ETSI TS 102 232-1 V3.37.1 (2026-05)

TECHNICAL SPECIFICATION

Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery

Reference
RTS/LI-00316-1

Keywords
handover, IP, lawful interception, security

ETSI

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

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

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

Contents

Intellectual Property Rights 6
Foreword 6
Modal verbs terminology 6
Introduction 7
1 Scope 8
2 References 8
2.1 Normative references 8
2.2 Informative references 10
3 Definition of terms, symbols and abbreviations 11
3.1 Terms 11
3.2 Symbols 13
3.3 Abbreviations 14
4 General 15
4.1 Functionality 15
4.2 Intercepted data types 16
4.2.1 Introduction 16
4.2.2 Interception at network operator or access provider 16
4.2.3 Interception at service providers 16
4.3 Relationship to other standards 16
4.4 Handover for GPRS/UMTS/EPS and 3GPP CS Domains 18
4.4.1 PS Access 18
4.4.2 Applications 18
4.4.3 3GPP CS domain 18
4.5 Common parameters 18
4.6 Handover for services defined in 3GPP TS 33.128 18
5 Headers 19
5.1 General 19
5.2 Description and purpose of the header fields 19
5.2.1 Version 19
5.2.2 LIID 19
5.2.3 Authorization Country Code 19
5.2.4 Communication IDentifier 19
5.2.5 Sequence number 20
5.2.6 Payload timestamp 21
5.2.7 Payload direction 22
5.2.8 Payload type 22
5.2.9 Interception type 22
5.2.10 IRI type 23
5.2.11 Interception Point IDentifier 23
5.2.12 Session direction 23
5.2.13 Extended Interception Point IDentifier 23
5.2.14 Network Function IDentifier 24
5.3 Encoding of header fields 24
6 Data exchange 24
6.1 Overview 24
6.2 Handover layer 25
6.2.1 General 25
6.2.2 Error reporting 26
6.2.3 Aggregation of payloads 26
6.2.4 Sending a large block of application-level data 27
6.2.5 Padding data 27
6.2.6 Payload encryption 27

6.3 Session layer 27
6.3.1 General 27
6.3.2 Opening and closing connections 28
6.3.3 Buffering 28
6.3.4 Keep-alives 28
6.3.5 Option negotiation 29
6.3.5.1 Introduction 29
6.3.5.2 Option negotiation message exchange 29
6.3.6 PDU acknowledgement 30
6.4 Transport layer 31
6.4.1 Overview 31
6.4.2 TCP settings 31
6.4.3 Acknowledging data 31
6.5 Network layer 32

7 Delivery networks 32
7.1 Types of network 32
7.1.1 General 32
7.1.2 Private networks 32
7.1.3 Public networks with strict control 32
7.1.4 Public networks with loose control 32
7.2 Security requirements 33
7.2.1 General 33
7.2.2 Confidentiality and authentication 33
7.2.3 Integrity 33
7.3 Further delivery requirements 33
7.3.1 Test data 33
7.3.2 Timeliness 33

Annex A (normative): ASN.1 syntax trees 34

A.1 ASN.1 syntax tree for HI2 and HI3 headers 34

A.2 ASN.1 specification 35

A.3 Importing parameters from other standards 35

Annex B (informative): Recommendation 36

Annex C (informative): Notes on TCP tuning 37

C.1 Implement IETF RFC 5681 37

C.2 Minimize roundtrip times 37

C.3 Enable maximum segment size option 37

C.4 Path MTU discovery 37

C.5 Selective acknowledgement 37

C.6 High speed options 37

C.7 PUSH flag 38

C.8 Nagle's algorithm 38

C.9 Buffer size 38

Annex D (informative): IRI-only interception 39

D.1 Overview 39

D.2 Definition HI information 39

D.3 IRI deriving 39

D.4 IRI by post and pre-processing CC information 40

Annex E (informative): Purpose of profiles 41
E.0 Background 41
E.1 Formal definitions 41
E.2 Purpose of profiles 41
Annex F (informative): Traffic management of the handover interface 43
F.0 Rationale 43
F.1 Factors to consider 43
F.1.0 Background 43
F.1.1 Burstiness 43
F.1.2 Mixed content 43
F.1.3 Network facilities for traffic management 44
F.1.4 Evidentiary considerations 44
F.1.5 National considerations 44
F.2 Traffic management strategies 44
F.3 Bandwidth estimation 45
F.4 National considerations 45
F.5 Implementation considerations 46
F.5.1 Volatile versus non-volatile storage 46
F.5.2 Maximum buffering time 46
F.5.3 Transmission order of buffered data 46
F.5.4 Buffer overflow processing 46
Annex G (normative): Implementation of payload encryption 47
Annex H (informative): ETSI TS 102 232 family relationship 48
Annex I (informative): Option negotiation 51
I.0 Summary 51
I.1 Example use cases 51
I.1.1 Option negotiation not supported in LGW 51
I.1.2 Simple negotiation by both endpoints 52
I.1.3 Simple DF-only option request 53
I.1.4 Simple LGW-only option request 54
I.1.5 Complex negotiation 55
Annex J (normative): Implementation of Integrity Checks 56
J.1 Definitions 56
J.2 Process description 56
J.3 Example integrity Chain 57
Annex K (informative): Change history 59
History 65

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

The present document is part 1 of a multi-part deliverable covering the Handover Interface and Service-Specific Details (SSD) for IP delivery, as identified below:

Part 1: "Handover specification for IP delivery";

Part 2: "Service-specific details for messaging services";

Part 3: "Service-specific details for internet access services";

Part 4: "Service-specific details for Layer 2 services";

Part 5: "Service-specific details for IP Multimedia services";

Part 6: "Service-specific details for PSTN/ISDN services";

Part 7: "Service-specific details for Mobile Services".

The ASN.1 module is available as an electronic attachment to the present document (see clause A.2 for more details).

Modal verbs terminology

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

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

Introduction

The objective of the present document is to form the basis for a standardized handover interface for use by both telecommunications service providers and network operators, including Internet Service Providers that will deliver the interception information required by Law Enforcement Authorities under various European treaties and national regulations.

The present document describes how to handover intercepted information via IP-based networks from a CSP to an LEMF. The present document covers the transportation of traffic, but does not specify functionality within CSPs or LEMF (see clause 4.1). The present document handles the transportation of intercepted Content of Communication (CC), Intercept-Related Information (IRI), Transport Related Information (TRI) and HI1 notification information. The tasking and management of Lawful Interception via the HI1 interface is outside the scope of the present document.

The present document is intended to be general enough to be used in a variety of situations: it is not focused on a particular IP-based service. The present document therefore provides information that is not dependent on the type of service being intercepted. In particular the present document describes delivery mechanisms (clause 6), and the structure and header details (clause 5) for both HI2 and HI3 information.

References within the main body of the present document are made if applicable to the 3GPP specification number with in square brackets the reference number as listed in clause 2. In clause 2 "References" the corresponding ETSI specification number is indicated with a reference to the 3GPP specification number. 3GPP specifications are available faster than the equivalent ETSI specifications.

1 Scope

The present document specifies the general aspects of HI2 and HI3 interfaces for handover via IP based networks.

The present document:

- specifies the modular approach used for specifying IP based handover interfaces;
- specifies the header(s) to be added to IRI and CC sent over the HI2 and HI3 interfaces respectively;
- specifies protocols for the transfer of IRI and CC across the handover interfaces;
- specifies protocol profiles for the handover interface.

The present document is designed to be used where appropriate in conjunction with other deliverables that define the service-specific IRI data formats (including ETSI TS 102 227 [i.1], ETSI TS 101 909-20-1 [33], ETSI TS 101 909-20-2 [34], ETSI TS 102 232-2 [5], ETSI TS 102 232-3 [6], ETSI TS 102 232-4 [32], ETSI TS 102 232-5 [37], ETSI TS 102 232-6 [36] and ETSI TS 102 232-7 [38]). Where possible, the present document aligns with 3GPP TS 33.108 [9] and ETSI TS 101 671 [4] and supports the requirements and capabilities defined in ETSI TS 101 331 [i.9] and ETSI TR 101 944 [i.4].

For the handover of intercepted data within GSM/UMTS PS and CS domains, the present document does not override or supersede any specifications or requirements in 3GPP TS 33.108 [9].

For the handover of services defined in 3GPP TS 33.128 [46], in the event of conflict between the present document and 3GPP TS 33.128 [46], the terms of 3GPP TS 33.128 [46] apply.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] Void.

[2] Void.

[3] Void.

[4] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

NOTE: ETSI TS 101 671 is in status "historical" and is not maintained.

[5] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services".

[6] ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".

[7] Void.

[8] Void.

[9] ETSI TS 133 108: "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)".

[10] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions — Part 1: Country code".

[11] Recommendation ITU-T X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[12] Recommendation ITU-T X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[13] Void.

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

[15] Void.

[16] IETF RFC 9293: "Transmission Control Protocol (TCP)".

[17] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".

[18] Void.

[19] Void.

[20] Void.

[21] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

NOTE 1: IETF RFC 5246 obsoletes IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1" and IETF RFC 3268: "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)" which was referenced until ETSI TS 102 232-1 (V2.6.1).

NOTE 2: IETF RFC 4346 obsoletes IETF RFC 2246: "The TLS Protocol Version 1.0".

[22] Void.

[23] IETF RFC 5681: "TCP Congestion Control".

NOTE: IETF RFC 5681 obsoletes IETF RFC 2581: "TCP Congestion Control".

[24] Void.

[25] Void.

[26] Void.

[27] IETF RFC 6298: "Computing TCP's Retransmission Timer".

NOTE: IETF RFC 6298 obsoletes IETF RFC 2988: "Computing TCP's Retransmission Timer".

[28] Void.

[29] Void.

[30] IETF RFC 6818: "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

NOTE: IETF RFC 6818 updates IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[31] Void.

[32] ETSI TS 102 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services".

[33] ETSI TS 101 909-20-1: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services".

[34] ETSI TS 101 909-20-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services".

[35] Void.

[36] ETSI TS 102 232-6: "Lawful interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services".

[37] ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".

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

[39] Void.

[40] FIPS PUB 186-5: "Digital Signature Standard (DSS)".

[41] IETF RFC 7525: "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)".

[42] FIPS PUB 180-4: "Secure Hash Standard (SHS)".

[43] Void.

[44] ETSI TS 103 280: "Lawful Interception (LI); Dictionary for common parameters".

[45] ETSI TS 103 462: "Lawful Interception (LI); Inter LEMF Handover Interface".

[46] ETSI TS 133 128: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Security; Protocol and procedures for Lawful Interception (LI); Stage 3 (3GPP TS 33.128)".

[47] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TS 102 227: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception".

[i.2] Library of Congress document Z39.50.

[i.3] Void.

[i.4] ETSI TR 101 944: "Telecommunications security; Lawful Interception (LI); Issues on IP Interception".

[i.5] ETSI TR 102 503: "Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception and Retained data handling Specifications".

[i.6] Void.

[i.7] IETF RFC 2923: "TCP Problems with Path MTU Discovery".

[i.8] ISO/IEC TR 10000-1: "Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework".

[i.9] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.10] ETSI TS 101 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

[i.11] IETF RFC 792: "Internet Control Message Protocol".

[i.12] IETF RFC 7323: "TCP Extensions for High Performance".

[i.13] IETF RFC 1191: "Path MTU discovery".

[i.14] IETF RFC 2018: "TCP Selective Acknowledgement Options".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 101 158 [i.10], 3GPP TS 33.128 [46], ETSI TS 101 331 [i.9] and the following apply:

Access Provider (AP): provides a user of some network with access from the user's terminal to that network

NOTE: This definition applies specifically for the present document. In a particular case, the access provider and network operator may be a common commercial entity.

(to) buffer: temporary storing of information in case the connection to the LEMF is temporarily unavailable

call: any temporary switched connection capable of transferring information between two or more users of a telecommunications system

NOTE: In this context a user may be a person or a machine.

communication: information transfer according to agreed conventions

Communication IDentifier (CID): See definition in clause 5.2.4.

Communication Identity Number (CIN): See definition in clause 5.2.4.

Communications Service Provider (CSP): organizations (e.g. Service Providers (SvP), Network Operators (NWO) or Access Providers (AP)) who are obliged by law to provide interception

communications session: session that consists of either a single self-contained transaction or a series of protocol data units that together form a single self-contained communication

Content of Communication (CC): information exchanged between two or more users of a telecommunication service, excluding Intercept Related Information

NOTE: This includes information which may, as part of some telecommunication service, be stored by one user for subsequent retrieval by another.

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

identity: technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunication identity number (such as a telephone number) or the logical or virtual telecommunication identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis

information: intelligence or knowledge capable of being represented in forms suitable for communication, storage or processing

NOTE: Information may be represented for example by signs, symbols, pictures or sounds.

interception: action (based on the law), performed by a network operator/access provider/service provider, of making available certain information and providing that information to a Law Enforcement Monitoring Facility

NOTE: In the present document the term interception is not used to describe the action of observing communications by a law enforcement agency.

interception measure: technical measure which facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations

interception subject: person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted

Intercept Related Information (IRI): collection of information or data associated with telecommunication services involving the target identity, specifically communication associated information or data (including unsuccessful communication attempts), service associated information or data (e.g. service profile management by subscriber) and location information

international standardized profile: internationally agreed-to, harmonised document which describes one or more profiles

invocation and operation: describes the action and conditions under which the service is brought into operation

NOTE: In the case of a lawful interception this may only be on a particular communication. It should be noted that when lawful interception is activated, invocation is applicable on all communications (invocation takes place either subsequent to or simultaneously with activation). Operation is the procedure which occurs once a service has been invoked.

Law Enforcement Agency (LEA): organization authorized by a lawful authorization based on a national law to request interception measures and to receive the results of telecommunications interceptions

Law Enforcement Monitoring Facility (LEMF): transmission destination for the results of interception relating to a particular interception subject

lawful authorization: permission granted to a LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator/access provider/service provider

NOTE: Typically this refers to a warrant or order issued by a lawfully authorized body.

Lawful Interception (LI): See interception.

Lawful Interception IDentifier (LIID): See definition in clause 5.2.2.

location information: information relating to the geographic, physical or logical location of an identity relating to an interception subject

Mediation Function (MF): mechanism which passes information between a network operator, an access provider or service provider and a Handover Interface, and information between the Internal Network Interface and the Handover Interface

network element: component of the network structure, such as a local exchange, higher order switch or service control processor

Network Element IDentifier (NEID): See definition in clause 5.2.4.

Network IDentifier (NID): See definition in clause 5.2.4.

NetWork Operator (NWO): operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means

profile: set of one or more base standards and/or international standardized profiles, and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base standards or International Standardized Profiles necessary to accomplish a particular function

Quality of Service (QoS): quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc.

NOTE: Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

reliability: probability that a system or service will perform in a satisfactory manner for a given period of time when used under specific operating conditions

result of interception: information relating to a target service, including the Content of Communication and Intercept Related Information, which is passed by a network operator, an access provider or a service provider to a Law Enforcement Agency

NOTE: Intercept Related Information is provided whether or not call activity is taking place.

sequence number: See definition in clause 5.2.5.

service information: information used by the telecommunications infrastructure in the establishment and operation of a network related service or services

NOTE: The information may be established by a network operator, an access provider, a service provider or a network user.

Service Provider (SvP): natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network

target identity: technical identity (e.g. the interception's subject directory number), which uniquely identifies a target of interception

NOTE: One target may have one or several target identities.

target service: telecommunications service associated with an interception subject and usually specified in a lawful authorization for interception

NOTE: There may be more than one target service associated with a single interception subject.

telecommunications: any transfer of signs, signals, writing images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system

Transport Related Information (TRI): information which is sent across a Handover Interface in order to maintain, test or secure the interface

NOTE 1: TRI does not include any CC or IRI.

NOTE 2: TRI is categorized as either information relating to the delivery of data to the LEA or the maintenance of transport connections between a DF (at a CSP) and LGW (at an LEA) - see clause 5.2.8.

3.2 Symbols

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

<parameter>	parameters are indicated by angle brackets
kB	Kilobyte

3.3 Abbreviations

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

NOTE: Some abbreviations are only used in the ASN.1 referenced in clause A.2.

3GPP	3rd Generation Partnership Project
AP	Access Provider
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
BER	Basic Encoding Rules
CBC	Cipher-Block Chaining
CC	Content of Communication
CID	Communication IDentifier
CIN	Communication Identity Number
CMS	Call Management Service
CPE	Customer Premises Equipment
CR	Change Request
CS	Circuit Switched
CSP	Communications Service Provider
DCC	Delivery Country Code
DER	Distinguished Encoding Rules
DF	Delivery Function
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
EIPID	Extended Interception Point IDentifier
EPS	Evolved Packet System
FIFO	First-In-First-Out
FIPS	Federal Information Processing Standards
GCSE	Group Communications System Enablers
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HI	Handover Interface
HI1	Handover Interface 1 (for Administrative Information)
HI2	Handover Interface 2 (for Intercept Related Information)
HI3	Handover Interface 3 (for Content of Communication)
HM	Handover Manager
ICMP	Internet Control Message Protocol
ID	IDentifier
ILHI	Inter LEMF Handover Interface
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPID	Interception Point IDentifier
IPSec	IP Security
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
IV	Initialization Vector
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LGW	Law enforcement monitoring facility GateWay
LI	Lawful Interception
LIID	Lawful Interception IDentifier
MF	Mediation Function (at CSP)
MPLS	Multi-Protocol Label Switching
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NEID	Network Element IDentifier
NF	Network Function
NFID	Network Function IDentifier

NID	Network IDentifier
NIST	National Institute of Standards and Technology
NWO	NetWork Operator
OID	Object IDentifier
OPID	OPerator IDentifier
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PROSE	PROximity SErvices
PS	Packet Switched
PSTN	Public Switched Telephone Network
PUB	PUBlication
QoS	Quality of Service
resLEMF	responding LEMF
RFC	Request For Comments
RTT	Round Trip Time
SACK	Selective ACKnowledgement
SHA	Secure Hash Algorithm
SSD	Service-Specific Details
SvP	Service Provider
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Type Length Value element
TRI	Transport Related Information
UDP	User Datagram Protocol
ULIC	UMTS LI Correlation
UMTS	Universal Mobile Telecommunications System
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

4 General

4.1 Functionality

Figure 1 shows the stages in the interception chain.

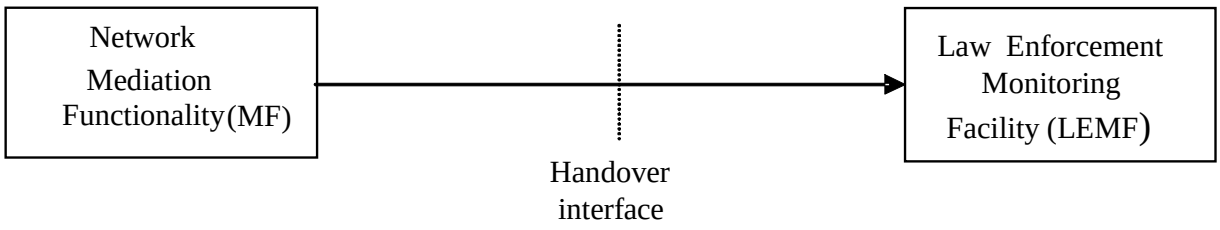

Figure 1: Stages of the interception chain

The first stage includes the creation or separation of intercepted data from the target network or target service, and the creation of IRI data. It is typically the responsibility of the CSP and is outside the scope of the present document.

The second stage ("Handover interface") consists of formatting the results of interception (except where IRI formats are specified in other standards), managing the connection between the CSP Mediation Functionality (MF) and the Law Enforcement Monitoring Facility (LEMF) and transporting the data. It should as far as possible be independent of the other stages and is the joint responsibility of the CSP and the LEA. The present document focuses on the handover interface.

The third stage includes functionality for interpreting and displaying the results of interception. It is typically the responsibility of the LEA and is outside the scope of the present document.