Implementing ETSI ES 201 671 in the Netherlands

Version 1.1; 21 September 2011

Agreed by "Working group ETSI-LI standard in the Netherlands"

This specification was produced by
"Ad hoc Working group standard"
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 ES 201 671 version 1.1.1. This standard 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 (LEA). In the Netherlands, this interface shall be used as the standard interface for the transport of circuit switched lawful intercepted information.

Reference: ETSI ES 201 671: Handover interface for the lawful interception of telecommunication traffic; version 1.1.1 (1999-07)

List of abbreviations

AP	Access Provider
CC	Content of Communication
CCLID	CC Link Identifier
CdP Sub	Called Party Subaddress
CgP Sub	Calling Party Subaddress
CHAL	challenge (authentication parameter)
CID	Call Identifier
CIN	Call Identity Number
CIPH	cipher text (authentication parameter)
CLIP	Calling Line Identification Presentation
COLP	Connected Line Identification Presentation
CoP Sub	Connected Party Subaddress
CUG	Closed User Group
DES	Digital Encryption Standard
EN	European Norm
ES	ETSI Standard
ETSI	European Telecommunications Standards Institute
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HI	Handover Interface
HV	Handle Value (authentication parameter)
IIF	Internal Intercepting Function
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part (of signalling system No.7)
K1	Mediation Key
K2	Law Enforcement Key
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identifier
MF	Mediation Function
NEID	Network Element Identifier
NID	Network Identifier
NWO	Network Operator
PSTN	Public Switched Telephone Network
ROSE	Remote Operation Service Element
RSA	Rivest Shamir Adlemann (authentication mechanism)
SEQ	sequence number (authentication parameter)
SHA	Secure Hashing Algorithm
SMS	Short Message Service
SvP	Service Provider

TC LI	ETSI Technical Committee Lawful Interception
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TTP	Trusted Third Party
UUS	User-to-User Signalling

List of references

ES 201 671 ed1	"Handover interface for the lawful interception of telecommunication traffic; version 1.1.1 (1999-07)"
ETSI-NL	"Implementing ETSI ES 201 671 in the Netherlands; Version 1.0; 6 February 2001"
ES 201 671 ed2	"Handover interface for the lawful interception of telecommunication traffic; version 2.1.1 (2001-09)
TR 102 053	"Notes on ISDN lawful interception functionality; v1.1.1 (2002-03)"
TS 101 671	"Handover interface for the lawful interception of telecommunication traffic; version 2.9.1 (2004-05)"
ISO 3166-1	"Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".

1 Scope of this document

This document only relates to the sections of ES 201 671 v3.1.1 concerning 64 kbit/s based services like PSTN, ISDN and GSM.

This document should be read aside ES 201 671 v3.1.1. The sections of this document will clarify the Dutch implementation of ES 201 671 v3.1.1. Section 12 "Use of subaddress to carry correlation information" is based on enhancements made by ETSI TC-LI on the optional use of subaddressing in HI3.

In ETSI TC-LI continues to enhance ES 201 671. All modifications are collected in the latest version of TS 101 671.

2 General requirements

Reference: ES 201 671 section 4.3

It shall be possible to implement up to three simultaneous delivery addresses for one target. In practice these three addresses can be part of one, two or three simultaneous lawful authorizations.

Remark: Different lawful authorizations can ask for different interception functionalities. This can also apply if the same target is part of different lawful authorizations.

3 HI1 specification

Reference: ES 201 671 sections 4.3, 5.1, 7.2, A.4.4.2

HI1 is the administrative interface. Detailed specification of the HI1 interface does not belong to the scope of this document. However, references to the functionality of this interface will be made.

The lawful authorization shall be sent via HI1 to the administration centre of the NWO/AP/SvP. The LEA shall provide the following information:

- Telephone number, IMSI or IMEI number of the interception subject;
- Lawful Interception Identifier (LIID);
- Start and end time of the interception;
- Kind of information to be provided (IRI, CC or both) (note 1);
- Datanet 1, X.25 address of the LEMF, to which the IRI-Records shall be sent;
- ISDN number of the LEMF, to which the Content of Communication (CC) shall be sent (note 2);
- Secret key K1 and K2 for the authentication of HI3 (note 2, note 3);
- A reference for authorization of the interception;
- Technical contact for issues relating to set-up and execution of the interception.

NOTE 1: Juridically there is no reason to exclude the option "CC only". However, in the Dutch situation it is agreed with the authorities that this option will not be requested by the LEAs. Therefore there is no need to implement this option.

NOTE 2: These are only applicable if the CC is requested.

NOTE 3: These authentication keys will be exchanged in an electronic way, see section 11.1.

Normally, the NWO/AP/SvP shall send confirmation of the acceptance, implementation and expiration of the lawful authorisation. In exceptional cases messages could be sent for example to indicate that the target service is out of order or the interception facility is out of order. For Informational messages see section 11.2.

Beside information related to an intercept also unrelated information could be sent from the NWO/AP/SvP. Examples are the network, service or intercept facility is (temporarily) not available or is available again. For alarm messages see section 11.2.

4 HI2 Specification

Reference: ES 201 671 sections 5.2, 8.1, A.3.1, C.1

Handover interface HI2 shall transport the Intercept Related Information (IRI). For this interface the public X.25 data network, Datanet 1, shall be used.

Other X.25 data networks that are generally available could be used. In this case there need to be an interconnection between this data network and Datanet 1, to prevent the necessity of more interfaces to the LEMFs.

For the application layer ROSE shall be used while for the layers 1 to 3 TCP/IP on top of X.25 shall be used.

4.1 IRI continue records

Reference: ES 201 671 section 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 UUS messages.

4.2 Structure HI2 delivery IP address

The IRI data is delivered via the HI2 interface. The IP address of the entities will have the following structure:

A,B,C,D

- A = 010;
- B represents the operator or the LEMF;
- C = 001 – 253 (MF / LEMF code);
- D = 001 – 253 (MF / LEMF code).

The list of operator and LEMF codes (for B) will be maintained by the Agency Telecom .

The HI2 delivery port at the LEMF is 1250.

4.3 Specific X.25 network parameters

Related to section 4 (ETSI-NL)

According rough calculations on the network entities about 100 MFs, 48 LEMFs en 10 management systems might be installed for the ETSI-NL interception system. A typical value for the number of logical channels for the LEMF is 128 channels and for the Mediator 40 channels.

As guideline for the configuration of the X.25 links between the Mediators and the LEMFs to following values are of interest for local settings and for the Datanet 1 connection.

Table 2: Physical Layer Parameters Network interface MF and LEMF

Parameter	Value
Interface	X.21
Signalling	X.21
Clock	Internal
DCE/DTE	DCE
Baud Rate	64kbit/s / 9600bit/s

Table 3: LAPB Parameters

Parameter	Router/ Terminal equipment value
Interface outage	0 (default, disable this function)
Modulo	8 (default)
T1	1 second
T4	0 (default, t4 disabled)
K	7
N1	In case of Cisco router and EICON card this value is calculated automatically
N2	20

Table 4: X.25 Parameters MF and LEMF

Parameter	Router value
X.25 mode	DTE
Packet size	128
Window size in/out	2
Highest Two way Circuit	128
Lowest Two way Circuit	1
Lowest/Highest Outgoing Circuit	0 (disabled)
Lowest/Highest Incoming Circuit	0 (disabled)
PVCs	None
Accept reverse charge	Disabled
CUG	To be added
Hold queue	10 (default)
Hold-VC-timer	0 (default)
Idle	2 (recommended 90s; but in case of Cisco resolution is determined in minutes)
Protocol	IP
Modulo	8 (default)
NVC	1
T20	180s (default)
T21	200s (default)
T22	180s (default)
T23	180s (default)

4.4 CUG (X.25 Datanet 1)

For security purposes, one Preferential CUG will be defined in the Datanet 1 profile.

The Agency Telecom is coordinating the request for access to the Preferential CUG.

4.5 Datanet 1 connection

Related to section 4 (ETSI-NL)

For the Datanet 1 connection, a dedicated profile for the ETSI-NL Lawful Interception system is defined. The settings of the X.25 parameters are according the tables given in section 4.3 Specific X.25 network parameters.

A unified request procedure is available to get connected on the Datanet 1. Forms are available at the depositary (Agency Telecom).

5 HI3 Specification

Reference: ES 201 671 sections A.4, A.4.2

Handover interface HI3 shall transport the Content of Communication (CC). For the delivery of the circuit switched Content of Communication, a public circuit switched ISDN network shall be used. For the delivery of non-circuit switched Content of Communication, e.g. UUS and SMS, HI3 shall use the same physical delivery mechanism as used for HI2 information.

5.1 Mono/Stereo mode

Reference: ES 201 671 section 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.

For transport of the indication of mono/stereo mode in the HI3 message, the "direction" field in the Calling Party Subaddress shall be used (see table 8).

6 Specific identifiers for LI

6.1 Lawful Interception Identifier (LIID)

Reference: ES 201 671 section 6.1

For each interception measure an identifier is defined by the Lawful Enforcement Agency (LEA), the Lawful Interception Identifier (LIID). For this LEA the LIID value is unique.

In the case that one lawful authorisation specifies more than one (maximum is 3, see section 2) delivery address, the same number of LIIDs has to be defined. The values of these LIIDs have to be safeguarded with the LEAs where the delivery has to be provided. This guarantees that for the NWO/AP/SvP the combination of the LIID and HI2/3 delivery address is always unique.

The LIID shall consist of 5 decimal characters. This in not in line with ES 201 671 v3.1.1 where 25 alphanumeric characters (octets) are reserved for the LIID. However, later drafts of the ETSI Standard define a maximum length of 25 decimals (half octets). For transport of the LIID in the HI3 message, the Calling Party Subaddress shall be used. The five LIID decimals shall be mapped to octets 4, 5 and 6 together with a field separator (see table 8).

6.2 Call Identifier (CID)

Reference: ES 201 671 section 6.2

For each call or other activity relating to a target identity, a Call Identifier (CID) is generated by the relevant network element. The CID consists of the following two identifiers:

- Network Identifier (NID);
- Call Identity Number (CIN).

6.2.1 Network Identifier (NID)

Reference: ES 201 671 section 6.2.1

The Network Identifier is an international unique parameter describing an operator and a specific Mediation Function (MF). It consists of the following two identifiers:

1. Operator identifier. This parameter shall consist of 5 decimal characters describing internationally unique a network operator, access provider or service provider. In the Netherlands, it will consist of 31 plus three digits. This list will be maintained and made available by the Directorate General for Telecommunication and Post of the Ministry of Transport of Public works. For transport of the operator-id. in the HI3 message, the Called Party Subaddress shall be used. The operator-id. shall be mapped to octets 4, 5 and 6 together with a field separator (see table 6).
2. Network Element Identifier (NEID). The purpose of the NEID is to uniquely identify the relevant mediator function, which is carrying out the LI operation. The NEID is the Calling Party number, which is available via the ISDN supplementary service CLIP.

6.2.2 Call Identity Number (CIN)

Reference: ES 201 671 section 6.2.2

The Call Identity Number (CIN) is a temporary identifier of an intercepted call, related to a specific target identity, to identify uniquely an intercepted call.

For transport of the CIN in the HI3 message, the Called Party Subaddress shall be used. The call identity number is 8 decimal digits long and shall be mapped to octets 7, 8, 9 and 10 (see table 6).

6.3 CC Link Identifier (CCLID)

Reference: ES 201 671 sections A.1.1, A.5.4

The CC Link Identifier (CCLID) will only be used at the interface ports HI2 and HI3 in case of reuse of CC links (option B).

Juridically from the LEA side the need to know accurately which communication is going on, demands option A.

Juridically from the operator side there is no reason to exclude option A.

On the implementation side the capacity issue seems to be not relevant. The actual availability of option A and B in the switch could be an item for discussion.

In case of Option B the CCLID contains valid information.

However, if the CCLID is not available, the CCLID will get the value 00000000.

The LEMF shall support both options A and B.

If applicable, in the HI3 message the Called Party Subaddress shall be used. The CC link identifier is 8 decimal digits long and shall be mapped to octets 11 - 15.

NOTE 1: CCLID is not the same as the CIN. The CIN may implicitly represent the CCLID (see ES 201 671 v3.1.1 section A.1.1)

NOTE 2: CCLID must (also) be sent after an HI3 channel has been set-up. This implies UUS3. Since only subaddresses are available, option B will cause a conflict and must be avoided.

6.4 Correlation between CC and IRI

Reference: ES 201 671 v3.1.1 section 6.2 and A.1.2

To assure correlation between the independently transmitted content of communication (CC) and intercept related information (IRI) of an intercepted call 3 parameters are used. (LIID, CID and CCLID)

The parameter Call Identifier (CID) is defined as: CID = NID + CIN

Where NID = NWO/AP/SvP-identifier + NEID.

The NEID is optional.

If the NEID is used the NEID together with the CIN is unique within the domain of a NOW/AP/SvP. If the NEID is not used the CIN is unique within the domain of a NOW/AP/SvP. In both cases the correlation between CC and IRI is provided unequivocally. Both situations can be used for the delivery to a LEMF.

If the NEID is used it will be present in the ASN.1 message in the HI2.

7 Timing definitions

7.1 Definition of interception start

Reference: ES 201 671 section A.3.1

In order to decrease the possibility that the first part of the conversation to be intercepted is missed (the CC will not be buffered), the call set-up to the LEMF should start at the earliest possible moment. If possible, interception (connection of the circuit of the target to the circuit of the LEMF) should start immediately after reception of the answer signal in the call of the target.

7.2 Date & time indication

Reference: ES 201 671 section A.3.2.1

Local Dutch time shall be used. The indication for winter or summertime as defined in ES 201 671 shall be used. The option LocalTimeStamp as defined in ES 201 671 v3.1.1 section D.5 shall be used.

8 Security aspects

Reference: ES 201 671 section 11

The two communicating entities, the LEMF and the MF, must be convinced of each other's identity. The LEMF must only accept information sent by an authorized MF.

The MF must only send information to an existing and authorised LEMF.

8.1 Security requirements at the interface port HI2

Reference: ES 201 671 section 8, 11

The protocol used to transport data at HI2 is standard TCP/IP. The data transported at HI2 must have the following security properties: The two communicating parties must be authenticated and the transported data must have integrity and confidentiality. Integrity means that the data cannot be altered unnoticed during transport and confidentiality means that the data cannot be interpreted by third parties eavesdropping on the communications link. A standard security mechanism that incorporates all these requirements is TLS *Transport Layer Security*. This paragraph will specify the security parameters of TLS.

TLS uses the notion of a client and a server. The client initiates the session to the server. In our setup, the MF shall be the client that transports data to the server, the LEMF.

8.1.1 Authentication

Every TLS connection MUST have both client-side and server-side authentication. That means that the MF can be sure that it is talking to the right LEMF, and the LEMF can be sure that it receives data from the correct MF. If either one of these authentication steps fails an alarm MUST be generated. The LEMF can choose whether or not it wants to receive data from a MF which authentication failed. An MF can NEVER send data to an LEMF that fails authentication. (If that would happen, confidential or secret information would end up in a wrong place).

The key material for authentication is stored in *certificates*. A certificate is a dataset that contains the identity of the communicating party together with the necessary cryptographic key material to perform

the authentication. These certificates should be renewed every year (this is a standard amount of time for renewal of authentication certificates)

RSA is an authentication mechanism that recently has been given free because of the expiration of the patent date. RSA is the mechanism that will be used for authentication.

The RSA key shall have a length of 4096 bits. The interface shall also be capable to handle shorter key lengths. Shorter key lengths may only be used as an interim solution if 4096 bits keys are not available (for example limited TTP capabilities).

8.1.2 Confidentiality

For the confidentiality of the data Triple DES shall be used. This is a free, standard cryptographic algorithm that has been studied for more than twenty years.

8.1.3 Integrity

For the integrity of the data SHA will be used. This is a free, standard cryptographic algorithm.

8.1.4 TLS parameter

TLS as defined in RFC 2246 will be used with the following Cipher suite:

```
Cipher suite TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00, 0x0a)
```

With *both* client-side authentication *and* server-side authentication.

8.1.5 Distribution of certificates

The certificates that are used for the client and server authentication need to be managed. Certificates need to be generated, signed, distributed and possibly revoked. A central organisation shall be in place that takes care of these technical and operational activities. This should typically an external party that is trusted by all the other parties (TTP or Trusted Third Party).

8.2 Security requirements at the interface port HI3

Reference: ES 201 671 section A.4.5

8.2.1 Verification

For verification CLIP and COLP shall be checked by the LEMF and MF.

In the Netherlands, ISDN CUG is not available and therefore not applicable.

8.2.2 Authentication

Before CC can be delivered from the MF to the LEMF, the communication link shall be authenticated using cryptographic techniques. For authentication, a minimum of two messages is required: one from the MF to the LEMF and one back from the LEMF to the MF.

During the administrative phase, two secret 128 bits keys K1 and K2 for use in a symmetric crypto system, shall be transferred from the LEA to the MF via interface port HI1. As a result, for each monitored subscriber, there shall be a unique secret key pair K1 and K2. Key K1 is the secret Mediation Key and key K2 is the secret LawEnforcement Key.

Before a HI3 set-up message is sent from the MF to the LEMF, the MF creates an 8 octet number CHAL1. This number consists of the following fields:

- Sequence number SEQ. This is a 3 octet number which is increased by 1 for any new set-up message. In case of rollover SEQ advances from 0xFFFFFF to 0x000000. In every MF there is one SEQ for every LEMF. The LEMF must check on the increase of the SEQ.
- The LIID. This 3 octet field holds all 5 digits of the LIID plus the field separator.
- Handle value HV. This is a 2 octet random value.

$$\mathbf{CHAL1}_{\mathbf{8\ octet}} = \mathbf{SEQ}_{\mathbf{3\ octet}} + \mathbf{LIID}_{\mathbf{3\ octet}} + \mathbf{HV}_{\mathbf{2\ octet}}$$

CHAL1 is encrypted using Triple DES and secret key K2 to produce cipher text CIPH1

Cipher text CIPH1 is sent from the MF to the LEMF in the Called Party Subaddress.

NOTE: The only messages that are transferred transparently through the ISDN network are subaddressing and user-to-user signalling (UUS). UUS is not supported in the Netherlands and in-band signalling is not an option. Only subaddressing is suitable for authentication.

CIPH1 is 8 octets long and shall be mapped to octet 16 to 23.

In the LEMF, CIPH1 is decrypted with secret key K2 to obtain CHAL1. The LIID shall be compared with the LIID that is also transmitted in plain text via the Calling Party Subaddress. In case of a mismatch, an alarm should be raised and the pending communication link with the MF must be terminated immediately.

If no mismatch occurred, the LEMF constructs a similar challenge CHAL2. This is a concatenation of SEQ, LIID and the result of HV exored with magic value 0xFB3C.

$$\mathbf{CHAL2}_{\mathbf{8\ octet}} = \mathbf{SEQ}_{\mathbf{3\ octet}} + \mathbf{LIID}_{\mathbf{3\ octet}} + \mathbf{(\ HV}_{\mathbf{2\ octet}} \oplus \mathbf{0xFB3C\ )}$$

CHAL2 shall be encrypted using Triple DES and secret key K1 to produce cipher text CIPH2. This is sent via the Connected Party Subaddress back to the MF. In the MF, CIPH2 shall be decrypted using secret key K1 to produce challenge CHAL2. After XORing HV with magic value 0xFB3C, CHAL2 must be compared with CHAL1. In case of any mismatch an alarm should be raised and the connection must be terminated immediately.

9 Undefined parameters

Reference: ES 201 671 sections A.3.3, A.5.1

In all cases signals have to be translated into existing ASN.1 codes. In cases this is not possible (no examples available) the owner of the specification should assign new codes.

10 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 ETSI ES 201 671 in the Netherlands reverse to version 1.1.1 of that specification the implementations shall follow newer versions of ASN.1 considering releases of ES 201 671 and TS 101 671. The LEMF shall be able to accept the ASN.1 version that is sent by the mediator.

In ASN.1 version 1 the "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.

10 Contents of HI2 and HI3 Test call

Related to sections 10 and 11.4 (ETSI-NL)

Three types of test calls are defined:

- Initial Test Call;
- Special Request Test Call;
- Still-Alive Test Call..

Single Test Calls

A single test call is a unique delivery to check the correct configuration of an intercept.

The test call will be sent automatically at the start of interception of a target or after receiving a Test Call Initiation Message from the LEA. The LEA might want to do this after a period of inactivity of a target.

Still Alive Test Calls

Still alive test calls are frequent delivery to check the correct configuration of an intercept.

Default the still alive test call functionality is switched off.

The still alive test calls can be (de)activated by the provider or a LEA. A LEA can use the Test Call Initiation Message to (de)activate still alive test calls.

A still alive test call will be sent automatically after a period of 24 hours elapses. The actual moment for sending the still alive test call can be chosen in accordance with performance optimisation (for example to avoid congestion).

NOTE: Still alive test calls might be simulated by an LEMF application requesting single test calls. This can allow for different interval periods or dependencies with the target activity.

Test call handling

It is required that an indication is available, so the LEMF can recognise that the received information is a test call.

The CIN consists of 8 digits. In the Netherlands the value "AAAAAAAA" (hex) is allocated for the "Test call indication".

A test call will activate the whole chain from IIF, Mediator, delivery network and LEMF with HI2 records and a HI3 connection. In case the IIF can not be part of the test call this will be made explicitly known before activation.

Networks and services might have more IIFs and Mediators that can service a target. A test call will activate all chains sequentially in 3-second intervals.

The test call will create an IRI-Report record containing the mandatory fields and a test call field.

The test call on the HI3 connection can contain test tones. The HI3 test call connection will be released after being active for 1 to 2 seconds.

Test Call Initiation

A Test Call Initiation Message can only be assiociated with a single target.

To **initiate** a test call the LEA will send a "*TestCallRequestMessage*". This message will contain the "*LawfulInterceptionIdentifier*", the "*HandoverInterface3Address*" and the "*TypeofTestCall*": "SingeTestCall".

To **activate** still alive calls the LEA will send a "*TestCallRequestMessage*". This message will contain the "*LawfulInterceptionIdentifier*", the "*HandoverInterface3Address*" and the "*TypeofTestCall*": "*StillAlliveEnable*".

To **deactivate** still alive calls the LEA will send a "*TestCallRequestMessage*". This message will contain the "*LawfulInterceptionIdentifier*", the "*HandoverInterface3Address*" and the "*TypeofTestCall*": "*StillAlliveDisable*".

HI3 test call

With regard to the HI3 test call specific test content (i.e. tones etc) is not needed. All what is tested is that the interception parameters have been set-up correctly (LEMF address, keys etc.) and that the LEMF has been set-up to accept the calls correctly.

Establishing and disconnecting of test calls is performed by the MF. The time duration of a test call shall be circa one second.

HI2 test call

With regard to the HI2 test call an IRI-Report record will be sent by the MF to the LEMF.

11 Digital extensions to HI1

This section gives an overview of the possible digital extensions to HI1. The main purpose is to automate the Key management. The general mechanism, however, can also be used to facilitate the exchange of alarms, informational messages and test call requests. The only mandatory part in this section is the key management. The other mechanisms are optional.

The HI1 interface uses the same *transport mechanism* as is used for HI2, including all the security features, certificates, ROSE and ASN.1 present in the interface. Please refer to section 8.1 for details on the applied security mechanism. This interface should however never be misinterpreted for an HI2 interface since that interface only carries the Intercept Related Information.

This interface is located at the LI management centre of the operator. This centre shall therefore also have a connection to the same network as the HI2 interface (in this case "Datanet 1"). The way the information is processed by the management software of the operator is left to the responsibility of the operator.

11.1 Key management (mandatory)

This section describes the exchange process for the keys used for the authentication mechanism of HI3. This mechanism uses two large keys, 16 octets each, to ensure the security properties of this interface. Please refer to section 8.2.2 for details on the mechanism itself. This section describes the mechanism that shall be used for the electronic exchange of these keys. The only information that is exchanged electronically are the keys. The signed lawful authorisation will, because of legal reasons, use a non electronic mechanism (also part of the administrative HI1 interface).

NOTE: The original administrative HI1 interface shall also be present to function as a backup mechanism in case of emergency situations or network failures.

The message is sent according to section 12.5 from the LEMF to the management centre of the operator.

11.1.1 Coding of parameters

The **LawfulInterceptionIdentifier** and the **HandoverInterface3Address** are being coded using the ASCII representation. Example: The number (ASCII) "12345" is represented as the following five octets (decimal ASCII code) "049 050 051 052 053".

The **HandoverInterface3Address** is represented using the national Dutch format (currently ten digits). These ten digits will be put in the first ten octets of this field. The last fifteen octets shall be set to zero. This space can be used for future extensions to the current telephone numbering scheme.

The two **authentication keys** of 16 octets are transparently encoded in the two octet strings of 16 octets. Octet 1 of the octet string represents the most significant octet of the key.

For the communication at a **TCP level**, port 2811 will be used.

11.1.2 Description of parameters

The **LawfulInterceptionIdentifier** and the **HandoverInterface3Address** are the same as used on the lawful authorisation. These numbers uniquely define the target in this specific LEMF/MF combination. This respectively five-digit and ten-digit number will also appear on the administrative interface (e.g. the fax) together with signatures and additional information.

The **HandoverInterface3Address** is the telephone number of the LEMF to where the Content of Communication should be delivered. The regular Dutch representation will be used (the ten-digit number).

The two **authentication keys** are described in the section describing the algorithm used for the authentication on HI3.

11.2 Specification of Alarm messages (optional)

Alarm messages can be sent from the Management System to the LEMF or from the LEMF to the Management System regarding network or connection failures.

The following parameters are defined in the ASN.1 coding of the "HandoverAlarm":

- LawfulInterceptionIdentifier (optional) LIID target
- HandoverInterface3Address (mandatory) HI3 address LEMF
- AlarmNumber (mandatory) message code
- AlarmDescription (optional) additional alarm

If Alarm messages are transferred via the HI1 interface the following basic set of messages shall be applicable. More messages can be agreed between the operator and the authorities.

Table 5: Alarm messages from the Management system to an LEMF

Description (Management system -> LEMF)	LIID	LEMF HI3 addr	Nr	Parameters	To	Comment
Switch out of service	no	yes	000	"switch name"; "MF HI3 address"; "date/time"	all LEMFs	To be logged in LEMF
MF out of service	no	yes	002	"MF HI3 address"; "date/time"	all LEMFs	To be logged in LEMF
Test call failed	yes	yes	105		applicable LEMF	Automated message to LEMF *TestCallRequest* message (SingleTestCall)
Test call not performed Interception measure not active	yes	yes	106		applicable LEMF	Automated message to LEMF *TestCallRequest* message (SingleTestCall) in case the interception measure is not active at this moment
Keys not accepted duplicate LIID	yes	yes	111		applicable LEMF	Automated response to LEMF *HandoverInformationKey* message
LIID unknown	yes	yes	199		applicable LEMF	Automated response to LEMF *TestCallRequest* message and the messages 301 and 302 in the case the LIID is unknown in Management system
Message	yes or no	yes	400	"free text" (max. 256 characters)	Applicable LEMFs or all LEMFs	To be logged in LEMF
NOTE: The alarm messages 111 and 199 in this table are also appearing in table 7 with management messages.						

Table 6: Alarm messages from an LEMF to the Management systems

Description (LEMF-> Management system)	LIID	LEMF HI3 addr	Nr	Parameters	Comment
LEMF out of service	no	yes	200	"date/time"	To be logged in Management system
Message	no	yes	400	"free text" (max. 256 characters)	To be logged in Management system
NOTE: Alarm message 200 in this table is also appearing in table 8 with management messages.					

The use of Alarm messages is an issue of negotiation between the authorities and a provider. The meaning of the Alarm messages will also be agreed between the operator and the authorities.

If these Alarm messages are agreed the format of section 12.5 will be used.

11.3 Specification of Information messages (optional)

Information messages can be sent from the Management System to the LEMF or from the LEMF to the Management System regarding the network or LI functionalities.

The following parameters are defined in the ASN.1 coding of the "HandoverNotification":

- LawfulInterceptionIdentifier (optional) LIID target
- HandoverInterface3Address (mandatory) HI3 address LEMF
- InformationNumber (mandatory) message code
- InformationDescription (optional) additional information/parameters

If Information and Management messages are transferred via the HI1 interface the following basic set of messages shall be applicable. More messages can be agreed between the operator and the authorities.

Table 7: Information and Management messages from the Management system to an LEMF

Description (Management system -> LEMF)	LIID	LEMF HI3 addr	Nr	Parameters	To	Comment
Switch out of service	no	yes	000	"switch name"; "MF HI3 address"; "date/time"	all LEMFs	To be logged in LEMF
Switch in service again	no	yes	001	"switch name"; "MF HI3 address"; "date/time"	all LEMFs	To be logged in LEMF
MF out of service	no	yes	002	"MF HI3 address"; "date/time"	all LEMFs	To be logged in LEMF
MF in service again	no	yes	003	"MF HI3 address"; "date/time"	all LEMFs	To be logged in LEMF
Test call mechanism enabled	yes	yes	100		applicable LEMF	Automated response to LEMF *TestCallRequest* message (StillAlliveEnable)
Test call mechanism disabled	yes	yes	101		applicable LEMF	Automated response to LEMF *TestCallRequest* message (StillAlliveDisable)
Test call mechanism enabled but not activated	yes	yes	102		applicable LEMF	Automated response to LEMF *TestCallRequest* message (StillAlliveEnable)
Test call mechanism not allowed	yes	yes	103		applicable LEMF	Automated response to LEMF *TestCallRequest* message (StillAlliveEnable)
Test call performed	yes	yes	104		applicable LEMF	Automated message to LEMF *TestCallRequest* message (SingleTestCall)
Test call failed	yes	yes	105		applicable LEMF	Automated message to LEMF *TestCallRequest* message (SingleTestCall)
Test call not performed Interception measure not active	yes	yes	106		applicable LEMF	Automated message to LEMF *TestCallRequest* message (SingleTestCall) in case the interception measure is not active at this moment
Interception measure registered	yes	yes	107	"keys"; "start date/time"; "end date/time"	applicable LEMF	Automated message after registration

Description (Management system -> LEMF)	LIID	LEMF HI3 addr	Nr	Parameters	To	Comment
Interception measure activated	yes	yes	108	"date/time"	applicable LEMF	Automated message after activation
Interception measure deactivated	yes	yes	109	"date/time"	applicable LEMF	Automated message after deactivation or a cancellation before an activation
Keys accepted	yes	yes	110		applicable LEMF	Automated response to LEMF *HandoverInformationKey* message
Keys not accepted duplicate LIID	yes	yes	111		applicable LEMF	Automated response to LEMF *HandoverInformationKey* message
Interception measure modification	yes	yes	112	"keys"; "start date/time"; "end date/time"	applicable LEMF	Automated message after a modification
LIID unknown	yes	yes	199		applicable LEMF	Automated response to LEMF *TestCallRequest* message and the messages 301 and 302 in the case the LIID is unknown in Management system
Message	yes or no	yes	400	"free text" (max. 256 characters)	Applicable LEMFs or all LEMFs	To be logged in LEMF

Table 8: Information and Management messages from an LEMF to the Management systems

Description (LEMF-> Management system)	LIID	LEMF HI3 addr	Nr	Parameters	Comment
LEMF out of service	no	yes	200	"date/time"	To be logged in Management system
LEMF in service again	no	yes	201	"date/time"	To be logged in Management system
Interception established	yes	yes	301	"date/time"	To be logged in Management system. If the specific LIID is not registered, Management system replies with message 199 (Error LIID unknown)
Interception removed	yes	yes	302	date/time	To be logged in Management system. If the specific LIID is not registered, Management system replies with message 199 (Error LIID unknown)
Message	no	yes	400	"free text" (max. 256 characters)	To be logged in Management system

The use of Information messages is an issue of negotiation between the authorities and a provider. The meaning of the Information messages will also be agreed between the operator and the authorities. For example messages see Annex B.

If these Information messages are agreed the format of section 12.5 will be used.

11.4 Specification of Test calls (optional)

The use of test calls is an issue of negotiation between the authorities and a provider. The implementation of the test calls will also be agreed between the operator and the authorities. If these messages are agreed the following format will be used.

11.5 National electronic HI1 interface

By means of the use of the national parameters the electronic HI1 parameters can be signalled between the LEMF and the Operator.

Below is the definition of the implementation of the National LI Parameters for HI1: "NL-HI1-Parameters". These specific NL National parameters for HI1 are included as part of the National-HI1-ASN1parameters which are defined as part of the HI1-Operation, Notification and Alarm_Indicator as defined in section D.4 of TS 101 671 v2.9.1.

```
National-HI1-ASN1parameters     ::= SEQUENCE
{
    countryCode         [1] PrintableString (SIZE (2)),
        -- Country Code according to ISO 3166-1,
        -- the country to which the parameters inserted after the extension marker
apply
        -- For The Netherlands the code is "NL".
    ...,
    nL-HI1-Parameters   [2] NL-HI1-Parameters
}

-- ==========================
-- NL HI1 national Parameters
-- ==========================

NL-HI1-Parameters   ::= SEQUENCE
    -- Content defined by national law.
{
    specificationVersion    [1] INTEGER (0..255),
        -- This version of the specific NL HI1 ASN.1 is "1".
    nL-HI1-Operation        [2] NL-HI1-Operation,
    ...
}
```

```
NL-HI1-Operation    ::= CHOICE
{
    handoverInformationKey  [1] SEQUENCE
        -- Message generally sent from LEA to provider.
    {
        lawfullnterceptionIdNL  [1] LawfulInterceptionIdNL,
        mediationKey            [2] OCTET STRING (SIZE(1..16)),
            -- OCTET string filled with the 16 octets of the HI3 authentication key.
        lawEnforcementKey       [3] OCTET STRING (SIZE(1..16))
            -- OCTET string filled with the 16 octets of the HI3 authentication key.
            -- The description of these keys can be found in the section
            -- describing the HI3 authentication mechanism.
    },
    handoverAlarm           [2] SEQUENCE
        -- Message generally sent from provider to LEA.
    {
        lawfullnterceptionIdNL  [1] LawfulInterceptionIdNL,
        alarmNumber             [2] OCTET STRING (SIZE(1..3)),
            -- ASCII characters of the number, e.g. "123" = 3 octets 0x31 0x32 0x33)
            -- This is the number of the alarm. This number is taken from
            -- a central maintained list of all possible alarms.
        alarmDescription        [3] OCTET STRING (SIZE(1..256)) OPTIONAL
            -- This field (in ASCII characters) gives space for optional comments
            -- or alarm details.
    },
    handoverNotification    [3] SEQUENCE
        -- Message sent from LEA to provider or from provider to LEA
    {
        lawfullnterceptionIdNL  [1] LawfulInterceptionIdNL,
        informationNumber       [2] OCTET STRING (SIZE(1..3)),
            -- ASCII characters of the number, e.g. "123" = 3 octets 0x31 0x32 0x33)
            -- This is the number of the notification.
            -- This number is taken from a central maintained list of
            -- all possible information messages.
        informationDescription  [3] OCTET STRING (SIZE(1..256)) OPTIONAL
            -- This field (in ASCII characters) gives space for optional comments
            -- or information details.
    },
    testCallRequest         [4] SEQUENCE
        -- Message generally sent from LEA to provider.
    {
        lawfullnterceptionIdNL  [1] LawfulInterceptionIdNL,
        typeOfTestCall          [2] ENUMERATED
        {
            singleTestCall(0),
            stillAlliveEnable(1),
            stillAliveDisable(2),
            ...
        }
    }
}
```

```
LawfulInterceptionIdNL  ::= SEQUENCE
{
    lawfulInterceptionIdentifier    [1] OCTET STRING (SIZE(5)) OPTIONAL,
        -- ASCII characters of the number, e.g. "12345" = 5 octets 0x31 0x32 0x33 0x34
0x35
        -- The same identifier as used on the lawful authorization.
    handoverInterface3Address       [2] OCTET STRING (SIZE(10..25)),
        -- ASCII characters of the ISDN number,
        --  e.g. "0201234567" = 10 octets 0x30 0x32 0x30 0x31 0x32 0x33 0x34 0x35 0x36
0x37
        -- This is the (currently 10 digits) Dutch ISDN number of the LEMF.
    operator-Identifier             [3] OCTER STRING (SIZE(1..5)) OPTIONAL
        -- Notification of the NOW/AP/SvP in ASCII- characters. See also
        -- 'Implementing ETSI ES 201 671 in the Netherlands' clause 6.2.1.
        -- This parameter is MANDATORY if message is sent from provider to LEA.
}
```

12 Use of subaddress to carry correlation information

Reference: ES 201 671 Annex E

12.1 Introduction

This section is based on enhancements made by ETSI TC SEC WG LI on the optional use of subaddressing in HI3.

In the Netherlands the supplementary service UUS1 is not applicable as transport mechanism for the correlation identifiers. In stead the subaddressing mechanism shall be used.

The calling party number, the calling party subaddress (CgP Sub) and the called party subaddress (CdP Sub) are used to carry correlation information.

The calling party subaddress (CgP Sub) and the connected party subaddress (CoP Sub) are used to carry authentication information.

Specifically for the Netherlands octets 16 to 23 of the Called Party Subaddress are allocated for the transport of authentication information from the MF to the LEMF (see table 6).

For the transport of the authentication information from the LEMF to the MF octets 4 to 11 of the Connected Party Subaddress are allocated (see table 7).

12.2 Subaddress options

The coding of a subaddress information element is given in EN 300 403-1. The following options shall be chosen:

Table 1: Subaddress options

Option	Value
Type of subaddress	user specified
Odd/even indicator	employed for called party subaddress when no national parameters are used

12.3 Subaddress coding

The coding of subaddress information shall be in accordance with EN 300 403-1.

12.3.1 BCD Values

The values 0-9 shall be BCD coded according to their natural binary values. The hexadecimal value F shall be used as a field separator. This coding is indicated in table 2.

Table 2: Coding BCD values

Item	BCD representation			
	Bit 4	Bit 3	Bit 2	Bit 1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
Test call indicator	1	0	1	0
Field separator	1	1	1	1

When items are packed two to an octet, the least significant item shall be coded by mapping bit 4 to bit 8, bit 3 to bit 7, etc.

12.3.2 Field order and layout

Fields shall be presented into the subaddress in the following order:

Table 3: Fields in the Called Party Subaddress

Order	Field
1	Operator-ID
2	CIN
3	CCLID
4	CIPH1

Table 4: Fields in the Connected Party Subaddress

Order	Field
1	CIPH2

Table 5: Fields in the Calling Party Subaddress

Order	Field
1	Lawful Interception Identifier (LIID)
2	Direction
3	Service Octets

Each field noted above shall be included, whether empty or not, and a field separator shall separate each field. When a field is empty, that shall be indicated by two consecutive field separators. There shall be a field separator after the final field, too.

The Service Octets as available shall always be mapped into the Calling Party Subaddress, as appropriate. If one of the parameters TMR, BC or HLC is not available, the octet shall be fill with 'FF' hex. If Mobile Teleservice Code is not available, that octet shall not be transmitted. If Mobile Teleservice Code and Mobile Bearer Service Code are not available, both octets shall not be transmitted.

Table 6 represents the called party subaddress, table 7 represents the connected party subaddress and table 8 the calling party subaddress.

Table 6: Called Party Subaddress

Bits								Octets
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
Called party subaddress identifier								1
Length of called party subaddress contents								2
Type of subaddress = user specified, odd/even indicator								3
Operator-ID ②				Operator-ID ①				4
Operator-ID ④				Operator-ID ③				5
Field separator				Operator-ID ⑤				6
CIN ②				CIN ① (note 1)				7
CIN ④				CIN ③				8
CIN ⑥				CIN ⑤				9
CIN ⑧				CIN ⑦				10
CCLID ①				Field separator				11
CCLID ③				CCLID ②				12
CCLID ⑤				CCLID ④				13
CCLID ⑦				CCLID ⑥				14
Field separator				CCLID ⑧				15
CIPH1 ① (note 2)								16
CIPH1 ②								17
CIPH1 ③								18
CIPH1 ④								19
CIPH1 ⑤								20
CIPH1 ⑥								21
CIPH1 ⑦								22
CIPH1 ⑧								23

NOTE 1: In the Netherlands the value "AAAAAAAA" (hex) is allocated for the "Test call indication".

NOTE 2: The Octets after the final field (CCLID) of the Called Party Subaddress are reserved for national use, e.g. for authentication purposes. In the Netherlands these octets are allocated to carry the authentication information (CIPH1).

Table 7: Connected Party Subaddress

Bits								Octets
8	7	6	5	4	3	2	1	
Connected party subaddress identifier								1
Length of connected party subaddress contents								2
Type of subaddress = user specified, odd/even indicator								3
CIPH2 ① (note)								4
CIPH2 ②								5
CIPH2 ③								6
CIPH2 ④								7
CIPH2 ⑤								8
CIPH2 ⑥								9
CIPH2 ⑦								10
CIPH2 ⑧								11

NOTE: In the Netherlands the octets 4 to 11 are allocated to carry the authentication information (CIPH2).

Table 8: Calling Party Subaddress

Bits								Octets
8	7	6	5	4	3	2	1	
Calling party subaddress identifier								1
Length of called party subaddress contents								2
Type of subaddress = user specified, odd/even indicator according to the amount of BCD-digits								3
LIID ②				LIID ① (note 6)				4
LIID ④				LIID ③				5
Field separator				LIID ⑤				6
Field separator				Direction				7
Spare				Spare				8
Q.763 TMR (note 1)								9
Q.931 BC octet 3 (note 2)								10
Q.931 HLC octet 4 (note 3)								11
Mobile Bearer Service Code (note 4)								12
Mobile Teleservice Code (note 5)								13

NOTE 1: if available, the Transmission Medium Requirement according to EN 300 356. If not available, the value is 'FF' hex.

NOTE 2: if available, only octet 3 of the Bearer Capability I.E. according to EN 300 403. If not available, the value is 'FF' hex.

NOTE 3: if available, only octet 4 of the High Layer Compatibility I.E. according to EN 300 403. If not available, the value is 'FF' hex.

NOTE 4: if available, the Mobile Bearer Service Code according to GSM 09.02. If not available, these octets shall not be transmitted.

NOTE 5: if available, the Mobile Teleservice Code according to GSM 09.02. If not available, this octet shall not be transmitted.

NOTE 6: In the Netherlands the LIID consists of 5 decimal characters.

12.3.3 Missing parameters in the Subaddresses

Table E.3.6: Example how field separator should be used when field is empty

Called party subaddress without CIN parameter

Bits								Octets
8	7	6	5	4	3	2	1	
Called party subaddress identifier								1
Length of called party subaddress contents								2
Type of subaddress = user specified, odd/even indicator								3
Operator-ID ②				Operator-ID ①				4
Operator-ID ④				Operator-ID ③				5
Field separator				Operator-ID ⑤				6
CCLID ①				Field separator				7
CCLID ③				CCLID ②				8
CCLID ⑤				CCLID ④				9
CCLID ⑦				CCLID ⑥				10
Field separator				CCLID ⑧				11
spare				spare				12
spare				spare				13
spare				spare				14
spare				spare				15
(see note)								16 17 18 19 20 21 22 23

NOTE: The Octets after the final field (CCLID) of the Called Party Subaddress are reserved for national use, e.g. for authentication purposes.

12.4 Field coding

Each field shall employ decimal coding, except for the Service Octets of the CgP Sub and the octets reserved for national use (octets 16-23 of the CdP Sub). In the Netherlands in the CdP Sub the CIN value "AAAAAAAA" (hex) is allocated for the "Test call indication". Other values are not permitted.

12.4.1 Direction

The direction field shall be coded as follows:

Table 9: Direction coding

Indication	Value
Mono mode (combined signal)	0
CC from target	1
CC to target	2
Direction unknown	3

12.4.2 Coding of the Calling Party Number

The Coding of the Calling Party Number has been made more flexible in the ETSI specification. Besides the international number the Calling Party number may e.g. also be coded as a national number as indicated by the Nature of address.

The Network Element Identifier (NEID) shall be carried by the calling party number information element. The coding shall be as follows, depending on the type of network access (see note 1):

Numbering plan identification: ISDN/telephony numbering plan (ITU-T Recommendation E.164 [58])

Nature of address: As specified in ITU-T Recommendation Q.731.3 (see note 1) **(e.g. national (significant) number or international number) (in case of ISUP signalling)**

Type of number: As specified in ITU-T Recommendation Q.951-1 and ITU-T Recommendation Q.951-3, EN 300 092 (e.g. unknown, subscriber number, national number or international number), and Network Operator specific type of access (BRA or PRA) (in case of DSS1 signalling, see notes 2 and 3)

Screening indicator: Network provided (in case ISUP signalling)

Screening indicator: User-provided, not screened (in case of DSS1 signalling, see note 3)

Presentation indicator: Presentation allowed

NOTE 1: The relevant national specification of the Signalling System Number 7 may also specify requirements on the Nature of address for national specific use in national variants of ISUP.

NOTE 2: Usually, the IIF respectively the Mediation Function is connected to the network by links using Signalling System Number 7 and ISDN User Part (ISUP), whereby the parameters are coded according to EN 300 356. But in some cases, the IIF respectively the Mediation Function may be connected via a Basic Rate Access or a Primary Rate Access using D-Channel signalling, whereby the parameters are coded according to EN 300 403-1.

NOTE 3: The network will perform screening, i.e. the number will arrive at the LEMF as "user-provided, verified and passed" with the appropriate "type of number" indicator. A network provided number shall also be accepted at the LEMF.

12.5 Length of fields

The length of the identifiers is variable. The minimum and maximum length of each field shall be as given in the table below.

Table 10: field length

Field	Minimum length (decimal digits)	Maximum length (decimal digits)	Maximum length (Half-Octets)	I.E.
Operator ID	2	5	5+1	CdP Sub
CIN	6	8	8+1	CdP Sub
CCLID	1	8	8+1	CdP Sub
LIID	2	25	25+1	CgP Sub
Direction	1	1	1+1	CgP Sub
Service Octets			10	CgP Sub
CIPH1			16	Cgp Sub
CIPH2			16	CoP Sub

13 Location Information

In mobile networks, the geographical location of the target in the network will be delivered as part of an intercept. The location information can be delivered in network specific co-ordinates or in network independent co-ordinates.

Via ETSI-NL the network specific coordinates will be delivered (for example for GSM the Global Cell Identification). In parallel, the location will be delivered in geographical coordinates either according to WGS84 or RD-coordinates (Amersfoort coordinates/ RijksDriehoek coordinates). By means of the use of the national parameters the RD coordinates can be included.

Below is the definition of the implementation of the National LI Parameters for HI2: "NL-HI2-Parameters". These specific NL National parameters for HI2 are included as part of the National-HI2-ASN1parameters which are defined as part of the IRI parameters as defined in section D.5 of TS 101 671 v2.9.1.

```
National-HI2-ASN1parameters     ::= SEQUENCE
{
    countryCode         [1] PrintableString (SIZE (2)),
        -- Country Code according to ISO 3166-1,
        -- the country to which the parameters inserted after the extension marker
apply
        -- For The Netherlands the code is "NL".
    ...,
    nL-HI2-Parameters   [2] NL-HI2-Parameters
}

-- ==========================
-- NL HI2 National Parameters
-- ==========================

NL-HI2-Parameters   ::= SEQUENCE
    -- Content defined by national law.
{
    specificationVersion    [1] INTEGER (0..255),
        -- This version of the specific NL HI2 ASN.1 is "2".
    nLLocation              [2] NLLocation OPTIONAL,
    ...
}

NLLocation      ::= SEQUENCE
{
    azimuth         [0] INTEGER (0..359) OPTIONAL,
        -- The azimuth is the bearing, relative to true north.
    rDX-coordinate  [1] PrintableString (SIZE(6..10)),
        -- X-coordinate RD form e.g. 155000 (RD X coordinate OV-church Amersfoort)
    rDY-coordinate  [2] PrintableString (SIZE(6..10)),
        -- Y-coordinate RD form e.g. 463000 (RD Y coordinate OV-church Amersfoort)
    ...
}
```

Annex A Example implementation (informative)

```
/*
 * Demonstration implementation of the authentication mechanism of HI3
 * Date: 6 December 2000
 *
 * This is a reference implementation, not optimised for speed but for
 * evaluation of the mechanism. The execution speed of this program on
 * a Pentium III 800 Mhz is 7 milliseconds, so speed should not be a
 * problem. The crypto routines are from the OpenSSL library. This is a
 * public crypto library available on http://www.openssl.org
 *
 * FreeBSD compile command:
 * cc -Wall -pedantic auth_hi3.c -ldes
 */

#include <des.h>
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <string.h>

int __i;
des_key_schedule    schedK1a, schedK1b, schedK2a, schedK2b;

#define printarray( name, length, array ); \
        printf(name); \
        for( __i=0; __i<length; __i++ ) printf(" %.2X",array[__i]); \
        printf("\n");


void make_deskey( des_cblock *Ka, des_key_schedule schedKa ) {

    /*
     * This is a small routine to compute a 'safe' DES key.
     */

    int i;

    i = -1;
    while( i<0 ) {
        des_random_key( Ka );
        i = des_set_key_checked( Ka, schedKa );
    }
}


void generate_keys( unsigned char *K1, unsigned char *K2 ) {

    /*
     * This routines provides the two 128 bits keys, K1 and K2.
     * 3Des uses two 8 octets keys, let's call the Ka and Kb.
     * The left eight octets of each K are used for Ka and the
     * right eight byes are used for Kb.
     * K = Ka + Kb (Octetwise concatenation)
     * While generating the Keys, one should check for 'weak keys'
     * in thes. Most cryptolibraries have build in functions to do
     * that...
     */

    des_cblock      K1a, K1b, K2a, K2b;

    make_deskey( &K1a, schedK1a );
    make_deskey( &K1b, schedK1b );
    make_deskey( &K2a, schedK2a );
    make_deskey( &K2b, schedK2b );

    memcpy( K1, K1a, 8 );
    memcpy( K1+8, K1b, 8 );
    memcpy( K2, K2a, 8 );
    memcpy( K2+8, K2b, 8 );
}
```

```
void print_data_mf( unsigned char *K1, unsigned char *K2, int SEQ, int LIID,
                int HV, unsigned char *CHAL1, unsigned char *CIPH1 ) {

    /*
     * This routine prints out the data that is used to send the
     * information from the MF to the LEMF.
     */

    printarray( "K1:", 16, K1 );
    printarray( "K2:", 16, K2 );
    printf( "SEQ\t= %.2X\n", SEQ );
    printf( "LIID\t= %.2X\n", LIID );
    printf( "HV\t= %.2X\n", HV );
    printarray( "CHAL1:", 8, CHAL1 );
    printarray( "CIPH1:", 8, CIPH1 );
    printf( "\nSending CIPH1 from MF to LEMF\n\n" );
}


void print_data_lemf( unsigned char *CIPH1, unsigned char *CHAL1_LEMF,
                      int SEQ, int LIID, int HV, int HV_LEMF,
                      unsigned char *CHAL2, unsigned char *CIPH2 ) {

    /*
     * This routine prints out the data is used to send the
     * information from the LEMF to the MF.
     */

    printarray( "LEMF Received Ciphertext:", 8, CIPH1 );
    printarray( "Decrypted:", 8, CHAL1_LEMF );
    printf( "Resulting SEQ\t= %.2X\n", SEQ );
    printf( "Resulting LIID\t= %.2X\n", LIID );
    printf( "Resulting HV\t= %.2X\n", HV );
    printf( "HV xor 0xFB3C\t= %.2X\n", HV_LEMF );
    printarray( "CHAL2:", 8, CHAL2 );
    printarray( "CIPH2:", 8, CIPH2 );
    printf( "\nSending CIPH2 from LEMF to MF\n\n" );
}


void split_3octets( int source, int *b1, int *b2, int *b3 ) {

    /*
     * This routine does an explicit octetwise split of a
     * Three octet identifier into the three separate
     * octets.
     */

    int temp;

    temp = source;
    *b1 = (int) ( temp / 65536 );
    temp = temp - ( 65536 * *b1 ) ;
    *b2 = (int) ( temp / 256 );
    temp = temp - ( 256 * *b2 );
    *b3 = temp;
}


void generate_challange( unsigned char *CHAL, int SEQ, int LIID, int HV ) {

    int     seq_byte0, seq_byte1, seq_byte2;
    int     liid_byte0, liid_byte1, liid_byte2;
    int     hv_byte_dummy, hv_byte0, hv_byte1;

    /* because of big and little endians and because of the fact that
     * this is reference code, the octets are copied in a slow but correct
     * way to the various octets of the CHAL sequence
     * We fill the octets with the most significant value on the left
     * side. The numbering also starts on the left side.
     * So octet 0 of SEQ contains the leftmost of three octets, having
     * the most siginifcant value.
     * The routine split_3octets() performs this function for a maximum
     * of three octets;
     */
```

```
    split_3octets( SEQ, &seq_byte0, &seq_byte1, &seq_byte2 );
    split_3octets( LIID, &liid_byte0, &liid_byte1, &liid_byte2 );
    split_3octets( HV, &hv_byte_dummy, &hv_byte0, &hv_byte1 );

    CHAL[0] = seq_byte0;
    CHAL[1] = seq_byte1;
    CHAL[2] = seq_byte2;
    CHAL[3] = liid_byte0;
    CHAL[4] = liid_byte1;
    CHAL[5] = liid_byte2;
    CHAL[6] = hv_byte0;
    CHAL[7] = hv_byte1;
}


void check_data( unsigned char *CHAL, int *SEQ, int *LIID, int *HV ) {

    /*
     * This routine reconstructs the separate datafields from
     * a received challange.
     */

    *SEQ  = 65536 * CHAL[0] + 256 * CHAL[1] + CHAL[2];
    *LIID = 65536 * CHAL[3] + 256 * CHAL[4] + CHAL[5];
    *HV   =                   256 * CHAL[6] + CHAL[7];

}


void compare_challange( unsigned char *CHAL1, unsigned char *CHAL2 ) {

    int i;
    int a,b;

    printf( "Comparing CHAL1 with CHAL2.\n" );

    for( i=0; i<8; i++ ) {
        a = CHAL1[i];
        b = CHAL2[i];
        printf( "CHAL1[%d] == %d\tCHAL2[%d] == %d\t",i,a,i,b );
        if( a==b ) {
            printf( "Checked!\n" );
        } else {
            printf( "ALERT!\n" );
        }
    }
}


int main( int argc, char *argv[] ) {

    des_cblock  CHAL1;
    des_cblock  CHAL2;
    des_cblock  CIPH1;
    des_cblock  CIPH2;
    des_cblock  CHAL1_LEMF;
    des_cblock  CHAL2_MF;
    int     SEQ;
    int     SEQ_LEMF;
    int     LIID;
    int     LIID_LEMF;
    int     HV;
    int     HV_LEMF;
    unsigned char   K1[16], K2[16];


    LIID = 0x123456;

    srandom( time(NULL) );
    SEQ= (int) random() & 0xFFFFFF;
    HV = (int) random() & 0xFFFF;

    /*
     * In this example, the keys are securely generated. This should
     * also be done in the real world.
```

```
     */

    generate_keys( K1, K2 );

    /*
     * From the SEQ, the LIID and the HV the Challange is generated
     * by concatenating them.
     */

    generate_challange( CHAL1, SEQ, LIID, HV );

    /*
     * The Challange is encrypted using K2 and 'send' to the LEMF
     */

    des_ecb2_encrypt(&CHAL1 ,&CIPH1, schedK2a, schedK2b, DES_ENCRYPT );
    print_data_mf( K1, K2, SEQ, LIID, HV, CHAL1, CIPH1 );

    /*
     * The LEMF will decrypt the received data and check of everything
     * is alright. This example completely emulates the decryption process
     * (there is a 'data separation' between the LEMF routinges and the
     * MF routines.
     */

    des_ecb2_encrypt(&CIPH1, &CHAL1_LEMF, schedK2a, schedK2b, DES_DECRYPT );
    check_data( CHAL1_LEMF, &SEQ_LEMF, &LIID_LEMF, &HV_LEMF );

    /*
     * The HV is xored with the magic value and a new challange is
     * created.
     */

    HV_LEMF = HV ^ 0xFB3C;
    generate_challange( CHAL2, SEQ, LIID, HV_LEMF );

    /*
     * The data is encrypted and 'send' to the the MF
     */

    des_ecb2_encrypt( &CHAL2, &CIPH2, schedK1a, schedK1b, DES_ENCRYPT );
    print_data_lemf( CIPH1, CHAL1_LEMF, SEQ, LIID, HV, HV_LEMF,
                     CHAL2, CIPH2 );

    /*
     * The MF decrypts the information and obtains the original HV
     * back by xoring again the last two octets of the challange
     * with the magic value.
     */

    des_ecb2_encrypt( &CIPH2, &CHAL2_MF, schedK1a, schedK1b, DES_DECRYPT );
    CHAL2_MF[6] = CHAL2_MF[6] ^ 0xFB;
    CHAL2_MF[7] = CHAL2_MF[7] ^ 0x3C;

    /*
     * Now the result is compared with the original CHAL1 as send by the
     * MF.
     */

    compare_challange( CHAL1, CHAL2_MF );

    return 0;

}
```

Annex B Management reports (informative)

In this informative annex examples are given of Management reports:

1 Indication that the Interception measure "12345" has been disconnected before expiry of the original duration.

This report indicates that the sending of intercepted information of a certain Interception Measure is not longer needed and that the LEMF is not longer receiving intercepted information. Implicitly this report indicates that error messages on this LIID doesn't need to be checked anymore.

2 Disturbance reception on LEA address "1234567890"

This report indicates that the LEA with the indicated address is not available.

3 Disturbance reception on LEA address "1234567890" till hh:mm hours

This report indicates that the LEA with the indicated address is temporary not available till hh:mm because of e.g. maintenance.

Annex C (informative): Document and Change Request History

Status of ETSI.nl		
Date	**Version**	**Remarks**
February 2001	1.0	First concept, July 7th 2006
September 2011	1.1	Adding to the document: - *.Appendix A to Implementing ETSI ES 201 671 in the Netherlands; Version 1.0; July 2004,* - *Information note to Implementing ETSI ES 201 671 in the Netherlands; Version 1.0; 16 December 2004,* - *Appendix A to Implementing ETSI ES 201 671 in the Netherlands; Version 1.1; 3 July 2007,*