ETSI TS 102 232-1 V3.8.1 (2014-10)

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

Reference

RTS/LI-00124-1

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

Important notice

The present document can be downloaded from:
http://www.etsi.org

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

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

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 also available as an electronic attachment to the original document from the ETSI site (see clause A.2 for more details).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**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). It handles the transportation of intercepted traffic (HI3) and intercept-related information (HI2) but not the tasking and management of Lawful Interception (HI1).

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] and ETSI TS 102 232-6 [36]). 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 [1] and ETSI TR 101 944 [i.4].

For the handover of intercepted data within GSM/UMTS PS domain, the present document does not override or supersede any specifications or requirements in 3GPP TS 33.108 [9] and ETSI TS 101 671 [4].

2 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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

2.1 Normative references

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

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

[2] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

[3] Void.

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

NOTE: Periodically TS 101 671 is published as ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

[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; 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 codes".

[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 0791: "Internet Protocol".

[15] IETF RFC 0792: "Internet Control Message Protocol".

[16] IETF RFC 0793: "Transmission Control Protocol".

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

[18] IETF RFC 1323: "TCP Extensions for High Performance".

[19] IETF RFC 1191: "Path MTU discovery".

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

[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 TS 102 232-1 (V2.6.1).

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

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

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

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

[24] IETF RFC 5321: "Simple Mail Transfer Protocol".

NOTE: IETF RFC 5321 obsoletes IETF RFC 2821: "Simple Mail Transfer Protocol".

[25] IETF RFC 5322: "Internet Message Format".

NOTE: IETF RFC 5322 obsoletes IETF RFC 2822: "Internet Message Format".

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

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

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

[28] IETF RFC 3174: "US Secure Hash Algorithm 1 (SHA1)".

[29] Void.

[30] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

NOTE: IETF RFC 5280 obsoletes IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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

[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] ANSI/J-STD-025-B: "Lawfully Authorized Electronic Surveillance", (July 2006) as amended by ANSI/J-STD-025-B-1: "Lawfully Authorized Electronic Surveillance (LAES) Addendum 1 - Addition of Mobile Equipment IDentifier (MEID)" (September 2006) and by ANSI/J-STD-025-B-2: "Lawfully Authorized Electronic Surveillance (LAES) - Addendum 2 - Support for Carrier Identity" (April 2007) - Published by TIA/ATIS.

[40] FIPS PUB 186-4: "Digital Signature Standard (DSS)".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[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.

NOTE: See http://www.loc.gov/z3950/agency/.

[i.3] ETSI TS 123 107: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Quality of Service (QoS) concept and architecture (3GPP TS 23.107)".

[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] ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 101 671 [4], ETSI ES 201 158 [2], ETSI TS 101 331 [1] and the following apply:

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

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

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

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

NOTE: It does not include any CC or IRI.

3.2 Symbols

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

<parameter> parameters are indicated by angle brackets

3.3 Abbreviations

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

3GPP	Third 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
CR	Change Request
CSP	Communications Service Provider
DCC	Delivery Country Code
DER	Distinguished Encoding Rules
DF	Delivery Function
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
DSS/DSA	Digital Signature Standard / Digital Signature Algorithm
EPS	Evolved Packet System
FIFO	First-In-First-Out
FIPS	Federal Information Processing Standards
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
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
HO	Handover
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPSec	IP Security
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
IV	Initialization Vector
kB	Kilobyte
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LGW	Law enforcement monitoring facility GateWay
LI	Lawful Interception
LIID	Lawful Interception IDentifier
MD	Mediation Device
MF	Mediation Function (at CSP)
MPLS	Multi-Protocol Label Switching
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NEID	Network Element Identifier
NID	Network IDentifier
NWO	NetWork Operator
OID	Object Identifier
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PS	Packet Switched
PS-PDU	Packet Switched PDU
PSTN	Public Switched Telephone Network
PUB	Publication
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
TIPHON	Telecommunication and Internet Protocol Harmonization Over Networks
TLS	Transport Layer Security
TLV	Type Length Value element
TRI	Transport Related Information
UDP	User Datagram Protocol
UK	United Kingdom
ULIC	UMTS LI Correlation
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network

4 General

4.1 Functionality

Figure 1 shows the stages in the interception chain.

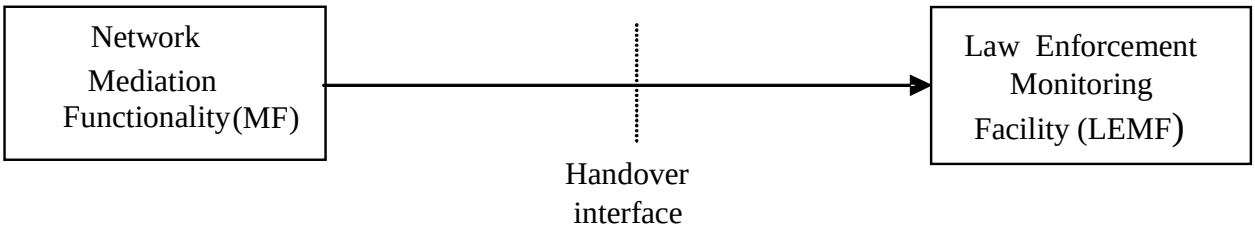

Figure 1: Stages of the interception chain

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.

4.2 Intercepted data types

Interception is possible at the following network elements: access element, network connectivity element and service element (as defined in ETSI TR 101 944 [i.4], clause 5.1). Each method is associated with one or more OSI Layer(s) and produces intercepted data in one or more formats, as shown by table 1 (see also ETSI TR 101 944 [i.4], figure 3).

Table 1: Intercepted data types

Component	OSI Layer(s)	Format of intercepted data
Access provider	1 (Physical)	Physical PDUs
	2 (Data link)	Data link PDUs
	3 (Network)	(IP) Datagrams
Network connectivity	3 (Network)	(IP) Datagrams
Service provider	5/7 (Application)	Application layer transactions (but see clause 4.2.2)

The present document covers the handover of data in the following two cases:

- "Network level" interception, consisting of (IP) datagrams from Network Operators or Access Providers.
- "Application level" interception, consisting of application layer transactions from Service Providers.

The present document does not cover the handover of intercepted physical PDUs or data link PDUs (OSI Layer 1 and Layer 2).

NOTE: The application level is also sometimes called the "service level"; the present document always refers to "application level" to avoid confusion over the term service.