end-to-end encrypted, the provider may not access content; still, metadata can be provided). This change was driven by law enforcement demand to intercept popular messaging services beyond SMS. Additionally, earlier changes (circa 2012) improved unified messaging handover for new features (as seen by various CRs listed in Part 2's history) [64] [98]. The general trajectory: Part 2 started with classic email/voicemail, then evolved to handle rich messaging (email, SMS, MMS, IM) in one framework.

- **ETSI TS 102 232-3 (Internet access):** One major recent addition was the **Packet Data Summary Report (PDSR)** introduced by v3.9.1 (Nov 2020) [75]. This was likely in response to 5G's enhanced data volumes and LEA requirement to have summary statistics. The PDSR provides a concise report of a data session, complementing per-packet or per-flow reports. The 2020 update also ensured Part 3 could handle **IPv6 and new access types fully** (though IPv6 was already included earlier). Over time, Part 3 also refined the list of IRI attributes – for instance, including **"Use of location field"** for when location info should be provided (such as WiFi hotspot location) [74]. Another subtle update: earlier versions had a fixed notion of target identity; newer ones allow multiple identifiers (e.g. additional IPs or usernames associated with target) [2] [3], reflecting realities of multi-homing and dual-stack IPs. In essence, Part 3’s changes were about **expanding intercept data types and optimizing delivery** for high-speed broadband and 5G.

- **ETSI TS 102 232-4 (Layer 2):** This part has remained at v2.2.1 (2010) for a long time, but there was mention of a v3.3.1 (2017) in some references. If an update occurred, it might have been to align terminology or include newer layer2 tech (like intercepting Carrier Ethernet services). However, the core scenarios (xDSL, cable) haven’t drastically changed. The stable nature of Part 4 indicates that layer2 interception methods reached maturity earlier, and subsequent innovations (like most traffic moving to IP) reduced the need for frequent changes. The main conceptual changes here historically were in the early 2010s, making sure intercept could handle wholesale arrangements (RADIUS proxy setups) – once set, those principles still apply today.

- **ETSI TS 102 232-7 (Mobile):** Being tied to 3GPP, Part 7 saw continuous updates to incorporate new releases:

- **v3.7.1 (Dec 2019)** – included intercept for LTE features and IMS (as IMS-based VoIP, ProSe, GCSE are mentioned in contents) [99] [93] . It likely aligned with 3GPP Rel-14/15.
- **v3.8.1 (2020)** – as per ETSI update, extended to cover EPS and also referenced 5G handover (33.128) for the first time [97] . This means the spec now acknowledged 5G NSA/SA intercepts, ensuring things like 5G SUPI (Subscriber Permanent ID), gNodeB, and new interfaces (like N3, Xn) are accounted for in the LI model. However, details for 5G are primarily in 33.128; Part 7 might just direct implementers to use those in conjunction with Part 1 handover.

- In general, each new 3GPP release that added services (e.g. Rel-9 IMS SMS, Rel-10 SRVCC, Rel-12 Wi-Fi calling, Rel-14 C-V2X communications) needed corresponding LI support. Part 7’s revisions make sure these are not gaps. For example, intercepting a voice call that moves from LTE to 3G (SRVCC) would involve correlating an ongoing intercept across technology change – later versions of Part 7/33.108 included such scenarios.

- **ETSI TS 103 280 (Dictionary):** The dictionary is updated frequently (it was at v2.4.1 in 2020, v2.7.1 by 2021 [100] ). Changes here are usually to **add new parameter definitions or clarify existing ones**. For instance, as 5G arrived, new identifiers like **SUCI/SUPI (Subscription Concealed Identifier/ Permanent Identifier)** were added. Time stamp formats were refined, as noted (clarification of DateTime in 2020) [20] . These changes ensure all other LI specs remain consistent – e.g., if Part 7 says to include “IMEI” in an IRI, the format of IMEI is defined in TS 103 280, and any change to IMEI format (like the inclusion of the check digit or handling of 15 vs 16 digits) would be updated in TS 103 280 and then used by all.

- **Other general changes:** The ETSI TC LI has also worked on aligning terminology with 3GPP (for example, using “LI System Function” names similarly) and improving security. For instance, internal interfaces X1/X2 were updated to use modern protocols (HTTP/2, TLS1.3) in TS 103 221 as of 2020 [35] . While not directly in our listed docs, these affect how implementations work under the hood.

In conclusion, the LI standards are living documents. They are periodically revised to **address new communications services (e.g., OTT messaging, 5G network slicing), new technical challenges (encryption, massive data volumes), and new regulatory requirements**. The changes between versions we’ve highlighted reflect an ongoing effort to keep lawful interception effective in an era of rapid telecom evolution, while maintaining the standardized approach that ETSI and 3GPP have established.

## Conclusion

Lawful interception is a complex technical capability that must be built into diverse communication systems – fixed, mobile, IP-based, legacy and futuristic – in a way that meets law enforcement needs without compromising network integrity or user privacy beyond authorized scope. The ETSI TS 102 232 series (Parts 1, 2, 3, 4, 7) and related specs like TS 103 280 and 3GPP TS 33.108 provide a comprehensive blueprint for achieving this. They define **clear technical requirements** (ensuring correctness, reliability, security, and minimal service impact), a modular **architecture** (with functions like ADMF, IRI/CC delivery functions, IAPs, and standardized interfaces), well-specified **HI1/HI2/HI3 procedures** (so that issuing a warrant and delivering intercept data can be done uniformly across operators), and detailed **service-specific intercept instructions** (covering everything from a phone call or text message to an email or a 4G internet session).

By adhering to these standards, law enforcement agencies are able to receive intercept information in a consistent format regardless of the provider or technology, facilitating efficient investigation. Meanwhile, service providers have guidelines to implement interception capabilities that fulfill legal obligations while protecting networks and non-target users from any negative effects. The documents also illustrate an evolutionary path: as telecommunication technologies evolve (IMS, LTE, 5G, OTT apps), the LI framework expands to encompass them – evident in the changes incorporated in newer versions [66] [97] .

Ultimately, the ETSI LI specifications aim to strike a balance between the needs of society (lawful access to communications of suspects) and the rights of individuals (ensuring only authorized intercepts occur, with strict controls). The comprehensive nature of TS 103 280’s parameter dictionary and the common delivery format in TS 102 232-1 ensure that all intercept data – whether it’s a traditional phone call or a chat message – can be understood and correlated by the monitoring agency [19] [33] . This structured approach, with its clear separation of administrative and content interfaces, is a model that has been adopted in many jurisdictions worldwide.

**Sources:**

- ETSI TS 102 232-1 V3.17.1 – Handover Interface for IP Delivery (2018) [33] [11]
- ETSI TS 102 232-2 V3.12.1 – Messaging Services SSD (2020) [61] [66]
- ETSI TS 102 232-3 V3.9.1 – Internet Access SSD (2020) [2] [38]
- ETSI TS 102 232-4 V2.2.1 – Layer 2 Services SSD (2010) [77] [78]
- ETSI TS 102 232-7 V3.7.1 – Mobile Services SSD (2019) [26] [97]
- ETSI TS 103 280 V2.7.1 – LI Common Parameters Dictionary (2021) [18] [19]
- 3GPP TS 33.108 V17.0.0 (2022) – 3G Security; LI Handover Interface (Rel-17) [41] [51]
- Domenico R. Cione, *ETSI LI & RD Status (Dec. 2020) – Sicurezza e Giustizia* journal [66] [97] .

[1] [4] [5] [21] [22] [23] [24] [25] [26] [27] [30] [31] [32] [40] [41] [49] [50] [51] [52] [67] [68] [69] [85] [86] [88] [89] [90] [91] [92] [93] [94] [95] [96] TS 133 108 - V17.0.0 - Universal Mobile Telecommunications System (UMTS); LTE; Digital cellular telecommunications system (Phase 2+) (GSM); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 version 17.0.0 Release 17)
https://www.etsi.org/deliver/etsi_ts/133100_133199/133108/17.00.00_60/ts_133108v170000p.pdf

[2] [3] [6] [7] [8] [9] [14] [15] [16] [17] [37] [38] [39] [70] [71] [74] [76] [79] TS 102 232-3 - V3.9.1 - Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services
https://www.etsi.org/deliver/etsi_ts/102200_102299/10223203/03.09.01_60/ts_10223203v030901p.pdf

[10] [11] [12] [13] [33] [34] [36] [42] [43] [44] [45] [46] [47] [48] [53] [54] [55] [56] [57] [58] TS 102 232-1 - V3.17.1 - Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery
https://www.etsi.org/deliver/etsi_ts/102200_102299/10223201/03.17.01_60/ts_10223201v031701p.pdf

[18] [PDF] Nr. Standard reference Title 1 ETSI EN 319 102-1 V1.3.1 (2021-11)
https://standard.md/wp-content/uploads/2021/12/ETSI-noiembrie-2021.pdf

[19] [PDF] II
https://standard.md/wp-content/uploads/2022/03/Proiect-PSN-2022-Final-01.03.pdf

[20] [28] [29] [35] [59] [66] [75] [87] [97] ETSI LI & RD Status (Dec. 2020) - Sicurezza e Giustizia
https://www.sicurezzaegiustizia.com/etsi-li-rd-status-dec-2020/

[60] [61] [62] [63] [64] [65] [98] TS 102 232-2 - V3.12.1 - Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services
https://www.etsi.org/deliver/etsi_ts/102200_102299/10223202/03.12.01_60/ts_10223202v031201p.pdf

[72] [73] [77] [78] [80] [81] [82] [83] [84] TS 102 232-4 - V2.2.1 - Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services
https://www.etsi.org/deliver/etsi_ts/102200_102299/10223204/02.02.01_60/ts_10223204v020201p.pdf

[99] TS 102 232-7 - V3.7.1 - Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services
https://www.etsi.org/deliver/etsi_ts/102200_102299/10223207/03.07.01_60/ts_10223207v030701p.pdf

[100] TS 103 280 - V2.7.1 - Lawful Interception (LI); Dictionary for common parameters
https://www.etsi.org/deliver/etsi_ts/103200_103299/103280/02.07.01_60/ts_103280v020701p.pdf