Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
Département fédéral de l'Environnement, des Transports, de l'Energie et de la Communication
Dipartimento federale dell'Ambiente, dei Trasporti, dell'Energia e delle Comunicazioni

UVEK
ETEC
ATEC

Dienst für Besondere Aufgaben
Service des tâches spéciales
Servizio per compiti speciali

CONFIDENTIAL

Lawful Interception of Telecommunications Traffic

Packet Switched Services

Technical Requirements for the

Delivery of Intercepted Electronic Mail

V 1.0: 02 April 2002

valid from: 15 April 2002

Document History

Version	Date	Status	Remarks
0.2	31st December 2001	Draft	First draft
0.3	11th January 2002	Draft	Revision after WG-meeting of January 10th, 2002
0.4	30th January 2002	Draft	Revision after WG-meeting of January 28th, 2002
0.9	7th March 2002	Final	Revision after WG-meeting of February 25th, 2002
1.0	2nd April 2002	Published	

Contents

1 Scope 4
2 References 4
3 Abbreviations 4
4 Definitions 5
5 Notational conventions 5
6 General requirements 6
6.1 Delivery mechanism for the results of interception 6
6.1.1 Header fields of the container e-mail 6
6.1.2 Security mechanisms 7
6.1.3 Delivery failure 8
6.2 Date and time specifications 8
6.2.1 Timestamp syntax 8
6.2.2 Synchronization 9
7 Interception of e-mail contents 9
7.1 Data structure 9
7.2 Delivery specifications 10
8 Interception of telecommunication parameters 10
8.1 Data structure 10
8.1.1 Data structure for incoming e-mail 11
8.1.2 Data structure for relayed e-mail 12
8.1.3 Data structure for mailbox access 13
8.1.4 Data structure for Internet access 13
8.2 Delivery period 15
8.2.1 Actual data fetched in real-time 15
8.2.2 Historical data 15
9 Test requirements 15
10 Final Provisions 16
10.1 Temporary arrangement 16
10.2 Further provisions 16
11 Appendix 17
11.1 Document type definitions 17
11.1.1 Incoming e-mail 17
11.1.2 Relayed e-mail 17
11.1.3 Mailbox access 17
11.1.4 Internet access 17

1 Scope

This document provides the technical requirements for interfacing the internet service providers (ISP) with the governmental Special Duties Unit (SDU) concerning the issues of lawful interception for packet switched services. These services include

- e-mail
- Internet access

Reference is made to the legal provisions related to lawful interception in Switzerland, as denoted in [1] and [2], in particular to the articles 24, 25, and 26 of [2].

The interfaces described herein cover the delivery of real-time and historical results of interception according to article 24 of [2]. Details about administrative and operational requirements concerning lawful interception, the interface for administrative information (denoted as HI1 in [3]) and the requirements related to the article 27 of [2] will be defined in separate documents.

2 References

[1]	SR 780.1	"Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs" (BÜPF) vom 6. Oktober 2000 (http://www.admin.ch/ch/d/sr/c780_1.html)
[2]	SR 780.11	"Verordnung über die Überwachung des Post- und Fernmeldeverkehrs" (VÜPF) vom 31. Oktober 2001 (http://www.admin.ch/ch/d/sr/c780_11.html)
[3]	ETSI ES 201 158	"Telecommunication security; Lawful interception (LI); Requirements for network functions", version 1.1.2, May 1998 (www.etsi.org)
[4]	RFC 2822	"Internet Message Format", April 2001
[5]	RFC 2045 - 2049	"Multipurpose Internet Mail Extensions (MIME)", November 1996
[6]	RFC 2821	"Simple Mail Transfer Protocol", April 2001
[7]	RFC 2440	"OpenPGP Message Format", November 1998
[8]	RFC 1305	"Network Time Protocol (Version 3) Specification, Implementation and Analysis", March 1992
[9]	RFC 2279	"UTF-8, a Transformation Format of ISO 10646", January 1998

3 Abbreviations

[CRLF]	Sequence of "carriage return" (CR) and "line feed" (LF), i.e. of ASCII-codes 13 and 10 (decimal).
[SP]	"Space", i.e. ASCII-code 32 (decimal)
ASCII	American National Standard for Information Interchange
CLI	Calling Line Identity (calling party number)
DTD	Document Type Definition
GPRS	General Packet Radio Service
HI	Handover Interface
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISP	Internet Service Provider

LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identifier
MAC	Medium Access Control
MIME	Multi-purpose Internet Message Extension
MTA	Mail Transfer Agent
NTP	Network Time Protocol
PGP	Pretty Good Privacy
POP	Post Office Protocol
PSTN	Public Switched Telephone Network
RFC	Request for Comment
SDU	Special Duties Unit
SMTP	Simple Mail Transfer Protocol
UMTS	Universal Mobile Telecommunication Standard
xDSL	All types of Digital Subscriber Lines (DSL)
XML	Extensible Markup Language

4 Definitions

Container e-mail Signed and encrypted delivery message transmitted by the ISP to the LEMF

Delivery message MIME-conform message containing results of interception in clear.

Interception type See [2] (article 24 section f and g of [2] are combined to one interception type)

Internet Service Provider The legal entity providing internet services to the intercepted

Law Enforcement Monitoring Facility The data center of the SDU, where the results of interception is collected and processed (see also [3])

Results of interception Intercepted information related to the target service provided by the ISP (see also [3])

Special Duties Unit The governmental authority responsible for the collection and processing of all intercept data in Switzerland

Target identifier Identity associated with a target service used by a person or persons whose telecommunications are to be intercepted (see also [3])

5 Notational conventions

Throughout this document the following syntactic notations hold:
Key-words, constants, and phrases that may occur in a message are enclosed in quotation marks, e.g. `"01"`. All quoted expressions are case-sensitive and must be used strictly following the syntax rules defined in this document. `[CRLF]` indicates a sequence of *carriage return* and *line feed*. `[SP]` denotes a *space*. Markups are enclosed by angle brackets, e.g. `<mail-from>`; printed characters are indicated as quoted strings.

6 General requirements

This chapter covers general technical requirements that need to be fulfilled by the ISPs when providing results of interception to the Swiss LEMF.

6.1 Delivery mechanism for the results of interception

Any result of interception must be packed into a MIME-conform [4, 5] *delivery message*, which must subsequently be signed and encrypted. The resulting *container e-mail* must be delivered to the LEMF through the Internet according to [6]. For each surveillance case a specific mailbox is maintained at the LEMF. The following sections define the generic format of the delivery message and the container e-mail, respectively.

6.1.1 Header fields of the container e-mail

The contents of the header fields *From*, *To*, and *Subject* according to [5] must be composed following the syntax listed below.

From: `"LI_monitor@" ISP-domain` (denotes the sender's address)
To: `LIID "@" LEMF-domain` (denotes the recipient's address)
Subject: `interception-type "_" major-version "." minor-version`

The variables are defined as follows:

`ISP-domain =` Domain name of the ISP (see also chapter 10.1)

`LIID =` Unique identifier of the surveillance case provided to the ISP by the SDU when commissioning the surveillance case. It consists of up to a maximum of 25 digits (0..9).

`LEMF-domain =` Domain name of the receiving LEMF.

`interception-type =` Two-digit code representing the *interception type* according to the classification in [2].

Interception type code	Representation
"00"	Is reserved for administrative e-mails
"01"	Real-time delivery of an e-mail incoming to the target identifier mailbox (according to chapter 7)
"02"	Real-time delivery of an e-mail sent by the target identifier (according to chapter 7)
"03"	Delivery of a list containing actual STMP envelope information of e-mails incoming to the target identifier mailbox (see chapter 8.1.1)
"04"	Delivery of a list containing actual mailbox access

	information of the target identifier (see chapter 8.1.3)
“05”	Delivery of a list containing STMP actual envelope information of e-mails sent by the target identifier (see chapter 8.1.2)
“06”	Delivery of a list containing historical internet access information of the target identifier (see chapter 8.1.4)
“07”	Delivery of a list containing historical STMP envelope information of e-mails sent and received by the target identifier (see chapter 8.1.1 and 8.1.2)

Results of interception belonging to different *interception types* must not be mixed in a *container e-mail.*

major-version = Single digit representing the major version of the format the results of interception are presented in the container e-mail. For each *interception type* the actual major version may be different.
“1” is the current major version for all interception types.

minor-version = Single digit representing the minor version of the format the results of interception are presented in the container e-mail. For each *interception type* the actual minor version may be different.
“0” is the current minor version for all interception types.

6.1.2 Security mechanisms

As lawful interception must be carried out such that no telecommunication party can take notice of it (see article 25 of [2]), a secure delivery channel from the ISP to the LEMF has to be established.

For authentication, integrity and confidentiality reasons, the contents of any delivery message must be signed and encrypted using OpenPGP [7].

For each surveillance case, both the ISP in charge and the LEMF generate a separate pair of public/ private keys when the ISP and the LEMF configure the new surveillance case in their systems used for interception. The key pair created by the LEMF is used for encrypting any delivery message related to the specific surveillance case whereas the key pair created by the ISP is used for signing the respective delivery message. The public keys are exchanged through a secure communication channel such as HI1.

The key pair type is Diffie-Hellman/DSS and its size is 2048/1024 bits. The key pairs expire after 1 year.

The ISP must perform for each container e-mail to be delivered to the LEMF the following signing and encrypting procedure:

1) The MIME entity of the delivery message is created according to the rules described in chapter 7.1 and 8.1.

2) The whole MIME entity, including its body and set of content headers and the boundaries, is signed using the SHA-1 hash algorithm and subsequently encrypted applying the Triple-DES algorithm.

3) The output of the encryption procedure is encoded into ASCII Armor.

4) New MIME content headers are generated:
```
Content-Type: text/plain
Content-Transfer-Encoding: 7bit
```

5) The resulting container e-mail is delivered to the LEMF according to chapter 6.1.

If the ISP or the LEMF assume that a private key has been compromised, the respective party must inform the other one immediately through HI1 and generate a new key pair replacing the compromised one.

6.1.3 Delivery failure

If, for any reason, a container e-mail cannot be delivered to the respective recipient mailbox at the LEMF, it must be resent periodically by the ISP. If undeliverable, a bounce must occur no later than after 7 days. In this case the ISP must contact the SDU through HI1.

The ISP must store any results of interception either until this data is delivered successfully to the LEMF (acknowledgment “250 ok” from the LEMF’s mail system) or for 7 days after a bounce has been reported to the SDU by the ISP.

6.2 Date and time specifications

Any event leading to a result of interception must be combined with the date and time of its creation. This section defines the timestamp syntax to be used and how the interception systems of the ISP must be synchronized with the Swiss time reference.

6.2.1 Timestamp syntax

Timestamps for indicating the date and time of logged events described later are composed according to the following syntax:

```
timestamp =             year month day [SP] hours ":" minutes ":"
                        seconds [SP] zone
```

The components of a timestamp are defined as follows:

`year =` Four-digit representation of the actual year

`month =` Two-digit representation of the actual month, i.e. one of the following values: `"01", "02", "03", ... , "12"`.

`day =` Two-digit representation of the actual day of the month, i.e. one of the following values: `"01", "02", "03"`, ... , number of the days allowed for the specific month.

`hours =` Two-digit representation of the hours of the actual time, i.e. one of the following values: `"00", "01", "02", ... , "23".`

`minutes =` Two-digit representation of the minutes of the actual time, i.e. one of the following values: `"00", "01", "02", ... , "59".`

`seconds =` Two-digit representation of the seconds of the actual time, i.e. one of the following values: `"00", "01", "02", ... , "59".`

`zone =` Offset of the actual time and date representation from Coordinated Universal Time (UTC). A `zone` specification consists of a sign symbol (either `"+"` or `"-"`) followed by a four-digit value. The `"+"` or `"-"` indicates whether the actual time is ahead or behind UTC. The first two digits of the four-digit value indicate the number of hours, the last two digits the number of minutes difference from UTC. For example, Central European Summer Time (CEST) is specified as `"+0200"`.

6.2.2 Synchronization

The precision of the timestamps generated by the ISP's systems with respect to the reference time base must be within +/- 5 seconds.

The following server is defined as the reference time base:

NTP primary (stratum 1) time server: swisstime.ethz.ch

It is proposed to use the Network Time Protocol (NTP) [8] for synchronization, but any other system (e.g. DCF77, GPS, etc.) may also be used as long as the offset from the reference time base remains within the range of +/- 5 seconds.

7 Interception of e-mail contents

The interception of e-mail contents is related to a specific e-mail address serving as target identifier. Any e-mail either received by the target identifier mailbox or sent by the target identifier must be intercepted, copied and forwarded to the LEMF in real-time.

This section defines the data structure and the delivery specifications for intercepting e-mail both for "incoming" and "outgoing" e-mails according to the article 24, section a and d of [2].

7.1 Data structure

Intercepted e-mails with its complete header and body information (including all attachments) must be attached as a *Message/RFC822* MIME-content type to a delivery message. For each intercepted e-mail a separate container e-mail must be created.

7.2 Delivery specifications

The container e-mail must be generated and delivered to the LEMF immediately upon delivery of an e-mail to the target identifier mailbox or upon transfer of an e-mail to the mail-server, respectively.

8 Interception of telecommunication parameters

The interception of communication parameters is based on specific events (e.g. transactions) related to a target identifier as listed below.

Interception type	Event type	Origin of interception data	Possible target identifiers	Remarks
03, 07	Incoming e-mail delivered to mailbox	SMTP envelope log	• e-mail address (recipient)	actual (real-time) and historical data
05, 07	E-mail relayed	SMTP envelope log	• e-mail address (sender)	actual (real-time) and historical data
04	Mailbox access	Mailbox access log	• e-mail address	actual (real-time) data only
06	Internet access service attach and detach	Dial-up log, DHCP-log	• IP-address • login-name • MAC-address • calling number	historical data only

Events are commonly recorded by the ISP in log-files, from which particular data related to the given target identifier must be filtered out, formatted according to the rules described in section 8.1, and sent as container e-mail to the LEMF.

Unsuccessful events, i.e. attempts of relaying an e-mail, accessing the mailbox or establishing an Internet access, must be included into the results of interception if the event is logged and can be correlated to the respective surveillance case.

This section defines the data structure and the delivery specifications for intercepting communications parameters both for real-time and historical data according to the article 24, section b, c, e, f, g, and h of [2].

8.1 Data structure

The results of interception must be presented in a well-formed, valid XML document. The XML document type to be used is determined by the event type. The respective document type definitions are given in the appendix 11.1. A XML document containing the results of interception may consist of none, one or several events of the same type. If data of an event is missing, the respective empty XML element must be provided.

The defined data structures are independent of the results of interceptions being real-time or historical.

The characters "<" and "&" must be substituted by their character entities, i.e. "&#60;" and "&#38;", respectively.

The ISP must process the log-files such that neither the same logged events occur multiple times in one or several container e-mails nor a logged event will be discarded.

The XML documents containing the results of interception must be included inline in a delivery message as *text/plain* MIME-content type with character set *UTF-8* [9].

8.1.1 Data structure for incoming e-mail

For a single logged event for incoming e-mails (XML element `event_incoming-email`) the following XML elements are defined:

`timestamp =` timestamp denoting the date and time the e-mail has been delivered to the mailbox. The format of the timestamp is according to its definition in chapter 6.2.1

`mail-from =` The e-mail address of the sender is displayed as `mailbox` defined in [6]: `local-part "@" domain.`

`rcpt-to =` The e-mail address of the recipient is displayed as `mailbox` defined in [6]: `local-part "@" domain.`

`original-log =` Original event log of the SMTP envelope information. The data must be plain text, UTF-8 encoded.

`ip-address =` The IP-address of the sending unit is given in IPv4 or IPv6 format.

For each recipient of the e-mail, a `rcpt-to` element is created. The document type definition is listed in appendix 11.1.1.

Example: (the original event log is not included)

```
<?xml version="1.0"?>
<!DOCTYPE incoming-email SYSTEM "incoming-email.dtd">
<incoming-email>
  <event_incoming-email>
    <timestamp>20011217 16:25:37 +0100</timestamp>
    <mail-from>xy@example.com</mail-from>
    <rcpt-to>muster@example.net</rcpt-to>
    <rcpt-to>sample@example.org </rcpt-to>
    <original-log>
      ............
      ............
    </original-log>
    <ip-address>192.0.2.110</ip-address>
  </event_incoming-email>
</incoming-email>
```

8.1.2 Data structure for relayed e-mail

For a relayed e-mail event (XML element `event_relayed-email`) two event subtypes are distinguished: "`mail-server_in`" corresponds to receiving an e-mail at the mail server; "`mail-server_out`" corresponds to transferring an e-mail to the next MTA. When an e-mail is sent to several recipients served by different mail-servers, one event of the subtype "`mail-server_in`" and several events of the subtype "`mail-server_out`" are generated. In the case of local delivery, the event of the subtype "`mail-server_out`" may be omitted.

For a single event the following XML elements are defined:

`timestamp =` timestamp denoting date and time of receiving the e-mail at the mail server (for event type "`mail-server_in`") or of transferring the e-mail to the MTA (for event type "`mail-server_out`"). The format of the timestamp is according to its definition in chapter 6.2.1.

`ip-address =` IP-address of the sending unit (for event type "`mail-server_in`") or of the receiving unit (for event type "`mail-server_out`"). The IP-address is given in IPv4 or IPv6 format.

`mail-from`, `rcpt-to`, and `original-log` are used with the same format and meaning as described in chapter 8.1.1. For each recipient of the e-mail, an element `rcpt-to` is created. The document type definition is listed in appendix 11.1.2.

Example: (the original event log is not included)

```
<?xml version="1.0"?>
<!DOCTYPE relayed-email SYSTEM "relayed-email.dtd">
<relayed-email>
  <event_relayed-email subtype="mail-server_in">
    <timestamp>20011217 16:25:37 +0100</timestamp>
    <mail-from>xy@example.com</mail-from>
    <rcpt-to>muster@example.net</rcpt-to>
    <rcpt-to>sample@example.org</rcpt-to>
    <original-log>
      ............
    </original-log>
    <ip-address>192.0.2.110</ip-address>
  </event_relayed-email>
  <event_relayed-email subtype="mail-server_out">
    <timestamp>20011217 16:34:14 +0100</timestamp>
    <mail-from>xy@example.com</mail-from>
    <rcpt-to>muster@example.net</rcpt-to>
    <original-log>
    ............
    </original-log>
    <ip-address>192.0.2.24</ip-address>
  </event_relayed-email>
  <event_relayed-email subtype="mail-server_out">
```

```
    <timestamp>20011217 16:38:37 +0100</timestamp>
    <mail-from>xy@example.com</mail-from>
    <rcpt-to>sample@example.org </rcpt-to>
    <original-log>
      ............
    </original-log>
    <ip-address>192.0.2.178</ip-address>
  </event_relayed-email>
</relayed-email>
```

8.1.3 Data structure for mailbox access

For a single mailbox access event (XML element `event_mailbox-access`) the following XML elements are defined:

`timestamp =` timestamp denoting date and time the mailbox has been accessed. The format of the timestamp is according to its definition in chapter 6.2.1.

`ip-address =` IP-address of the accessing unit. The IP-address is given in IPv4 or IPv6 format.

`protocol =` Protocol used for accessing the mailbox. Common values are “POP3” and “IMAP4”. For proprietary protocols the name of the software manufacturer must be indicated, e.g. “LOTUS” or “HTTP”.

The document type definitions is listed in appendix 11.1.3.

Example:

```
<?xml version="1.0"?>
<!DOCTYPE mailbox-access SYSTEM "mailbox-access.dtd">
<mailbox-access>
  <event_mailbox-access>
    <timestamp>20011217 16:25:37 +0100</timestamp>
    <ip-address>192.0.2.110</ip-address>
    <protocol>POP3</protocol>
  </event_mailbox-access>
  <event_mailbox-access>
    <timestamp>20011217 16:34:14 +0100</timestamp>
    <ip-address>192.0.2.120</ip-address>
    <protocol>LOTUS</protocol>
  </event_mailbox-access>
</mailbox-access>
```

8.1.4 Data structure for Internet access

For Internet access the service attach and detach events are combined to a single logged event (XML element `event_internet-access`). The following XML elements are defined:

`start-time =` timestamp denoting the date and time a modem session is initiated (login at the ISP) or an IP-address is allocated. The format of the timestamp is according to its definition in chapter 6.2.1.

`stop-time =` timestamp denoting the date and time a modem session is closed or an IP-address is released. The format of the timestamp is according to its definition in chapter 6.2.1.

`ip-address =` IP-address of the accessing unit. The IP-address is given in IPv4 or IPv6 format. The IP-address may represent the target identifier.

`access =` Identifier of the accessing unit; its meaning depends on the access type which must be provided as an attribute to the element. The `access` element can serve as target identifier.

Access type	Contents of the element `<access>`
`"PSTN"` for analog or digital modem/router over PSTN	Calling number in CLI syntax
`"Cable"` for cable modem/ router	MAC-address of the accessing unit: The MAC-address is presented as a hexadecimal value (0 - F).
`"xDSL"` for xDSL modem/ router	None
`"LAN"` for direct access (incl. WLAN)	MAC-address of the accessing unit. The MAC-address is presented as a hexadecimal value (0 – F).
`"Mobile_PS"` for mobile packet switched service such as GPRS, UMTS	Calling number in CLI syntax

The format of the *calling number* is either national or international. Local calling numbers must not be used. For the international format there are two alternatives: The country code is either preceded by `"00"` or by `"+"`[1].

`login-name =` login-name for the accessed service. The login-name may serve as target identifier.

The document type definitions are listed in appendix 11.1.4.

When an Internet service attach or detach timestamp is not within the period of time specified in the inquiry the respective element need not be provided.

[1] In some cases of international calls, the country ID is not delivered by the network operators of the foreign country.

Example:

```
<?xml version=″1.0″?>
<!DOCTYPE internet-access SYSTEM “internet-access.dtd″>
<internet-access>
  <event_internet-access>
    <start-time>20011217 16:25:37 +0100</start-time>
    <stop-time>20011217 16:35:34 +0100</stop-time>
    <ip-address>192.0.2.110</ip-address>
    <access type=″PSTN″>013059554</access>
    <login-name>mighty_dragon</login-name>
  </event_internet-access >
</internet-access>
```

8.2 Delivery period

8.2.1 Actual data fetched in real-time

The ISP must deliver any list of intercepted telecommunication parameters as container e-mails at fixed periods. A respective container e-mail must be sent to the LEMF even if no log events have occurred since the last list was forwarded. The interval between two consecutive container e-mails transferred to the LEMF must not exceed 24 hours and must not be less than 30 minutes. For each interception type, a different period may be defined by the ISP.

8.2.2 Historical data

The data has basically to be delivered as soon as possible. The following deadlines for the delivery of the requested data to the SDU hold:

1) The historical data for the time period up to one month is to be delivered within one working day to the DBA.
2) The historical data for the time period from one month up to six months is to be delivered within five working days to the DBA.

If the delivery cannot be met as stated in 1) and 2), the ISP must contact the SDU in advance.

9 Test requirements

Each ISP must maintain a test e-mail account which is constantly monitored for incoming e-mails (interception type 01 according to chapter 6.1.1). The LI test e-mail address must have the following format:

```
LI-test-address = test-LIID ″@″ ISP-domain
```

The variables are defined as follows:

`test-LIID =` Unique identifier specifying the test account. It has the same format as the parameter LIID indicating a particular surveillance case.

`ISP-domain =` refers to the domain-name of the ISP

The test e-mail account allows the LEMF to check its connection to the ISP since test mails sent by the LEMF to the LI test e-mail address must be delivered immediately to the LEMF as a container e-mail. The SDU may install a repeated test mail sending process in order to periodically check the connection to the ISP and the correct processing and forwarding of incoming e-mails to the LEMF.

The test must be considered as a dummy surveillance case with a running period of 1 year. The SDU provides for each ISP the specific *test LIID.* All rules for delivering interception results of incoming e-mails described above apply.

10 Final Provisions

10.1 Temporary arrangement

According to article 36 of [2], the ISPs must deliver the results of interception to the LEMF starting from 1st April 2003. Up to that point in time, they must provide information according to article 14 of [1] and existing communication parameters of e-mail traffic.

It is planned to run a test phase starting in the middle of January 2003. The SDU will provide a test schedule defining a series of test windows by the end of November 2002. Within a specific test window, the correct interception as well as the processing and forwarding of the results of interception of all types of interception (see chapter 6.1.1) by the respective ISP is checked. The test program, which will be set up by the SDU and the ISPs, will be provided by the SDU by the end of November 2002.

Each ISP reports its *ISP-domain* name to be used with lawful interception to the SDU by the end of November 2002.

10.2 Further provisions

The chapter will be delivered in a later version of the document.

3003 Bern, 2. April 2002

Dienst für Besondere Aufgaben
Der Verantwortliche:

Adrien de Werra

11 Appendix

11.1 Document type definitions

This chapter contains the XML document type definition (DTD) associated to the XML data to be generated for the interception of telecommunication parameters (see section 8).

11.1.1 Incoming e-mail

```
<!-- incoming-email.dtd -->
<!ELEMENT incoming-email (event*)>
  <!ELEMENT event_incoming-email (timestamp, mail-from, rcpt-to+, original-log, ip-
address)>
    <!ELEMENT timestamp (#PCDATA)>
    <!ELEMENT mail-from (#PCDATA)>
    <!ELEMENT rcpt-to (#PCDATA)>
    <!ELEMENT original-log (#PCDATA)>
    <!ELEMENT ip-address (#PCDATA)>
```

11.1.2 Relayed e-mail

```
<!-- relayed-email.dtd -->
<!ELEMENT relayed-email (event*)>
  <!ELEMENT event_relayed-email (timestamp, mail-from, rcpt-to+, original-log, ip-
address)>
    <!ATTLIST event_relayed-email subtype (mail-server_in|mail-server_out) #REQUIRED>
    <!ELEMENT timestamp (#PCDATA)>
    <!ELEMENT mail-from (#PCDATA)>
    <!ELEMENT rcpt-to (#PCDATA)>
    <!ELEMENT original-log (#PCDATA)>
    <!ELEMENT ip-address (#PCDATA)>
```

11.1.3 Mailbox access

```
<!-- mailbox-access.dtd -->
<!ELEMENT mailbox-access (event*)>
<!ELEMENT event_mailbox-access (timestamp, ip-address, protocol)>
    <!ELEMENT timestamp (#PCDATA)>
    <!ELEMENT ip-address (#PCDATA)>
    <!ELEMENT protocol (#PCDATA)>
```

11.1.4 Internet access

```
<!-- internet-access.dtd --> Internet access
<!ELEMENT internet-access (event*)>
  <!ELEMENT event_internet-access (start-time?, stop-time?, ip-address, access,
login-name)>
    <!ELEMENT start-time (#PCDATA)>
    <!ELEMENT stop-time (#PCDATA)>
    <!ELEMENT ip-address (#PCDATA)>
    <!ELEMENT access (#PCDATA)>
      <!ATTLIST access type (PSTN|Cable|xDSL|LAN|Mobile_PS) #REQUIRED>
```

```
<!ELEMENT login-name (#PCDATA)>
```