Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
United States Department of Justice	)	RM No. 11376
	)	
Petition for Expedited Rulemaking to	)	
Establish Technical Requirements and	)	
Standards Pursuant to Section 107(b) of the	)	
Communications Assistance for Law	)	
Enforcement Act	)	

REPLY COMMENTS OF VERISIGN, INC.

Anthony M. Rutkowski
Vice President for Regulatory Affairs and
Standards
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

Filed: 25 Sept 2007

EXECUTIVE SUMMARY

In large measure, the views of the thirteen parties filing comments on the DOJ petition for rulemaking reflect the bifurcated treatment among the four capabilities that VeriSign suggested in its Comments. Effective time-stamp accuracy and packet activity reporting are well-settled requirements, are extensively available capabilities in most of the communications infrastructure today. There are no significant factual disputes, and the Commission can affirm and clarify these requirements by declaration, as well as make a J-STD-025-B deficiency finding. The critical importance of accurate time-stamps deserves explicit maintenance and traceability requirements such as found in the PacketCable™ CALEA standard – which the Commission can accomplish in a declaration as a compliance clarification and due diligence measure. More accurate time-stamps of 10 milliseconds or better - appropriate for today's forensic needs and now being pursued by other countries - can be treated in a NPRM.

The furnishing of reasonably available location information and the secure handover of call-identifying (intercept related) information to law enforcement suggest a need for further fact finding and applying relevant CALEA statutory tests, and is the proper subject of a rulemaking proceeding.

The implementation of DOJ's desired reliable VPN based handover capabilities was actually effected in the adoption of a new standard for this purpose several weeks ago in the principal international standardization body for lawful interception, and deserves substantial consideration as a means of meeting the DOJ reliable handover requirement in a NPRM.

I

THE COMMENTS SUPPORT BIFURCATED TREATMENT OF THE DOJ PETITION - A DECLARATION TO CLARIFY EXISTING TIME-STAMP ACCURACY AND PACKET REPORTING REQUIREMENTS COUPLED WITH A NPRM TO CONSIDER REMAINING CAPABILITIES BEING SOUGHT

1. Although only thirteen parties filed comments in the proceeding, the views largely reflected the bifurcated treatment among the four capabilities that VeriSign suggested in its Comments. Effective time-stamp accuracy and packet activity reporting seemed to reflect a view by most parties that these are well-settled requirements, and that the capabilities to support them are pervasively available in network infrastructure today. The arguments raised by opposing parties were essentially legal constructs aimed at precluding handover of port signalling data that have no technical or operational basis. There are no substantial factual disputes as to these two requirements, and the Commission can affirm and clarify these requirements by declaration, as well as make a J-STD-025-B deficiency finding.

II

THE RAISED PROCEDURAL CONCERNS ARE NOT A BAR TO THE COMMISSION PROCEEDING WITH A DECLARATION AND NPRM

2. Several parties filing opposing comments raised a variety of alleged procedural bars to proceeding to a declaration and NPRM. Some parties asserted that the petition lacks merit, is not required by CALEA, or is not timely. However, these arguments are not supported by either the law or the facts and themself lack merit. Whatever one's position might be on the reasonable availability of the forensics, it is difficult to imagine more fundamental characteristics of surveillance support than knowledge of when events occur, what basic signalling information is included in network digital packets, and reliable delivery of surveillance information to law enforcement monitoring facilities. As to timeliness, law enforcement provided requirements documents several years ago, expended significant resources participating in most of the ensuing standards

development work, and filed a deficiency petition within a few months of adoption of the standard. Given the constantly evolving nature of the requirements and technology, law enforcement is not precluded from adjusting its requirements as needed to support the necessary technology independent surveillance capabilities specified in CALEA.

3. Five parties filing opposing comments argued that DOJ cannot seek a deficiency determination that is applied broadly to all CALEA standards, asserting that deficiency petitions must be narrowly tailored to every developed CALEA standard for every technology platform and service. Aside from the fact that such a finding would result in a plethora of filings and potential proceedings that serve no party's interests, Sec. 107(b) of the CALEA statute allows for Commission to provide appellate relief among the disputing parties with the establishment of the Commission's own "rule, technical requirements, or standards" that provide the assistance capability requirements. Indeed, in the case of time-stamp accuracy, this very route has been previously taken, resulting in the current Commission promulgated standard for time-stamp accuracy, § 1.20007(a)(14) of the Rules. In taking this action, the Commission inherently establishes the capability standard for compliance. Furthermore, because the capabilities requested in the petition are all generic (with the exception of location accuracy), there is no technology platform dependence.

III

THE REQUIREMENT FOR TIME-STAMP ACCURACY SEEMS IMPLICITLY SUPPORT BY ALMOST ALL COMMENTING PARTIES

4. Only two parties argued against DOJ's request for a time-stamp accuracy clarification. One party asserted that time-stamps were "inconsistent" with the Internet. A second party asserted that DOJ provided insufficient detail in the petition concerning the deficiency. As to the former argument - aside from the fact that time-stamps are a ubiquitous technology-neutral means for network management and auditing – it is rather ironic that contemporary time-stamp accuracy technology based on the Network Time Protocol (NTP) was developed and deployed twenty years ago as a basic Internet service.

That technology now exists ubiquitously across all IP network infrastructures down to the personal computer level.

5. To the extent there may be any insufficiencies in the level of detail on time-stamp accuracy provided in the DOJ petition, the annexes on this topic in VeriSign's Comments provide an entire compendium of knowledge regarding this subject, how the various LI standards support or fail to provide the needed requirements, and what clarifications are needed. Furthermore, the CableLabs PacketCable 2.0 specifications on this subject provide a good industry-wide reference model. Accurate time-stamps are the most ubiquitous and important forensics data provided to law enforcement - as they are for effective network management, security, and auditing. The Commission should provide the necessary clarifications concerning reference clock traceability by declaration.

IV

THE REQUIREMENT FOR PORT AND OTHER SIGNALLING DATA SEEMS LARGELY SUPPORTED ON TECHNICAL CONSIDERATIONS

6. As with time-stamp accuracy, the provision of port and underlying transport layer information is an established requirement in virtually every LI signalling specification in the world and widely if not universally available at intercept access points. Ports are used for TCP and UDP layer routing – in many cases for special processing within network infrastructures. Notwithstanding the long-established treatment of this information as signalling, as well as the ubiquitous existence of the technical monitoring capability, several opposing parties in their comments raised hypothetical legal constructs and bald assertions that would preclude its availability as content-identifying information to law enforcement. Accepting such constructs would have substantial adverse effects not only for law enforcement, but for network operators who manage and protect their networks relying on port number analysis. The Commission should clarify in a declaration that packet transport layer and port signalling constitute call-identifying information and must be provided.

V

ACCESS TO ENHANCED LOCATION DATA SEEMS APPROPRIATE, IF REASONABLY AVAILABLE, ALTHOUGH IMPLEMENTATION DETAILS APPEAR SUBJECT TO DIVERGING CONCERNS

7. As with most of the other capabilities being sought, opposing parties raised primarily legal constructs rather than technical arguments against access to the information. This subject is also significantly entwined with Commission action concerning Enhanced 911 Phase II accuracy requirements in the Docket 07-114 proceeding for which long range goals were recently set by the Commission. The largest affected provider in its Comments seemed to offer a good analysis of the nature and extent of the difficulties in meeting various kinds of capability requirements.[1] The Commission in the NPRM phase of this proceeding explore the options raised and the associated costs and implementation timeframes.

VI

ALTHOUGH MOST COMMENTING PARTIES ARE CONCERNED ABOUT THE POTENTIAL SHIFTING OF COSTS AND BUFFERING, THE RECENT ADOPTION OF AN INTERNATIONAL STANDARD FOR RELIABLE LAWFUL INTERCEPTION DELIVERY HOLDS SIGNIFICANT PROMISE AS A GLOBALLY ACCEPTABLE SOLUTION

8. Most commenting parties seemed to focus at some length on DOJ's proffered solutions to the CALEA requirement for reliable delivery of surveillance information in an era of broadband IP-enabled local access network infrastructure. The responsibilities at the "handover interface" – which is the term used by the Lawful Interception industry worldwide, are clearly shared between operators/providers and law enforcement under CALEA. Even if law enforcement is responsible for transport, both parties must work together on a means of supporting the handover interface.

---

[1] *See Comments of Verizon Wireless in RM-11376* at 4.

9. For the past five years, significant numbers of providers, vendors, LI equipment suppliers, and law enforcement agencies worldwide have been working effectively together to enable this broadband LI handover requirement in the principal international standards forum for LI (TC LI), producing a technical standard that was adopted in July, which seems to provide the needed DOJ capability requirement.[2] Law enforcement agencies worldwide, like DOJ in the U.S., have identified this same capability requirement, and developed needed capabilities with industry in the form of the TS 102231-01. As with most LI technical specifications from the TC LI industry standards forum, there is substantial vendor implementation worldwide, as well as structured interoperability "bakeoff" testing that occurs to assure the standard is sufficient to meet handover needs – often resulting in subsequent improvement of the standard.

10. The first several pages of the specification are provided in an Appendix. As can be noted from the Table of Contents and introduction, the specification objective…

> …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 specification 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.

VeriSign suggests that full consideration of this specification be given in an NPRM responsive to the DOJ petition. Very significant reduction in costs for both providers and

---

[2] *See Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery*, Technical Specification ETSI TS 102 232-1 V2.2.1 (2007-07)

law enforcement, including the ability to implement transnational LI capabilities by affected providers, flows from the global implementation of a common, technically-thorough, broadband handover interface. The use of global reliable handover and delivery standards should be given full consideration as a means of meeting DOJ CALEA requirements.

VII

MOST CAPABILITIES SOUGHT BY DOJ CAN BE READILY IMPLEMENTED WITHIN THE DESIRED TIMEFRAME – ESPECIALLY BY TRUSTED THIRD PARTY CALEA PROVIDERS

11. With the exception of the location information – which Verizon Wireless notes in its comments as potentially requiring more than 12 months - it is not apparent that any of the other capability requirements at issue in the DOJ petition could not be implemented within the desired timeframe. In many cases, as also noted by Verizon Wireless, the capabilities already exist. To the extent that any affected carrier has difficulties meeting the requirements, Trusted Third Party CALEA providers such as VeriSign's NetDiscovery Service are available to provide solutions.

ETSI TS 102 232-1 V2.2.1 (2007-07)

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-00043-1

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2007.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights 6
Foreword 6
Introduction 6
1 Scope 7
2 References 7
3 Definitions and abbreviations 9
3.1 Definitions 9
3.2 Abbreviations 9
3.3 Symbols 10
4 General 10
4.1 Functionality 10
4.2 Intercepted data types 11
4.2.1 Interception at network operator or access provider 11
4.2.2 Interception at service providers 11
4.3 Relationship to other standards 12
4.3.1 Handover for GPRS / UMTS PS 13
5 Headers 13
5.1 General 13
5.2 Description and purpose of the header fields 13
5.2.1 Version 13
5.2.2 LIID 13
5.2.3 Authorization country code 13
5.2.4 Communication identifier 14
5.2.5 Sequence number 14
5.2.6 Payload timestamp 15
5.2.7 Payload direction 15
5.2.8 Payload type 15
5.2.9 Interception type 15
5.2.10 IRI type 15
5.2.11 Interception Point Identifier 15
5.3 Encoding of header fields 15
6 Data exchange 16
6.1 Introduction 16
6.2 Handover layer 17
6.2.1 General 17
6.2.2 Error reporting 18
6.2.3 Aggregation of payloads 18
6.2.4 Sending a large block of application-level data 18
6.2.5 Padding data 19
6.2.6 Payload encryption 19
6.3 Session layer 19
6.3.1 General 19
6.3.2 Opening and closing connections 19
6.3.3 Buffering 20
6.3.4 Keep-alives 20
6.4 Transport layer 20
6.4.1 Introduction 20
6.4.2 TCP settings 21
6.4.3 Acknowledging data 21
6.5 Network layer 21
7 Delivery networks 21

7.1 Types of network ... 21
7.1.1 General ... 21
7.1.2 Private networks ... 21
7.1.3 Public networks with strict control ... 22
7.1.4 Public networks with loose control ... 22
7.2 Security requirements ... 22
7.2.1 General ... 22
7.2.2 Confidentiality and authentication ... 22
7.2.3 Integrity ... 22
7.3 Further delivery requirements ... 24
7.3.1 Test data ... 24
7.3.2 Timeliness ... 24

Annex A (normative): ASN.1 syntax trees ... 25

A.1 ASN.1 syntax tree for HI2 and HI3 headers ... 25

A.2 ASN.1 specification ... 26

A.3 Importing parameters from other standards ... 31

Annex B (informative): Requirements ... 32

B.1 Types of intercepted information ... 32

B.2 Identification of traffic ... 32

B.3 Performance ... 32

B.4 Timeliness ... 33

B.5 Reliability and availability ... 33

B.6 Discarding information ... 33

B.7 Security ... 33

B.8 Other ... 34

Annex C (informative): Notes on TCP tuning ... 35

C.1 Implement RFC 2581 ... 35

C.2 Minimize roundtrip times ... 35

C.3 Enable maximum segment size option ... 35

C.4 Path MTU discovery ... 35

C.5 Selective acknowledgement ... 35

C.6 High speed options ... 35

C.7 PUSH flag ... 36

C.8 Nagle's algorithm ... 36

C.9 Buffer size ... 36

Annex D (informative): IRI-only interception ... 37

D.1 Introduction ... 37

D.2 Definition HI information ... 37

D.3 IRI deriving ... 37

D.4 IRI by post and pre-processing HI3 information ... 38

Annex E (informative): Purpose of profiles ... 39

E.1 Formal definitions ... 39

E.2 Purpose of profiles 39

Annex F (informative): Traffic management of the handover interface 41

F.1 Background 41
F.1.1 Burstiness 41
F.1.2 Mixed content..... 41
F.1.3 Network facilities for traffic management 42
F.1.4 Evidentiary considerations..... 42
F.1.5 National considerations..... 42

F.2 Traffic management strategies 42

F.3 Bandwidth estimation.....43

F.4 National considerations.....43

F.5 Implementation considerations 43
F.5.1 Volatile versus non-volatile storage 43
F.5.2 Maximum buffering time..... 44
F.5.3 Transmission order of buffered data..... 44
F.5.4 Buffer overflow processing 44

Annex G (informative): Bibliography.....45

Annex H (informative): Change request history.....46

History 48

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://webapp.etsi.org/IPR/home.asp).

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 E-mail 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".

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 specification 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.

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 TS 102 227 (see bibliography), TS 101 909-20-1 [33], TS 101 909-20-2 [34], TS 102 232-2 [5] and TS 102 232-3 [6]). Where possible, the present document aligns with 3GPP TS 33.108 [9] and TS 101 671 [4] and supports the requirements and capabilities defined in TS 101 331 [1] and TR 101 944 (see bibliography).

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 TS 101 671 [4].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version 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.

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

[9] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); 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] ITU-T Recommendation X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

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

[13] FIPS PUB 186-2: "Digital Signature Standard (DSS)".

[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 2246: "The TLS Protocol Version 1.0".

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

[23] IETF RFC 2581: "TCP Congestion Control".

[24] IETF RFC 2821: "Simple Mail Transfer Protocol".

[25] IETF RFC 2822: "Internet Message Format".

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

[27] IETF RFC 2988: "Computing TCP's Retransmission Timer".

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

[29] IETF RFC 3268: "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)".

[30] 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".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 671 [4], ES 201 158 [2], 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 Abbreviations

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

3GPP	Third Generation Partnership Project
AP	Access Provider
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
BER	Basic Encoding Rules
CC	Content of Communication
CID	Communication IDentifier
CIN	Communication Identity Number
CSP	Communications Service Provider
DCC	Delivery Country Code
DF	Delivery Function
DSL	Digital Subscriber Line
FIFO	First-In-First-Out
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
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPSec	IP Security
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider

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
NID	Network IDentifier
NWO	NetWork Operator
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PS	Packet Switched
PSTN	Public Switched Telephone Network
RTT	Round Trip Time
SACK	Selective ACKnowledgement
SvP	Service Provider
TCP	Transmission Control Protocol
TIPHON	Telecommunication and Internet Protocol Harmonization Over Networks
TLS	Transport Layer Security
TRI	Transport Related Information
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network

3.3 Symbols

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

<parameter>	Parameters are indicated by angle brackets

4 General

4.1 Functionality

Figure 1 shows the stages in the interception chain.

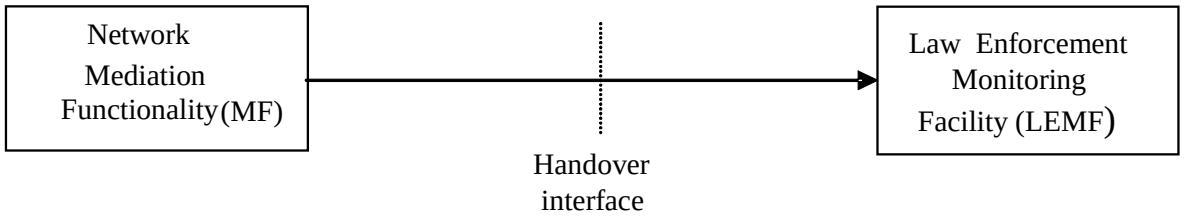

Figure 1: Stages of the interception chain

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.