ETSI-IP.nl

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

Version 4.0; 22 November 2017

Agreed by PF13 Ad hoc Working group “Afhechten ETSI.nl Specificaties”;
22 November 2017

Approved by Platform 13 on 16 October 2017

This specification was produced by
Ad hoc Working group “Afhechten ETSI.nl Specificaties”
and is owned by
"Ministry of Justice and Security "
and available via the Depositary.

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.

Section F.3 lists and fills in the specific items related to the ETSI-LI standard ES 201 671, which describes a handover interface for the transport of lawful intercepted information between a network operator, access provider and/or service provider and a Law Enforcement Agency. In the Netherlands, this interface shall be used as the standard interface for the transport of circuit switched lawful interception information.

This document refers to a role called the Depositary. This role is performed by Agentschap Telecom, part of the ministry of Economic Affairs. Contact details are as follows.

Postal: Agentschap Telecom
PO Box 450
9700 AL Groningen
The Netherlands

Phone: +31 50 587 7444
Fax: +31 50 587 7400
E-mail: info@agentschaptelecom.nl

List of abbreviations

AAA	Authentication, Authorization and Accounting
AMS-IX	Amsterdam Internet Exchange
ASN.1	Abstract Syntax Notation One
CBC	Cipher Block Chaining
CC	Content of Communication
CCLID	CC Link Identifier
CID	Call Identifier
CIN	Communication Identity Number
CN	Common Name
CSP	Communication Service Provider
DSA	Digital Signature Algorithm
DCC	Delivery Country Code
DF	Delivery Function
EPS	Evolved Packet System
ES	ETSI Standard
ETSI	European Telecommunications Standards Institute
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
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part (of signalling system No.7)
ITU-T	International Telecommunication Union-Telecommunication
LCF	LEMF Collection Function
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LGW	LEMF Gateway
LI	Lawful Interception
LIID	Lawful Interception IDentifier
MF	Mediation Function

NEID	Network Element IDentifier
NID	Network Identifier
NL-ix	Netherlands Internet Exchange
PCM	Pulse code modulation
PDU	Protocol Data Unit
PKI-LI	Public Key Infrastructure for Lawful Interception
PS	Packet Switched
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SSD	Service-Specific Details
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRI	Transport Related Information
TS	Technical Specification
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
UUS	User-to-User Signalling
VLAN	Virtual Local Area Network
WGS84	World Geodetic System 1984

References

NOTE: The specific version numbers of the ETSI specifications are the versions valid at the time of adaptation of this 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 3.13.1 (2017-03).

[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 messaging services" version 3.10.1 (2016-08).

[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 3.5.1 (2017-03).

[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 3.3.1 (2017-03).

[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 3.7.1 (2017-03).

[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 3.3.1 (2014-03).

[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 3.4.1 (2017-03).

[8] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic" version 3.12.1 (2013-10).

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] Void.

[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".

[14] Void.

[15] Void.

[16] Void.

[17] Void.

[18] Void.

[19] Void.

[20] Void.

[21] Void.

[22] Void.

[23] Void.

[24] 3GPP TS 33.108: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception (LI)" release 12.

[25] ETSI ES 201 671 ed1: "Handover interface for the lawful interception of telecommunication traffic" version 1.1.1 (1999-07).

[26] Void.

[27] Void.

[28] IETF RFC 7245: "A Uniform Resource Name Namespace for the Global System for Mobile Communications Association (GSMA) and the International Mobile station Equipment Identity (IMEI)".

[29] PF13 AES: "Electronic Handover Interface Specification for Lawful Interception requests and Lawful Disclosure: e-sub-HI1" version 1.0 (18 October 2017).

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 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".

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

A description of the administrative interface HI1 can be found in e-sub-HI1 [29].

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 random decimal digits followed by an MD5 hash of a random value, two octets for use by the Communication Service Provider (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 random decimal digits (BCD encoded, 4 octets);
- MD5 hash of a random value (16 octets);
- for CSP use (default value 0xFF00 set by the LEA, 2 octets);
- reserved for future use (initial value 0xFF00FF, 3 octets).

Example: 91283721AA8B621A042A0673D7023B094EE54B34FF00FF00FF

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.

For session layer keep alives (as described in section 4.10) the LIID shall be set to "-" (0x2D).

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). Use of the NEID is mandatory in NL. Both ASN.1 structures (networkElementIdentifier and eTSI671NEID) are supported by the LEA and may be used, as long as the NEID is unique within the CSP domain. The operator identifier shall consist of 8 decimal characters describing an internationally unique network operator, access provider or service provider and is mandatory. In the Netherlands, it will consist of 031 plus five digits from the range as specified in e-sub-HI1 [29] section 2.4.1.1. The operator identifier is assigned by the Depositary at the request of the CSP.

The operator identifier is identical to the CSP identifier defined in e-sub-HI1 [29] section 2.4.1.1.

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

The use of the Communication Identity Number (CIN) extension field is supported.

The delivery country code (DCC) is identical to the country-code defined in e-sub-HI1 [29] section 2.4.1.3.

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. The PS header field shall always contain a MicroSecondTimeStamp.

NOTE: A MicroSecondTimeStamp qualified as timeOfAggregation may show a substantial deviation from timeOfInterception or timeOfMediation qualified timestamps in the individual CC payloads.

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 Intercept Related Information (IRI) type is mandatory.

3.7 Interception Point Identifier (TS 102 232-1 clause 5.2.11)

If the Interception Point ID is used, the combination of the NEID as specified in section 3.3 and the Interception Point ID must be unique within the CSP domain. It is not required to assign an Interception Point ID to each interception point in the network.

4 Data exchange

Reference: TS 102 232-1 clause 6

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

See section I.1 for further information on the creation of DFs.

The possible techniques for Protocol Data Unit (PDU) distribution number 5) will be used: select randomly a Delivery Function (DF) across all available DFs for the delivery of all PDUs with the same LIID and CID, also after failure of the connection the selection randomly moves to a other available DF.

The logical communication path on the handover layer is one way, DF to LGW.

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

Error reporting from the Mediation Function (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 handover manager shall perform encrypted handover using the encryptedPayload ASN.1 structure. Encryption Type shall be AES-192-CBC (Cipher Block Chaining). Encryption shall be used for all Payload Types on the handover layer. An unencrypted Payload shall always be nested within an encrypted Payload.

The use of the encryptedPayloadType is mandatory in NL. The value "unknown(1)" is only used in exceptional situations.

For information table 4.1 gives guidance on the mapping between the ASN.1 structure used and the required value of the encryptedPayloadType structure. The table has not the intention to be complete. The use of this table is only applicable when the ASN.1 is described in TS 102 232-1 [1] (or an import in TS 102 232-1) instead of the SDSs itself.

Table 4.1: Mapping ASN.1 structure part 1 and value encrypted payload type

Part	Structure in TS 102 232-1 [1]	Value of encryptedPayloadType
1	TRI	part1
2	emailCC	part2
2	emailIRI	part2
2	messagingCC	part2
2	messagingMMCC	part2
2	messagingIRI	part2
3	iPCC	part3
3	iPIRI	part3
3	iPIRIOnly	part3
4	N/A	part4
5	iPMMCC	part5
5	iPMMIRI	part5
6	pstnIsdnIRI	part6
6	eTSI671IRI	part6
7	uMTSCC	part7
7	uMTSCC-CC-PDU	part7
7	uMTSIRI	part7
7	ePSCC	part7
7	ePSCC-CC-PDU	part7
7	ePSIRI	part7

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” shall be used. The values as defined in TS 102 232-1 clause 6.3.4 [1] shall be configured as:

<TIME1>: 60 seconds

<TIME2>: 15 seconds

<TIME3>: 30 seconds

The LIID shall be set as described in section 3.1. The requirements in sections 3.2, 3.3 and 3.4 shall be applied. A CIN value shall not be set.

4.11 Option negotiation (TS 102 232-1 clause 6.3.5)

The option negotiation shall not be used.

4.12 PDU acknowledgement (TS 102 232-1 clause 6.3.6)

The PDU acknowledgement shall not be used.

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

The port number for Transport Layer Security (TLS) is 3004.

4.14 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).

Closing a transport connection is supported based on the "keep-alive" condition. The value of the time-out period shall be configured as:

<M>: 15 minutes.

4.15 Time synchronisation

Delivery Functions (DF) and Handover Managers (HM) may run on multiple servers and at geographic different locations. Therefore all DFs and HMs within the same HM/DF domain of a CSP should maintain an accurate common system clock time. An accuracy tolerance of less than 10 millisecond is advised.

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 Virtual Local Area Networks (VLAN) at the Amsterdam Internet Exchange (AMS-IX) or the Netherlands Internet Exchange (NL-ix). The transport layer will use an IP connection with "like private peering" via the AMS-IX or NL-ix.

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_GCM_SHA384 with a fallback defined by TLS_RSA_WITH_AES_256_CBC_SHA RFC 5246 [13]. The fallback cipher is for cipher migration only and will be removed in a future version of this document.

A presented certificate shall only be trusted if it is signed by the PKI-LI CA (Certificate Authority) and the IP address in the common name (CN) field is equal to the IP address of the other party. An untrusted certificate shall result in a disconnect.

5.4 Integrity (TS 102 232-1 clause 7.2.3 and annex J)

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

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

<hashTimeout>:	1 (one) second
<dataPduCount> number of sent data PDUs:	1000
<signTimeout>:	300 seconds
<hashPduCount> number of sent hash based IC PDUs:	15

The hash based message digest shall be according SHA-256.

The signature based message digest shall be based on SHA-256 and a DSA (private) key with parameter pair (L,N) with the respective sizes (3072,256).

The HashAlgorithm field shall be used and set to 2 (SHA-256).

The Depositary is responsible for the retrieval, storage and verification of the authenticity of the Digital Signature Algorithm (DSA) public key of every CSP. The Depositary shall determine the procedure by which CSPs submit their DSA public keys, and provide a description thereof to each CSP.

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:

Void.

Annex B (normative): Requirements for messaging 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 IRI events

Reference: TS 102 232-3 clause 6.1

The use of the IRI Event in Table 1 “End of Interception with Session Active” shall be supported. It is up to the MF to decide whether or not to send the IRI-REPORT.

C.2 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 Authentication, Authorization and Accounting (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.

The use of the IRI Event in Table 1 “End of Interception with Session Active” shall be supported. It is up to the MF to decide whether or not to send the IRI-REPORT.

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-CONTINUE-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 Real Time Protocol (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 User Datagram Protocol (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).

E.6 Location Information

Reference TS 102 232-5 clause 5.2.3

If Location Information is available the common Location parameter as imported from TS 102 232-1 [1] shall be used. If the location of the User Equipment is available, the geodetic location information from the User Equipment shall be included. If the location of the User Equipment is not available, the location of the antenna of the serving cell shall be provided if available. The mapdatum shall be set to WGS84.

E.7 Direction for IMS IRI for Signaling Messages

Reference TS 102 232-5 clause 5.6

The payloadDirection field shall not be used.

E.8 Direction for SIP sessions

Reference TS 102 232-5 clause 5.7.1

The sessionDirection field shall not be used.

E.9 Use of additional signalling information

Reference TS 102 232-5 clause 5.2.5

The ASN.1 sipHeaderLine parameter can be used to hand over the target's IMEI as additional information. When used, the sipHeaderLine parameter shall have the following format as defined in RFC 7245 [28]:

```
Contact: <sip:target@ims>;+sip.instance="<urn:gsma:imei:49015420-323751-8>"
```

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

Applicable to Circuit Switched Public Switched Telephone Network (PSTN) services such as POTS, Integrated Services Digital Network (ISDN) and mobile 2G/3G telephony.

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].

NOTE 1: If the frameType audioFrame is used each CC payload preferably contains one or more multiples of 160 octets.

NOTE 2: When an artificial RTP header is used, the frame size is preferably limited to 1400 octets.

F.2 Sending supplementary information

Reference: TS 102 232-6 clause 6.3.3

When the codec is not G.711 [10] the supplementary information shall at least 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

This section only relates to the clauses of TS 101 671 [8] concerning 64 kbit/s based services like PSTN, ISDN and GSM.

This section should be read aside TS 101 671 [8] and-will clarify the Dutch implementation of TS 101 671 [8].

ETSI/TC-LI continues to enhance TS 101 671. All modifications are collected in the latest version of TS 101 671.

F.3.1 HI2 Specification

Reference: TS 101 671 [8] clauses 5.2, 8.1, A.3.1, C.1

Handover interface HI2 shall transport the Intercept Related Information (IRI). For this interface TS 102 232 6 [6], shall be used.

F.3.1.1 IRI continue records

Reference: TS 101 671 [8] clause A.3.1

When relevant information is available, an IRI continue record shall be sent.

Examples: any change in location information of intercepted mobile subscribers. In the fixed network it could be User-to-User Signalling (UUS) messages.

F.3.2 HI3 Specification

F.3.2.1 Mono/Stereo mode

Reference: TS 101 671 [8] clause A.4.1

In order to obtain optimal interpretation of the HI3 signal two channels (stereo mode) shall be used. In exceptional cases (strong technical reasons) it may be possible to deliver only the mono signal. The LEMF shall implement both options.

F.3.3 Specific identifiers for LI

F.3.3.1 Lawful Interception Identifier (LIID)

Reference: TS 101 671 [8] clause 6.1

This LIID is for internal use at the CSP only and may be ignored by the LEA.

F.3.3.2 Call Identifier (CID)

Reference: TS 101 671 [8] clause 6.2

This CID is for internal use at the CSP only and may be ignored by the LEA.

F.3.3.2.1 Network Identifier (NID)

Reference: TS 101 671 [8] clause 6.2.1

This NID is for internal use at the CSP only and may be ignored by the LEA.

F.3.3.2.2 Call Identity Number (CIN)

Reference: TS 101 671 [8] clause 6.2.2

This CIN is for internal use at the CSP only and may be ignored by the LEA.

F.3.3.3 CC Link Identifier (CCLID)

Reference: TS 101 671 [8] clauses A.1.1, A.5.4

This CCLID is for internal use at the CSP only and may be ignored by the LEA.

F.3.4 ASN.1 version 1 versus higher versions

There are some differences between the elements/parameter in ASN.1 v1 and higher versions.

Although the implementation of ES 201 671 in the Netherlands originally referred to version 1.1.1 [25] of that specification, new implementations shall follow newer versions of ASN.1 considering releases of ES 201 671 and TS 101 671. Legacy (Circuit Switched) systems that were implemented in the Netherlands before 2013 using implementations based on earlier versions of ES 201 671 or TS 101 671 will be supported by the LEMF. The LEMF shall be able to accept the ASN.1 version that is sent by the mediator.

In ASN.1 version 1 the ISDN User Part (ISUP) parameter is mandatory and in ASN.1 version 2 the parameters is optional. In this case in version 1 the mandatory field will be filled with zeros in case no ISUP parameter is available. An empty field will cause an ASN.1 syntax error.

NOTE 1: For the support of the HI1 NL parameters ASN.1 version 3 for the module "HI1NotificationOperations" is minimally needed.

NOTE 2: For the support of the HI2 NL parameters ASN.1 version 5 for the module "HI2Operations" is minimally needed.

F.4 Location Information

If Location Information is available then, as a minimum, geodetic location information from the Mobile Station shall be included. If the location of the Mobile Station is not available, the location of the antenna of the serving cell shall be provided. The geodetic coordinates are coded as GSMLocation, geoCoordinates according TS 101 671 [8]. The mapdatum shall be set to WGS84.

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

TS 102 232-7 [7] shall only be used for Packet Switched UMTS and EPS IRI and CC.

The handover of lawfully-intercepted information as defined in ANSI/J-STD-025-B is not allowed.

NOTE: The details of the reference to ANSI/J-STD-025-B can be found in TS 102 232 part 7 [7] in the reference list as reference [4].

G.1 Location Information

If Location Information is available then, as a minimum, geodetic location information from the Mobile Station shall be included. If the location of the Mobile Station is not available, the location of the antenna of the serving cell shall be provided. The geodetic coordinates are coded as GSMLocation, geoCoordinates according 3GPP TS 33.108 [24]. The mapdatum shall be set to WGS84.

G.2 CC format

Reference TS 102 232-7 clauses 6.3 and 10.3

In case the UMTS LI Correlation (uLIC) header is available the CC shall be sent using the ePSCC-CC-PDU or the uMTSCC-CC-PDU structure.

In case the uLIC-header is not available the CC is sent using the ePSCC or the uMTSCC structure.

G.3 IRI format

Reference TS 102 232-7 clauses 6.2 and 10.2

Use of the logicalFunctionInformation field according S3i150063_CR107 and S3i150064_CR108 as accepted by 3GPP TSG-SA3LI Meeting #56 (Sophia Antipolis, 20-22 January 2015) is allowed.

NOTE: The present section enables the use of this field, prior to the formal adaption of the involved 3GPP TS 33.108 [24] version in TS 102 232-7 [7]. This section can be removed after acceptation of the logicalFunctionInformation field by TC LI in TS 102 232-7 [7].

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 this 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: or ETSI-IP.nl	N /I	Normative referenced documents in TS 102 232 parts and in ETSI-IP.nl	version d.d. 19-10-2014
2	N	3GPP TS 23.003 (ETSI TS 123 003): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification".	12.4.0 (2014-10) 11.9.0 (2014-10) 10.10.0 (2014-10) 9.15.0 (2014-10) 8.21.0 (2014-10)
4		3GPP TS 23.060 (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)".	12.6.0 (2014-09) 11.11.0 (2014-09) 10.140 (2014-09) 9.14.0 (2013-04) 8.17.0 (2013-04) 7.11.0 (2011-06) 6.15.0 (2006-12)
2	N	3GPP TS 24.229 (ETSI TS 124 229): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".	12.5.0 (2014-07) 11.12.0 (2014-07) 10.16.0 (2014-07) 9.20.0 (2014-07) 8.28.0 (2014-07)
2	N	3GPP TS 29.002 (ETSI TS 129 002): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Mobile Application Part (MAP) specification".	12.6.0 (2014-10) 11.10.0 (2014-07) 10.10.0 (2013-09) 9.12.0 (2013-09) 8.21.0 (2013-09)
1,2,5,7 Annex G	N	3GPP TS 33.108 (ETSI TS 133 108): "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 Release 9)". 3GPP TS 33.108 (ETSI TS 133 108): "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 Release 12)".	12.6.0 (2014-10) 11.5.0 (2014-10) 10.5.0 (2012-10) 9.7.0 (2012-10) 8.14.0 (2012-10) 7.10.0 (2011-02) 6.10.0 (2005-01
2	N	ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface".	1: 4.2.1 (2001-07) 2: 4.2.1 (2001-07) 3: 4.2.1 (2001-07) 4: 4.2.1 (2001-07) 5: 4.1.2 (2001-07) 6: 4.1.2 (2001-07) 7: 4.1.2 (2001-07) 8: 4.1.2 (2001-07) 9: 4.1.2 (2001-07) 10: 4.1.2 (2001-07) 11: 4.1.2 (2001-07) 12: 4.2.1 (2001-07) 14: 4.2.1 (2001-07) 15: 4.2.1 (2001-07) 16: 4.1.2 (2001-07) 17: 4.1.2 (2001-07) 18: 4.1.2 (2001-07) 19: 4.2.1 (2001-07) 20: 4.3.1 (2001-07) 21: 4.2.1 (2001-07) 22: 1.1.1 (2003-07) 33: 4.1.1 (2003-07)
Annex F	N	ETSI ES 101 671 ed1: "Handover interface for the lawful interception of telecommunications traffic".	1.1.1 (1999-07)

TS 102 232 part: or ETSI-IP.nl	N /I	Normative referenced documents in TS 102 232 parts and in ETSI-IP.nl	version d.d. 19-10-2014
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)
2	N	ETSI TS 100 974: "Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) Specification (3GPP TS 09.02)".	7.15.0 (2004-03 6.14.0 (2003-09) 5.19.0 (2003-09)
1,2,4,5	I	ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".	1.4.1 (2014-02)
1,2,3,4,5, 6,7	N	ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".	3.12.1 (2013-10)
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".	3.7.1 (2014-07)
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 Messaging Services".	3.7.1 (2014-07)
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".	3.3.1 (2013-10)
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".	3.2.2 (2014-07)
1,2	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".	3.3.1 (2014-06
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".	3.3.1 (2014-03)
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".	3.2.1 (2013-07)
6	I	ETSI TS 187 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Lawful Interception; Lawful interception; Stage 1 and Stage 2 definition".	3.1.1 (2012-06) 2.1.1 (2009-09)
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		FIPS PUB 186-4: "Digital Signature Standard (DSS)".	19 July 2013
1,2	N	IETF RFC 0791: "Internet Protocol".	September 1981
1		IETF RFC 0792: "Internet Control Message Protocol".	September 1981
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
2		IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".	November 1996
2		IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".	November 1996
3		IETF RFC 2131: "Dynamic Host Configuration Protocol".	March 1997
3	N	IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".	March 1997

TS 102 232 part: or ETSI-IP.nl	N /I	Normative referenced documents in TS 102 232 parts and in ETSI-IP.nl	version d.d. 19-10-2014
4		IETF RFC 2341: "Cisco Layer Two Forwarding (Protocol) L2F". [status: historic]	May 1998
4	N	IETF RFC 2427: "Multiprotocol Interconnect over Frame Relay".	September 1998
1,2	N	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
2	N	IETF RFC 2806: "URLs for Telephone Calls" [Obsoleted by RFC 3966]	April 2000 [December 2004]
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
2	N	IETF RFC 3066: "Tags for the Identification of Languages". [Obsoleted by RFC 4646] [Obsoleted by RFC 5646]	January 2001 [September 2006] [September 2009]
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
2,5	N	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
2		IETF RFC 3696: "Application Techniques for Checking and Transformation of Names".	February 2004
2,3		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	N	IETF RFC 5321: "Simple Mail Transfer Protocol".	October 2008
1,2	N	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
2	N	IETF RFC 6335: "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry".	August 2011
1,2,3	N	ISO 3166-1:2013: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".	2013
3		IEEE 802.11 (ISO/IEC 8802-11): "IEEE Standards for Information Technology - Telecommunications and Information Exchange between systems Local and metropolitan area network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".	2012
1		ISO/IEC TR 10000-1: "Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: General principles and documentation framework".	October 1998

TS 102 232 part: or ETSI-IP.nl	**N /I**	**Normative referenced documents in TS 102 232 parts and in ETSI-IP.nl**	**version d.d. 19-10-2014**
2,4	N	ITU-T Recommendation E.164: "The international public telecommunication numbering plan".	November 2010 + amendments
2		ITU-T Recommendation E.212: "The international identification plan for public networks and subscriptions".	May 2008 + amendments
6	N	ITU-T Recommendation G.711 (1988): "Pulse code modulation (PCM) of voice frequencies".	November 1988 + amendments
5		ITU-T Recommendation H.225.0: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".	December 2009 + amendment
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	June 2000 + amendments
5		ITU-T Recommendation H.323: "Packet-based multimedia communications systems".	December 2009 + amendment
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
5,6		ITU-T Recommendation T.38: "Procedures for real-time Group 3 facsimile communication over IP networks".	November 2010
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 intermediate destinations: the so called LEMF-Gateways (LGW). In order to do so, the Handover Manager creates at least one Delivery Function (DF) for each specified LEMF-Gateway (see TS 102 232-1 [1] clause 6.3). For functional reasons or reasons of availability, multiple DFs associated with the same LGW may be created, e.g. per interception. The HM shall not create more than eight DFs per LGW, unless mutually agreed.

The HM may close the last DF associated with an LGW in case there are no applicable warrants that require delivery to that 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.

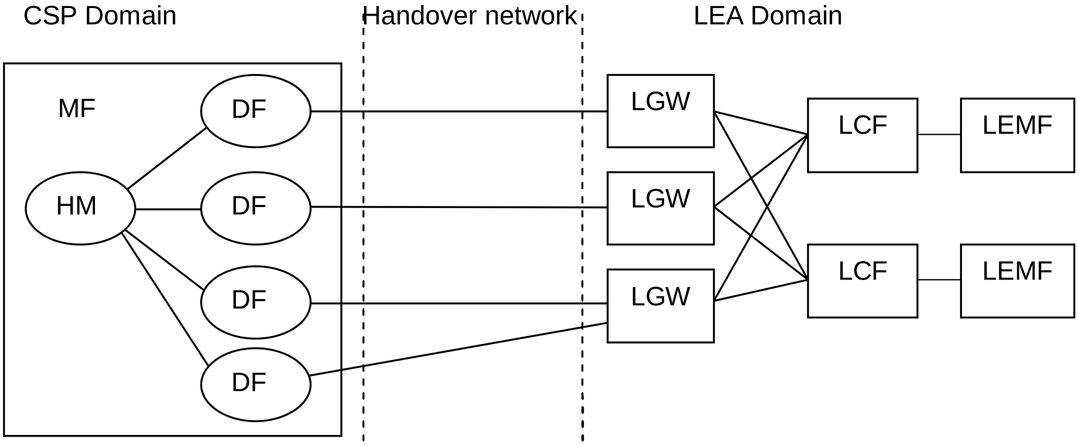

Figure I.1: The Dutch concept of the LEMF Gateway at the LEA side

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 one LGW defined in the legal authorisation. The keys are negotiated via the HI1. If an LGW cannot be reached the DF tries to re-connect (see sections 4.8 and 5.2).
- The TLS tunnel only accepts 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 the LGW using TCP-port 3004 (see section 4.13).

I.1.3 LEMF Gateway (LGW)

The LEMF Gateway performs the following operations:

- The LGW accepts incoming TLS tunnels from every known MF functional unit. Known means that both the IP address (range) and public key of the MF 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 MF 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 4.13).
- 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 4.13).
- The LCF decrypts all PDUs 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 4.13).

I.1.5 LEMF

The LEMF performs the following operations:

- Accept incoming connections from the LCF via TCP-port 3003 (see section 4.13).

Annex J (informative): Integrity and authenticity needs for data PDU delivery

This annex informs on the Dutch needs for integrity and authenticity. These needs can be used as reference point if changes to the integrity and authenticity implementations in ETSI TS 102 232-1 [1] are made.

The following integrity and authenticity needs for data PDU delivery apply:

- The integrity and authenticity of the complete data PDU that is handed over has to be guaranteed.
- The LEA has to be able to assure that the received data originated from the sending CSP.
- The LEA has to be able, without additional cooperation of the CSP, to assure that all data sent by the CSP is received by the LEA unaltered, even if there is no intercepted data to be delivered by the CSP.

Annex K (informative): Document and Change Request History

Status of ETSI-IP.nl Implementing ETSI TS 102 232-series in the Netherlands		
Publication Date	**Version**	**Remarks**
6 September 2011	1.0	First Publication within Platform 13 V1.0 approved by Platform13 at their meeting of 6 September 2011
4 September 2012	2.0	Inclusion of Annex A: "Electronic HI1 Interface (e-sub-HI1) Specification" with complete e-sub-HI1 XSD schema definition Update of version indication of referenced documents Alignment with edition 3 of the TS 102 232 series: - 4.1 Handover layer, general - 4.6 Payload encryption V2.0 approved by Platform13 at their meeting of 4 September 2012
3 December 2013	3.0	Approved Change Requests to version 2.0 by AES meetings starting from AES#25 (25 October 2012) until AES#38 (27 November 2013): CR002r1 on 2G/3G Circuit Switched services CR003r9 on ETSI-NL inclusion CR004r2 on Excluding the use of CALEA standards in the Netherlands CR005r1 on Update to refer to the latest version of TS 102 232-2 (and required imported 232 parts) and TS 101 671 CR009r1 on Clarification on the use of OpenPGP certificates CR012r1 on Clarify how to implement the NEID in NLCR013r3 on Timestamps within CC packets CR013r6 on Timestamps within CC packets CR014r2 on Location information shall always contain geographical informationCR015r1 on Limiting the artificial RTP frame size CR015r1 on Limiting the artificial RTP frame size CR016r5 on EncryptedPayloadType identifier value CR017r1 on Updated references to align with ETSI TS 102 232 updates CR018r1 on Support of VAS MMS in HI1 CR019r1 on Definition of Depositary, and CSP and operator identifier CR020r3 on e-sub-HI1-lite CR021r2 on Updating the scope of the Interception Point ID CR023r1 on Distribution and validation of DSA public key CR024r1 on Updated references to align with TS 102 232 updates from TC LI#33 CR025r3 on Addition of another form of the caseRefenceNumber CR026r1 on Size of keys for signing message digests CR027r1 on Include UMTS and EPS ULIC-header to avoid loss of information CR028r5 on InterceptServiceType message element hierarchical structure is not logical CR029r2 on Handling of RTP without headers in part 6 CR030r1 on Option negotiation cancelation CR031r1 on PDU acknowledgement is not used CR032r1 on New definition for version number in Annex A messages CR033r1 on Clarification of the procedure for submission of public DSA keys CR034r1 on Change to IRI-REPORT to signal end of intercept whilst session remains active (part 3) CR035r1 on Change to IRI-REPORT to signal end of intercept whilst session remains active (part 4) CR036r1 on EncryptedPayloadType identifier value CR037r1 on Annex A: E-sub-HI1 "filename" CR038r2 on Annex A: E-sub-HI1 "LIID" CR039r1 on Annex A: E-sub-HI1 "valueaddedservice" CR040r1 on Annex A: E-sub-HI1 "IMEI" CR042r1 on Annex A: E-sub-HI1 "IPv4 CIDR" CR043r1 on Annex A: E-sub-HI1 "telephone number" CR044r1 on Adding Time synchronisation CR045r1 on Updating Annex H CR046r1 on Align supplementary info with recent ETSI CR to part 6 CR047r1 on Statement on stand-alone XSD file and version indication V3.0 approved by Platform13 at their meeting of 3 December 2013

31 December 2014	3.1	Included approved Change Requests to version 3.0 by AES meetings starting from AES#39 (22 January 2014) until AES#45 (17 September 2014): CR048r1 on Addition of caseReferenceNumber CR049r3 on Enabling session layer keep-alives CR050r1 on Import the new ETSI TS 102 232 versions after TC LI#35 CR052r1 on Clarification of the existence of working draft versions of the XSD CR053r1 on Validate the CN of the LGW CR054r1 on PUT certificate message CR055r1 on Cipher to be used for message encryption in e-sub-HI1 CR056r1 on Correction in text section A.3.4.3 CR057r1 on Update for Location in TS 102 232-5 and Update references CR058r1 on Integrity and authenticity requirements CR059r1 on Updating of Annex H (status 19 October 2014) Upgrading XSD working version v3.0.1 to version 3.1 V3.1 approved by Platform13 in December 2014
22 November 2017	4.0	Included approved Change Requests to version 3.1 by AES meetings starting from AES#46 (19 November 2014) until AES#76 (22 November 2017): CR060r2 on Updated encryption algorithm on the Delivery Network CR061r1 on Adaption for logicalFunctionInformation field in 3GPP TS 33.108 CR062r1 on Incorrect HTTP response code for PUT requests CR063r1 on Improved XSD versioning scheme CR064r3 on Additional HI1 request parameters CR065r1 on Clarification of the DF-LGW connectivity (formally CR051r1) CR067r1 on Clarification of the messageIdentifier usage CR068r1 on Definition of the imei TargetIdentifier type CR069r1 on Adjust Transport layer section CR070r1 on Define default T_{poll} interval CR071r1 on Restriction on usage of interceptServiceType construct CR072r4 on Implementation of integrity measurement according to new specifications in TS 102 232-1 clause 7.2.3 CR074r1 on Adding “delivery country codes” for Dutch overseas countries and territories (OCTs) CR075r1 on valueAddedServiceType CR076r1 on Message Priority CR077r1 on Delegated CSP CR078r1 on HI1 Lite extension Required Correction in XSD: `<xs:simpleType name="priorityIndicator">` CR079r1 on Introduction of additional “primaryServiceType” CR083r2 on Inconsistencies in Annex A CR084r1 on Updated ETSI TS 102 232 references CR085r1 on Improve LIID description CR086r1 on Closing transport connections in a controlled and error-free manner CR087r2 on Correction of table names in annex A CR088r1 on Updated ETSI TS 102 232 references CR089r1 on Reserve an identifier for the Message Broker (in annex A) CR090r1 on Making annex A void Annex is transferred in total to e-sub-HI1 v1.0. V4.0 approved by Platform13 in October 2017