ETSI-IP.nl

Implementing ETSI TS 102 232 "Handover Interface and Service-Specific Details for IP delivery" in the Netherlands (ETSI-IP.nl)

Version 1.0; 6 September 2011

Agreed by Ad hoc Working group "Afhechten ETSI-IP.nl Specificatie"; 24 August 2011

Approved by Platform 13; 6 September 2011

This specification was produced by
Ad hoc Working group "Afhechten ETSI-IP.nl Specificatie"
and is owned by
"Ministry of Security and Justice"
and available via the depositary
"Agentschap Telecom;
Ministry of Economic Affairs, Agriculture and Innovation

Postal address: PO Box 450, 9700 AL Groningen; the Netherlands
Phone: +31 50 587 7444 - Fax: +31 50 587 7400
Email: info@agentschaptelecom.nl

Contents

Introduction

This document lists and fills in the specific items related to the ETSI-LI standard TS 102 232-1 [1] and its successive Service Specific Details (SSD) parts which together describe a handover interface for the transport of lawful intercepted information derived from IP-based networks between a network operator, access provider and/or service provider and a Law Enforcement Agency (LEA). In the Netherlands, this document is mandatory for implementations of TS 102 232.

NOTE: A reference made in the text of this document to a "clause" is pointing to the indicated ETSI Technical Specification. A reference made to a "section" is related to a section in this document.

List of abbreviations

ASN.1	Abstract Syntax Notation One
CC	Content of Communication
CIN	Communication Identity Number
CSP	Communication Service Provider
DCC	Delivery Country Code
DF	Delivery Function
ETSI	European Telecommunications Standards Institute
HI1	Handover Interface 1 (for Administrative Information)
HI2	Handover Interface 2 (for Intercept Related Information)
HI3	Handover Interface 3 (for Content of Communication)
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LGW	Local Gateway
LIID	Lawful Interception IDentifier
MF	Mediation Function
NEID	Network Element IDentifier
NID	Network Identifier
PDU	Protocol Data Unit
PS	Packet Switched
RTP	Real Time Protocol
SSD	Service-Specific Details
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

References

NOTE: The specific version numbers of the ETSI specifications are the versions valid at the time of adaptation of the present document.

[1] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery " version 2.7.1 (2011-08).

[2] 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" version 2.6.1 (2011-08).

[3] 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" version 2.3.1 (2011-08).

[4] 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" version 2.3.1 (2010-08).

[5] 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" version 2.5.1 (2010-10).

[6] 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" version 2.3.1 (2008-08).

[7] 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" version 2.2.1 (2011-03).

[8] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic" version 3.7.1 (2011-08).

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.

[9] Implementing ETSI ES 201 671 in the Netherlands Version 1.0; 6 February 2001

[10] ITU-T Recommendation G.711 (1988): "Pulse code modulation (PCM) of voice frequencies".

[11] IETF RFC 0793: “Transmission Control Protocol (TCP)”.

[12] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

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

1 Scope of this document

This document shall be read aside TS 102 232-1 [1]. The sections of this document will clarify the Dutch implementation of TS 102 232-1. Unless otherwise indicated no issues mentioned in informative annexes will affect the implementation of TS 102 232-1 in the Netherlands.

TS 102 232-1 [1] 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".

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

In this document NL specific requirements related to TS 102 232 part 2 and further are covered in the corresponding annexes B - G of this document.

2 General

Reference: TS 102 232-1 clause 4

No remarks.

3 Headers

Reference: TS 102 232-1 clause 5

3.1 Lawful Interception IDentifier *(TS 102 232-1 clause 5.2.2)*

For each warrant a globally unique identifier is defined. This Lawful Interception IDentifier (LIID) consists of 8 decimal digits followed by an MD5 hash, two octets for use by the CSP and three octets for future use. The LIID is generated by the Law Enforcement Agency (LEA).

Total length of the LIID is 25 octets:

- 8 decimal digits (BCD encoded, 4 octets);
- MD5 hash (16 octets);
- for CSP use (default value 0xFF00 set by the LEA, 2 octets);
- reserved for future use (initial value 0xFF00FF, 3 octets).

Example: 12345678001122334455667788 99AABBCCDDEEFFFF00FF00FF

In this way a LEA can generate its own identifiers, without compromising the interested Law Enforcement Monitoring Facility (LEMF) if the packet is intercepted en route.

The LEA can ignore the last five octets as received via HI2 or/and HI3.

3.2 Authorization country code *(TS 102 232-1 clause 5.2.3)*

Authorization country code for warrants originating in the Netherlands is: NL

3.3 Communication identifier *(TS 102 232-1 clause 5.2.4)*

The Network Identifier (NID) consists of the operator identifier and Network Element IDentifier (NEID). The NEID shall be implemented and used as dictated in TS 101 671 [8]. The operator identifier shall consist of 8 decimal characters describing internationally unique a network operator, access provider or service provider and is mandatory. In the Netherlands, it will consist of 031 plus five digits. The list will be maintained and made available by the Agency Telecommunication of the Ministry of “Economic Affairs, Agriculture and Innovation”.

NOTE: In ETSI TS 101 671 [8] the operator identifier consists of 5 decimal characters.

The use of the CIN extension field is supported.

The delivery country code (DCC) for the Netherlands is: NL.

3.4 Payload timestamp *(TS 102 232-1 clause 5.2.6)*

Use of the MicroSecondTimeStamp is mandatory for HI1, HI2 and HI3 for all services.

Use of the timeStampQualifier field is mandatory for all services.

3.5 Payload direction *(TS 102 232-1 clause 5.2.7)*

Use of payload direction is mandatory.

3.6 IRI type *(TS 102 232-1 clause 5.2.10)*

Use of IRI-type is mandatory.

4 Data exchange

Reference: TS 102 232-1 clause 6

4.1 Handover layer, general *(TS 102 232-1 clause 6.2.1)*

PDUs shall be distributed randomly across all available DFs.

The logical communication path is one way, DF to LGW.

4.2 Error reporting *(TS 102 232-1 clause 6.2.2)*

Error reporting from the MF Handover Manager to the LEMF Handover Manager shall be subject to bilateral agreement between CSP and LEA.

4.3 Aggregation of payloads *(TS 102 232-1 clause 6.2.3)*

Aggregation of payloads shall be done according to clause 6.2.3 in TS 102 232-1.

At most one second or one Megabyte of CCPayload traffic (measured on intercepted payload) can be aggregated in one PS-PDU. Timestamp on each item (i.e. CCPayload) shall be provided. IRIPayload cannot be aggregated.

4.4 Sending a large block of application-level data *(TS 102 232-1 clause 6.2.4)*

Application-level data shall be segmented when it exceeds a size of 1 (one) Megabyte.

4.5 Padding data *(TS 102 232-1 clause 6.2.5)*

Sending of padding data is allowed.

4.6 Payload encryption *(TS 102 232-1 clause 6.2.6)*

The delivery manager shall perform encrypted handover using the encryptedPayload ASN.1 structure. Encryption Type shall be AES-192-CBC. By concatenating the sequence number 4 times, a 128 bits Initialisation Vector is created. The Initialisation Vector is computed for each PDU. If padding is needed, it shall be all zeros. Encryption shall be used for all Payload Types (e.g. TRIPayload shall always be nested within encrypted Payload). An unencrypted Payload shall always be nested within an encrypted Payload.

The use of the encryptedPayloadType is mandatory in NL.

4.7 Session layer, general *(TS 102 232-1 clause 6.3.1)*

The path from DF to LEMF shall be an encrypted tunnel according TLS RFC 5246 [13]. Only for debugging purposes the use of plain TCP (IETF RFC 0793 [11]) is allowed.

4.8 Opening and closing connections *(TS 102 232-1 clause 6.3.2)*

The attempt retry interval shall be configurable between 30 and 300 seconds. The default attempt retry interval shall be 30 seconds.

4.9 Buffering *(TS 102 232-1 clause 6.3.3)*

The size of the cyclic buffer shall be sufficient to buffer an amount of traffic covering the actual retry interval as defined in clause 4.8 plus 5 seconds with a maximum of half of typical available RAM by the processor.

NOTE: State of the art August 2011 is typically 4GB.

4.10 Keep alives *(TS 102 232-1 clause 6.3.4)*

Session Layer “keep alives” will not be used.

4.11 Transport layer, TCP settings *(TS 102 232-1 clause 6.4.2)*

The port number for TLS is 3004.

The port number for plain TCP is 3003.

4.12 Acknowledging data *(TS 102 232-1 clause 6.4.3)*

Data is considered to be successfully sent once a further 1 (one) Megabyte of data has passed through the TCP socket (2).

5 Delivery networks

Reference: TS 102 232-1 clause 7

5.1 Types of network, general *(TS 102 232-1 clause 7.1)*

The network used for data exchange will be limited VLANs at the AMSiX or NLiX. The transport layer will use an IP connection with "like private peering" via the AMSiX or NLiX.

NOTE: For test purposes other solutions are allowed.

5.2 Security requirements, general *(TS 102 232-1 clause 7.2.1)*

The path from DF to LGW shall be an encrypted tunnel according TLS RFC 5246 [13].

5.3 Confidentiality and authentication *(TS 102 232-1 clause 7.2.2)*

Encryption shall be based on TLS_RSA_WITH_AES_256_CBC_SHA with a fallback defined by TLS_DHE_RSA_WITH_AES_256_CBC_SHA RFC 5246 [13].

5.4 Integrity *(TS 102 232-1 clause 7.2.3)*

The inclusion of the "message digests" is mandatory irregardless of the HI1 interface.

The following default values must be configurable in line with TS 102 232-1 clause 7.2.3 [1]. The current default values are:

<trafficTime>:	1 (one) second
<pduCount>:	not used
<hashTimeout>:	300 seconds
<predefined number of> IntegrityCheck PDUs:	15
<predefined number of> seconds:	1800

5.5 Test data *(TS 102 232-1 clause 7.3.1)*

Automatic generation of test PDUs at the activation of the intercept is not used.

Annex A (normative):
Electronic HI1 Interface (e-sub-HI1) Specification

For Further Study

Annex B (normative): Requirements for E-mail services (TS 102 232-2 [2])

B.1 SMTP HI2 event-record mapping

Reference: TS 102 232-2 clause A.4 Table A2: SMTP E-mail event records

SMTP events	Subject	HI2 record
E-mail send successful	Client	Report
E-mail send unsuccessful	Client	Report

B.2 POP3 HI2 event-record mapping

Reference: TS 102 232-2 clause B.4 Table B.2: POP3 E-mail event records

POP3 events	Subject	HI2 record
E-mail download	Client	Report
E mail partial download	Client	Report

B.3 Indication of e-mail-Sender-Validity

Reference: TS 102 232-2 clause F.2: SMTP protocol characteristics

The use of the "e-mail-Sender-Validity" to indicate the assurance by the CSP of the e-mail address is mandatory.

Annex C (normative): Requirements for Internet Access Services (TS 102 232-3 [3])

C.1 HI2 attributes

Reference: TS 102 232-3 clause 6.2

In Table 2 HI2 attributes: NOTE 2: The password need not be removed from the raw AAA data before handover.

Annex D (normative): Requirements for Layer 2 Services (TS 102 232-4 [4])

D.1 IRI events

Reference: TS 102 232-4 clause 6.1

CIN allocation shall be performed on the Access Attempt.

D.2 Target Location

Reference: TS 102 232-4 clause 8.1 (L2IRIContents) and clause A.1.1 table A.1 through A.8

Target Location is not required as long as this item is under study by ETSI.

Annex E (normative): Requirements for IP Multimedia Services (TS 102 232-5 [5])

E.1 General Requirements

Reference: TS 102 232-5 clause 4.3

Item 6) does not apply. Mapping of the IRI information onto specific messages at the handover interface is not used.

E.2 Events and IRI record types

Reference: TS 102 232-5 clause 5.4

Table 1: Mapping between IP MM Events and HI2 Records Type

The use of the IRI Record Types BEGIN, CONTINUE and END is not mandatory. If the IRI Record Type is not differentiated the IRI Record Type must be REPORT.

The choice of either implementation (BEGIN-CONTINU-END or REPORT) is made per communication session.

E.3 Interception of Content of Communication

Reference: TS 102 232-5 clause 5.5

The RTP CC shall always contain the RTP header. If the RTP header is not available the CSP shall add an artificial valid header in line with RFC 3550 [12].

The RTP CC shall contain the UDP header and IP header if available.

E.4 Correlation of IRI and CC

Reference: TS 102 232-5 clause 6.2

In case of multiple media streams the use of the streamIdentifier field for additional correlation is allowed.

E.5 Minimum set of functional attributes to be provided

Reference: TS 102 232-5 annex B

The minimum set of functional attributes as defined in annex B is considered to be informative for NL. Specific items are defined in the main body of this document (e.g. as buffering in section 4.9 of this document).

Annex F (normative): Requirements for PSTN/ISDN Services (TS 102 232-6 [6])

F.1 CC format

Reference: TS 102 232-6 clause 6.2

If no codec indication at all is sent the default codec is G.711 [10].

F.2 Sending supplementary information

Reference: TS 102 232-6 clause 6.3.3

Replacement of last part of clause 6.3.3 of TS 102 232-6:

Supplementary information shall be sent as IRI. When the codec is not G.711 [10] the supplementary information shall also be sent as CC-PDUs (in this case at least in the first PDU and in the following PDUs only if there are any changes during the session).

F.3 LI functionality

The functionality of the delivered PSTN/ISDN services described in ETSI TS 101 671 [8] and "Implementing ETSI ES 201 671 in the Netherlands" Version 1.0; 6 February 2001 [9] is applicable.

NOTE: The applicable content of "Implementing ETSI ES 201 671 in the Netherlands" Version 1.0; 6 February 2001 [9] is to be moved to this Annex F, as CS delivery becomes obsolete.

Annex G (normative): Requirements for Mobile Services (TS 102 232-7 [7])

No remarks.

Annex H (informative): Version numbers of related referenced documents

Table H.1 is included for maintenance purposes. It provides an overview of the versions of the normative reference documents that were used during the implementation of a given version of the present document (the ETSI-IP.nl specification). This table is actualised with every new issue of the ETSI-IP.nl specification. Upgrading a version number in this table to the newest version of a normative reference document is no automatism but a considered decision depending on the impact and necessity of such an upgrade.

Table H.1: List of referenced specifications with version numbers

TS 102 232 part:	N / I	Normative referenced documents in TS 102 232 parts	version d.d. 15-08-2011
5	N	ATIS-PP-1000678.2006: "Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunication Networks", Version 2 (Revision of ANS T1.678-2004).	2006
1	I	ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".	1.2.1 (2002-04)
6	I	ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".	1.1.1 (2006-03)
1	I	ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".	ed.1 (1995-11)
1,2,4,5	I	ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".	1.3.1 (2009-10)
1,2,3,4, 5,6,7	N	ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".	3.8.1 (2011-08)
1	N	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".	1.1.2 (2005-10)
1	N	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".	1.2.1 (2006-03)
2,3,4,5, 6,7	N	ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".	2.7.1 (2011-08)
1,4	N	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".	2.6.1 (2011-08)
1,4	N	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".	2.3.1 (2011-08)
1	N	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".	2.3.1 (2010-08)
1	N	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".	2.5.1 (2010-10)
1	N	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".	2.3.1 (2008-08)
1	N	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".	2.2.1 (2011-03)
4		ETSI TS 123 060: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description; Stage 2 (3GPP TS 23.060 Release 6)".	10.4.0 (2011-06)
1,2,5,7	N	ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 Release 9)".	10.4.0 (2011-06) 9.6.0 (2011-04) 8.13.0 (2011-04) 7.10.0 (2011-02)
6	I	ETSI TS 187 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Lawful Interception; Lawful interception functional entities, information flow and reference points".	2.1.1 (2009-09)
1		FIPS PUB 186-2: "Digital Signature Standard (DSS)".	27 January 2000
3		IEEE 802.11 (ISO/IEC 8802-11): "IEEE Standards for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan AreaNetwork - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".	2007

TS 102 232 part:	N / I	Normative referenced documents in TS 102 232 parts	version d.d. 15-08-2011
1		IETF RFC 0791: "Internet Protocol".	September 1981
1		IETF RFC 0792: "Internet Control Message Protocol".	September 981
1	N	IETF RFC 0793: "Transmission Control Protocol".	September 1981
1,3,4		IETF RFC 1122: "Requirements for Internet Hosts – Communication Layers".	October 1989
1		IETF RFC 1191: "Path MTU discovery".	November 1990
1		IETF RFC 1323: "TCP Extensions for High Performance".	May 1992
3,4		IETF RFC 1570: "PPP LCP Extensions".	January 1994
4		IETF RFC 1661: "The Point-to-Point Protocol (PPP)".	July 1994
2		IETF RFC 1939: "Post Office Protocol - Version 3".	May 1996
3		IETF RFC 1990: "The PPP Multilink Protocol (MP)".	August 1996
1		IETF RFC 2018: "TCP Selective Acknowledgement Options".	October 1996
3		IETF RFC 2131: "Dynamic Host Configuration Protocol".	March 1997
3	N	IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".	March 1997
4		IETF RFC 2341: "Cisco Layer Two Forwarding (Protocol) L2F".	May 1998
4	N	IETF RFC 2427: "Multiprotocol Interconnect over Frame Relay".	September 1998
1		IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".	December 1998
2		IETF RFC 2595: "Using TLS with IMAP, POP3 and ACAP".	June 1999
4		IETF RFC 2637: "Point-to-Point Tunneling Protocol (PPTP)".	July 1999
4		IETF RFC 2661: "Layer Two Tunneling Protocol (L2TP)".	August 1999
4	N	IETF RFC 2684: "Multiprotocol Encapsulation over ATM Adaptation Layer 5".	September 1999
3		IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".	June 2000
3		IETF RFC 2866: "RADIUS Accounting".	June 2000
1		IETF RFC 2923: "TCP Problems with Path MTU Discovery".	September 2000
3,4		IETF RFC 3046: "DHCP Relay Agent Information Option".	January 2001
3		IETF RFC 3118: "Authentication for DHCP Messages".	June 2001
1		IETF RFC 3174: "US Secure Hash Algorithm 1 (SHA1)".	September 2001
2		IETF RFC 3207: "SMTP Service Extension for Secure SMTP over Transport Layer Security".	February 2002
5		IETF RFC 3261: "SIP: Session Initiation Protocol".	June 2002
3		IETF RFC 3396: "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)".	November 2002
2		IETF RFC 3493: "Basic Socket Interface Extensions for IPv6".	February 2003
2		IETF RFC 3501: "Internet Message Access Protocol - Version 4 rev1".	March 2003
5	N	IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".	July 2003
6	N	IETF RFC 3551: "RTP Profile for Audio and Video Conferences with Minimal Control".	July 2003
3		IETF RFC 4282: "The Network Access Identifier".	December 2005
2		IETF RFC 4422: "Simple Authentication and Security Layer (SASL)".	June 2006
5,6	N	IETF RFC 4566: "SDP: Session Description Protocol".	July 2006
2		IETF RFC 4616: "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism".	August 2006
2		IETF RFC 4954: "SMTP Service Extension for Authentication".	July 2007
5		IETF RFC 4975: "The Message Session Relay Protocol (MSRP)".	September 2007
1	N	IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".	August 2008
1		IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",	May 2008
1,2		IETF RFC 5321: "Simple Mail Transfer Protocol".	October 2008
1,2		IETF RFC 5322: "Internet Message Format".	October 2008
1		IETF RFC 5681: "TCP Congestion Control".	September 2009
1		IETF RFC 6298: "Computing TCP's Retransmission Timer".	June 2011
1,2,3	N	ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".	July 2007
1		ISO/IEC TR 10000-1: "Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: General principles and documentation framework".	October 1998
4		ITU-T Recommendation E.164: "The international public telecommunication numbering plan".	November 2010

TS 102 232 part:	N / I	Normative referenced documents in TS 102 232 parts	version d.d. 15-08-2011
6	N	ITU-T Recommendation G.711 (1988): "Pulse code modulation (PCM) of voice frequencies".	November 1988
5		ITU-T Recommendation H.225.0: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".	December 2009
5		ITU-T Recommendation H.245: "Control protocol for multimedia communication".	May 2011
5		ITU-T Recommendation H.248: "Gateway control protocol". NOTE: H.248 was renumbered when revised on 2002-03-29. H.248 main body, Annexes A to E and Appendix I were included in H.248.1. Subsequent annexes were sequentially numbered in the series, e.g. H.248 Annex F became H.248.2	
5		ITU-T Recommendation H.323: "Packet-based multimedia communications systems".	December 2009
2		ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".	November 1988
1,2,3,4, 5,6		ITU-T Recommendation X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".	November 2008
1		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)".	November 2008
1,7	I	TIA/ATIS ANSI/J-STD-025-B: "Lawful Authorized Electronic Surveillance," (August 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).	August 2006
7	I	US 103rd Congress, Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414, 108 STAT. 4279 (Oct. 25, 1994).	October 1994

NOTE: N=Normative, I=Informative
Specifications are indicated as Normative:
1) in case the ASN.1 is importing data from that specification;
2) the specification is referenced in the ASN.1 definition;
3) the specification is referenced in this ETSI-IP.nl standard.

Annex I (informative): Transport implementation

NOTE: This annex describes the Dutch IP LI delivery architecture to clarify the choices of some of the TS 102 232 options as listed in ETSI-IP.nl.

I.1 General

The task of the Handover Manager (HM) is to handover intercepted data of all running intercepts to the appropriate destination(s). In order to do so, the Handover Manager creates minimally one Delivery Function (DF) (see TS 102 232-1 clause 6.3). For functional reasons or reasons of availability, multiple Delivery Functions may be created; each pointing to a different intermediate destination, a so called LEMF-Gateway (LGW). Only a one way logical communication path from the DF to the LGW is allowed (see section 4.1 of this document). The MF Handover Manager is responsible for distributing the PDUs over the appropriate LEMF-Gateway(s). The LEMF-Collection Function (LCF) is responsible for collecting traffic from the LGWs and delivery to the LEMF. Figure I.1 depicts the LEMF Gateway concept.

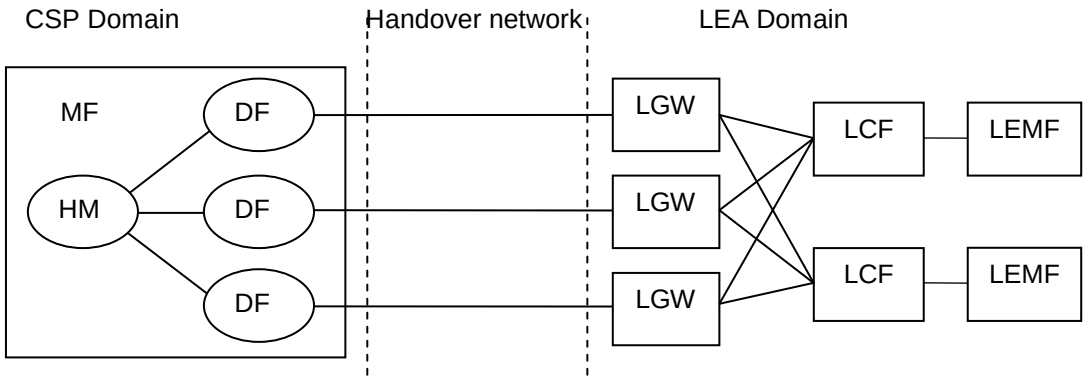

Figure I.1: The Dutch concept of the LEMF Gateway at the LEA side

I.1.1 Handover Manager (HM)

The Handover Manager performs the following operations:

- Aggregate or segment/reassemble payloads if required (see TS 102 232-1 clauses 6.2.3 and 6.2.4);
- Associate header information (see TS 102 232-1 clause 5.2);
- Create padding PDUs if required (see TS 102 232-1 clause 6.2.5);
- Assign PDUs to a Delivery Function (see TS 102 232-1 clause 6.2.1).

Except for debugging purposes the HM all PDUs are encrypted with a known cryptographic key. This key is specified for each LIID in the HI1 (see section 4.7).

I.1.2 Delivery Function (DF)

The Delivery Function is responsible for the following operations:

- The DF opens, establishes and maintains a TLS tunnel to every LGW defined in the legal authorisation. The keys are negotiated via the HI1. If a LGW cannot be reached the DF tries to re-connect (see sections 4.8 and 5.2).
- The TLS tunnel only accepts use allowed cryptosuites. Provisions are taken that the negotiation of other cryptosuites than the allowed set results in disconnection of the tunnel. An alarm can be raised to authorised personnel in this case (see section 5.3).

- The DF opens establishes and maintains a TLS tunnel to every LGW using TCP-port 3004 (see section 4.11).

I.1.3 LEMF-Gateway (LGW)

The LEMF-Gateway performs the following operations:

- The LGW accepts incoming TLS tunnels from every known DF functional unit. Known means that both the IP address (range) and public key of the DF are available to the LGW. The keys are negotiated via the HI1 (see sections 4.8 and 5.2).
- The LGW accepts traffic from every DF functional entity with which it has an authenticated client-server relation. The accepted traffic is to be forwarded to a LCF collection function. Which LCF will be chosen depends on the Lawful Interception Identifier (LIID) and on the EncryptedPayloadType information in the EncryptionHeader of the PDU (see TS 102 232-1 clause 6.2.1).
- The LGW can deliver incoming packets to more than one LCF.
- The LGW listens for incoming TLS based service connections on TCP-port 3004 (see section 4.11).
- The LGW can buffer PDUs (see TS 102 232-1 clause 6.3.3).

I.1.4 LEMF-Collection Function (LCF)

The LCF is part of the actual LEMF. The LCF performs the following operations.

- The LCF only accepts incoming TLS tunnels from known LEMF-Gateways.
- The LCF listens for incoming TLS based service connections on TCP-port 3004 (see section 4.11).
- The LCF decrypts all PDU’s with the cryptographic key which was negotiated via the HI1 (see section 4.7).
- The LCF can buffer encrypted or decrypted PDUs.
- The LCF delivers the decrypted PDUs to the LEMF via TCP-port 3003 (see section 4.11).

I.1.5 LEMF

The LEMF performs the following operations:

- Accept incoming connections from the LCF via TCP-port 3003 (see section 4.11).

Annex J (informative): Document and Change Request History

Status of ETSI-IP.nl Implementing ETSI TS 102 232-series in the Netherlands		
Date	**Version**	**Remarks**
6 September 2011	1.0	First Publication within Platform 13