Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP

**IT Service Center ISC-FDJP**
Post and Telecommunications Surveillance Service

# Lawful Interception of telecommunication traffic

## Organisational and administrative requirements (OAR)

Date: November 9, 2012

Version: 2.14

Address and contact:

IT Service Centre ISC-FDJP
Post and Telecommunications Surveillance Service
PTSS
Fellerstrasse 15
3003 Berne, Switzerland

Contact: https://www.li.admin.ch/

**Lawful Interception of telecommunication traffic**

Contents

# Document History

| Version | Date | Status | Remarks |
|---|---|---|---|
| 0.1 | 06.05.02 | Draft | First draft |
| 0.2 | 31.05.02 | Draft | • Work Items updated<br>• Removal of exception handling chapter |
| 0.3 | 21.06.02 | Draft | • Work Items updated |
| 0.4 | 12.07.02 | Final draft | • Work Items updated<br>• Removal of “Work Item” structure |
| 1.0 | 16.08.02 | Published Version | |
| 2.0 | 01.01.08 | Published version | • Addendum 1-4 included. |
| 2.01 | 15.02. 09 | Draft | • Appendices corrected (Syntax correction) |
| 2.10 | 19.05. 09 | Draft | • Add-ons for broadband Internet access surveillance |
| 2.11 | 01.08.09 | Enacted version | |
| 2.12 | 15.08.11 | Draft | • Editorial changes for alignment to TR TS v2.0 |
| 2.13 | 23.11.11 | Published and enacted version | • Editorial changes in accordance with VÜPF |
| 2.14 | 09.11.12 | Published and enacted version | • Editorial changes and adaptation of execution times |

# 1. Scope

This document provides the organisational and administrative requirements for interfacing the telecommunication service providers with the governmental PTSS, concerning the issues of lawful interception.

The specifications made in this document are based on the following documents:

- The legal provisions concerning lawful interception in Switzerland, as denoted in [1] and [2].
- The technical specifications for delivery of results of interception for fix and mobile circuit switched services as well as fix and mobile packet switched services as in [16].

Accordingly, the requirements specified in this document apply to the interfaces referred to in these documents above.

Furthermore this document draws on ideas and concepts from the respective ETSI documents as well, which include [9], [10], [15], [17], [18], [19], [20], [21], [22] and [23]. References to the respective ETSI specifications are made where applicable.

The requirements defined in this document apply to all providers of fix and mobile circuit switched telecommunication or fix and mobile internet access, as in [1] and [2].

# 2. References

| | | |
|---|---|---|
| [1] | SR 780.1 | Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 06. Oktober 2000 |
| [2] | SR 780.11 | Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) vom 31. Oktober 2001 |
| [3] | VOID | VOID |
| [4] | VOID | VOID |
| [5] | [CCIS] | Call Center Information system (CCIS); Regulatorische Aspekte |
| [6] | SR 120.4 | Verordnung über die Personensicherheitsprüfungen (PSPV) vom 19. Dezember 2001 |
| [7] | SR 235.1 | Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 |
| [8] | VOID | VOID |
| [9] | ETSI TS 101 331 | Telecommunication security; Lawful interception (LI); Requirements of Law Enforcement Agencies |
| [10] | ETSI ES 201 158 | Telecommunication security; Lawful interception (LI); Requirements for network functions |
| [11] | SR 784.101.113 / 1.7 | Technische und administrative Vorschriften betreffend die Identifikation des anrufenden Anschlusses (BAKOM/OFCOM) |
| [12] | VOID | VOID |
| [13] | SR 780.115.1 | Verordnung vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs |
| [14] | VOID | VOID |
| [15] | ETSI TS 102 232-3 | Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services |
| [16] | TR TS | Guidelines for Lawful Interception of Telecommunications Traffic; Technical Requirements for Telecommunication Surveillance. |
| [17] | ETSI TS 101 671 | Telecommunication security; Lawful interception (LI); Handover interface for the lawful interception of telecommunication traffic |
| [18] | ETSI TS 102 232-1 | Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery |
| [19] | ETSI TS 102 232-2 | Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for Email services |
| [20] | ETSI TS 102 232-4 | Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services |
| [21] | ETSI TS 102 232-5 | Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services |
| [22] | ETSI TS 102 232-6 | Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services |

**Lawful Interception of telecommunication traffic**

| | | |
|---|---|---|
| [23] | ETSI TS 133 108 | Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) |
| [24] | RFC 4880 | OpenPGP Message Format, 2007 |

# 3. Abbreviations

| | |
|---|---|
| BA | Basic Access interface |
| CC | Content of Communication |
| CCIS | Call Center Information system |
| CLIP | Calling Line Identification Presentation |
| CS | Circuit Switched |
| CSP | Communications Service Provider |
| CUG | Closed User Group |
| DDI | Direct Dialling In |
| ETSI | European Telecommunication Standards Institute |
| FTP | File Transfer Protocol |
| GSM | Global System for Mobile communications |
| HI | Handover Interface |
| ICCID | Integrated Circuit Card Identifier |
| IP | Internet Protocol |
| IRI | Intercept Related Information |
| IIF | Internal Interception Function |
| IMEI | International Mobile station Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| ISDN | Integrated Services Digital Network |
| ISP | Internet Service Provider |
| LAN | Local Area Network |
| LEA | Law Enforcement Agency |
| LEMF | Law Enforcement Monitoring Facility |
| LI | Lawful Interception |
| LIID | Lawful Interception Identifier |
| MAC | Media Access Control |
| MF | Mediation Function |
| MSISDN | Mobile Subscriber ISDN number |
| MSN | Multiple Subscriber Number |
| MVNO | Mobile Virtual Network Operator |
| PA | Primary Access interface |
| PGP | Pretty Good Privacy |
| POTS | Plain Old Telephony System |
| PRS | Premium Rate Service |
| PS | Packet Switched |
| PSTN | Public Switched Telephone Network |
| PTSS | Post and Telecommunications Surveillance Service |
| SIM | Subscriber Identity Module |
| SMS | Short Messages Service |
| SN | Subscriber Number |
| SPOC | Single Point Of Contact |
| TSP | Telecommunications Service Provider |
| TTI | Test Target Identity |
| UMTS | Universal Mobile Telecommunications System |
| UUS | User-User Signalling |
| VNO | Virtual Network Operator |
| VoIP | Voice over IP |
| WLAN | Wireless Local Area Network |
| xDSL | Digital subscriber line (x stands for various types) |

# 4. Definitions

| | |
|---|---|
| *Handover interface* | See [17], clause 3 |
| *Intercept related information* | See [17], clause 3 |
| *Interception order* | An order sent from the PTSS to a CSP for setting up an interception activity |
| *Law Enforcement Monitoring Facility* | See [17], clause 3<br>This is at the same time the data center of the PTSS |
| *Mediation function* | See [17], clause 3 |
| *PTSS* | Post and Telecommunications Surveillance Service<br>The governmental authority responsible for the collection and processing of all intercept data in Switzerland |
| *Surveillance order* | An order sent from the LEA to the PTSS to initiate an interception activity |
| *Target identity* | See [17], clause 3 |
| *Target service* | See [17], clause 3 |
| *Communications Service Provider* | The legal entity providing telecommunications services as defined in [1] art.1 section.2 |

# 5. Responsibilities

The responsibilities for interception are defined as following:

1. A CSP being ordered with an interception order or information request is responsible for the complete, correct and timely delivery of interception results or information responses to the PTSS, in compliance with the requirements in [2] and [16] for telecommunication service data being under control of the CSP. Subcontractors are obliged to assist the CSP in the fulfilment of the above mentioned duties.

   A “subcontractor” is defined hereafter as any third party CSP having a contractual agreement with the first party CSP to provide telecommunication/internet services on the first party CSP’s behalf in Switzerland.
2. A CSP assigned with an interception order is not responsible for delivery or interpretation of interception data accruing beyond its own or its subcontractors’ network/systems.
3. CSPs which provide for their subscribers a VoIP-solution that uses an E.164-Number, derived from the Federal Office of Communications numbering-range, as an addressing element, are obliged to intercept the complete real-time traffic based on the technical requirements defined in [16]. In addition the CSPs are also obliged to store and deliver the complete historical data based on the technical requirements defined in [16], for the target represented by this E.164-Number. The delivery of the interception results correspond at this stage exactly to the interfaces described in [16], all requirements of [16] apply.

# 6. Interception procedure

This section defines the interception procedures for delivery of real-time and historical data.

## 6.1. Interception types

This section defines the types of interception data that may be ordered from CSPs.

### 6.1.1. Circuit switched services

The following real-time interception types are defined according to [2] (this includes also VoIP-interception for CS_1 and CS_3):

| Type | Explanation |
|---|---|
| CS_1 | Content of Communication (CC), as defined in [2], art. 16 letter a. This includes CC as defined in [16]: Voice, data, fax and voice-mail. These services form one package for an interception order, i.e. it is not possible to split this type into only a subset of these services. Only the respective services for the concerning target identity must be intercepted. |
| CS_2 | Location information for mobile targets, as defined in [2], art. 16 letter b. |
| CS_3 | Intercept Related Information (IRI), as defined in [2], art. 16 letter c. This includes IRI as defined in [16], including UUS and SMS. The provision of IRI forms one package of interception order, i.e. it is not possible to split this type into only a subset of IRI information (e.g. it is not possible to order only the addressing elements of the underlying call). |

**Table 1: Real-time interception types for circuit switched services**

The following combinations are possible when combining real-time circuit switched interception types in a single interception order:

1. CS_3
2. CS_2 and CS_3
3. CS_1 and CS_3
4. CS_1 and CS_2 and CS_3

The following retroactive and network analysis interception types are defined according to [2] (this includes also VoIP-interception for CS_4 at this stage):

| Type | Explanation |
|---|---|
| CS_4 | Historical Data, as defined in [2], art. 16 letter d. The parameters contained in article 16 letter d are to be ordered as a package and cannot be split into further subsets of parameters. The technical details of the unitary format of the historical data and the delivery mechanisms for the transmission of this data to the LEMF are defined in [16]. |
| CS_5 | Network analysis by the CSP in preparation of a search by cell coverage, as defined in [2] art. 16 letter e. PTSS provides a defined period of time and the geographical coordinates that allow the CSP to determine the Cell-IDs of the cell coverage area which is relevant for the search. As a result the CSP provides a list of these Cell-IDs to the PTSS. |
| CS_6 | Search by cell coverage area, as defined in [2] art. 16 letter e. The PTSS provides a defined period of time of maximum 2 hours and one Cell-ID that is to be used for the search. As result the CSP provides the parameters of all successful communications carried by the cell during the defined period of time. The delivery mechanisms for the transmission of this data to the LEMF are defined in [16]. |
| CS_7 | Network analysis by the LEA in preparation of a search by cell coverage area, as defined in [2] art. 16 letter e. PTSS provides a list with reference call details to the CSP. The CSP identifies the Cell-IDs used by these reference calls and provides a list of these Cell-IDs to the PTSS. |

**Table 2: Retroactive and network analysis interception types for circuit switched services**

**Lawful Interception of telecommunication traffic**

No combinations of retroactive and network analysis interception types are allowed.

The following Figure 1 describes elaborately the phases and parameters related to the interception types CS_5, CS_6 and CS_7 as defined in Table 2:

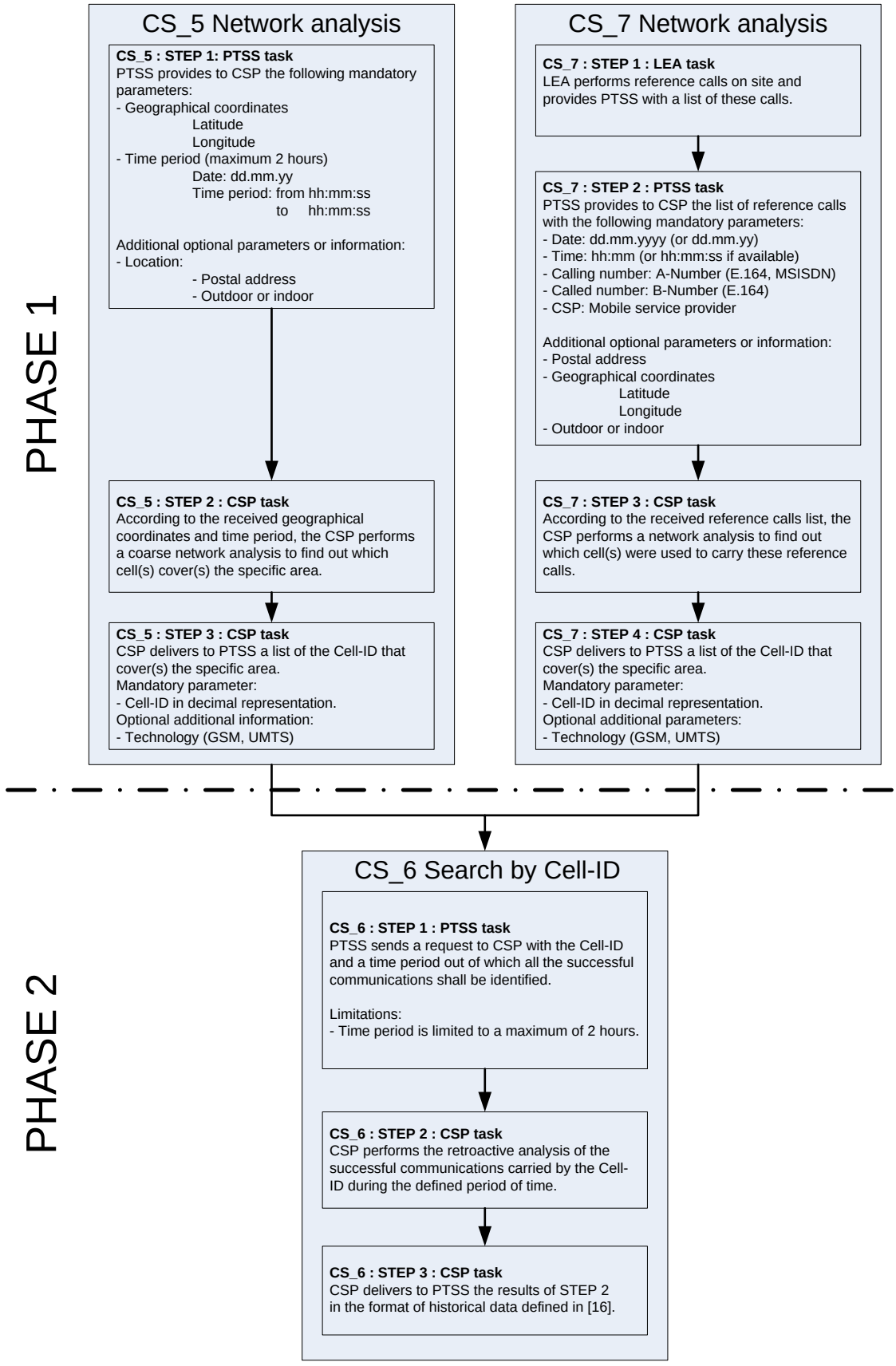


**Figure 1: Description of the phases for interception types CS_5, CS_6 and CS_7**

### 6.1.2. Packet switched services

The following real-time interception types are defined and can be ordered for packet switched services as in [2]:

| Type | Explanation |
|---|---|
| PS_1 | Real-time delivery of the complete communication of an internet access as defined in [2] art. 24a letter a. This includes the Content of Communication (CC) and the Intercept Related Information (IRI) of the internet access. |
| PS_2 | Provisioning and simultaneous or periodical transmission of communication parameters as defined in [2] art. 24a letter b. This includes Intercept Related Information (IRI) of the internet access. The provision of IRI forms one package of interception order, i.e. it is not possible to split this type into only a subset of IRI information. |
| PS_3 | Real-time delivery of the complete communication of an application as defined in [2] art. 24a letter c. This includes content of communication (CC) and the intercept related information (IRI) of the application. |
| PS_4 | Provisioning and simultaneous or periodical transmission of communication parameters as in [2] art. 24a letter d. This includes Intercept Related Information (IRI) of the application. The provision of IRI forms one package of interception order, i.e. it is not possible to split this type into only a subset of IRI information. |

**Table 3: Real-time interception types for packet switched services**

Note: PS_2 can only be ordered for mobile IP access interception according to [2] art. 24 letter c

No combinations of real-time interception types for packet-switched services are allowed.

The following retroactive interception types are defined and can be ordered for packet switched services as in [2]:

| Type | Explanation |
|---|---|
| PS_5 | Historical Data relating to an internet access as defined in [2] art. 24b letter a. The parameters listed in that paragraph must be ordered as a package and cannot be split into further subsets of parameters. |
| PS_6 | Historical Data relating to an asynchronous messaging application (email) as defined in [2] art. 24b letter b. The parameters listed in that paragraph must be ordered as a package and cannot be split into further subsets of parameters. |

**Table 4: Retroactive interception types for packet switched services**

No combinations of retroactive interception types for packet-switched services are allowed.

### 6.1.3. Emergency Paging

Based on [2] art. 16a the interception types for emergency paging are defined as follows:

| | |
|---|---|
| N_1 | **Location Determination:**<br>Location Determination N_1 identifies the latest active position of a mobile phone. Due to its urgency, the Location Determination is always performed manually. Normally the LEA will receive the coordinates (X/Y) of the latest active position as a result of this interception type. |

| | |
|---|---|
| N_2 | **Real-time Location Determination:**<br>The Real-time Location Determination N_2 is performed in the same way as N_1. For CSPs which are already connected to the LEMF, N_2 interceptions can only be activated with the LEMF. In that case, the latest location information and communication related information is received and stored in the LEMF. It is the LEA's responsibility to ensure they have access to the LEMF. For the technical feasibility of N_2 interceptions, CS_2 and CS_3 have to be activated preliminary on the LEMF. |
| N_3 | **Historical Location Determination**<br>For Historical Location Determination N_3, target identification and communication related information is delivered. N_3 is applied to determine locations which date back 24 hours and more. N_3 can only be activated during normal office hours. |

**Table 5: Emergency paging interception types**

## 6.2. Activation bases

The activation bases for interception orders, i.e. the definition of the possible target identities, are listed in [16]:

1. Circuit switched services:
    a. Fixnet-call-number
    b. MSISDN
    c. IMEI
    d. IMSI
    e. Voice-mail identifier: In case the ordered interception type is a “CC” and the target identity has a voice-mail service attached, the interception of the voice-mail communication must be activated as well.
2. Packet switched services:
    a. Identifier of the associated telephone line
    b. E-mail address
    c. Permanently assigned IP-address
    d. Login-name
    e. MAC-address
    f. Calling number
    g. User identifier assigned to the internet access route
    h. xDSL access according to ETSI TS 102 232-3 [15] section 5.1.2
    i. Cable modem access according to ETSI TS 102 232-3 [15] section 5.1.3
    j. WLAN access according to ETSI TS 102 232-3 [15] section 5.1.4
    k. LAN access
    l. Other designation for the transmission route
    m. Undefined access according to ETSI TS 102 232-3 [15] section 8: The use of this access must be approved by the PTSS.

## 6.3. Recipients of interception orders

### 6.3.1. Assigning target identities to CSPs

Upon reception of a surveillance order from the LEA the PTSS will contact the appropriate CSP which has to carry out the respective interception activity.

### 6.3.2. Multiple CSP involvement

In case more than one CSP is engaged in the interception of a single target identity, the following principles apply:

1. The CSP that was selected as defined in chapter 6.3.1 is regarded as the SPOC (Single Point Of Contact) to the PTSS. This means in particular, that the selected CSP will delegate interception requests to subcontractors if necessary in order to fully comply with the requirements of delivering the results of lawful interception as defined in [2], [16] with reference to the responsibilities defined in chapter 5.
2. The PTSS may submit an information request, in compliance with [2] and as specified in chapter 7, to the selected CSP in order to obtain officially stored (static) information from other CSPs the target is subscribed to (e.g. through pre-selection contracts).

## 6.4. Activation procedure

The activation procedure includes three steps:

1. The PTSS sends an interception order to the CSP
2. The CSP initiates the required interception activity
3. The CSP sends confirmation of the activation to the PTSS

### 6.4.1. Step one – Initiation

When requesting the activation of an interception activity, the PTSS sends an interception order to the selected CSP, providing the following information:

1. Form header

   This includes several administrative information elements, such as:

   a. CSP name
   b. Priority: This denotes the priority level assigned to this interception order. The priority levels are defined in chapters 9.2.1 and 9.2.2. In case the priority level is set to “required by time and date” (see chapter 9.2.1.1), the form states when (exact date and time) the activation has to be triggered.
   c. File number: File number of form for storage purposes
   d. Lawful Interception Identifier (LIID): Unique identifier of the interception order, consisting of 15 digits (the details are described in [16])
   e. Reference name: Identifier for referencing the surveillance order
   f. Date: Date of commissioning of the interception order

2. Target identity

   This contains the target identity of the interception, as defined in chapter 6.2.

3. Interception types

   This contains the various interception types as defined in chapter 6.1 that are delivered to the LEMF.

4. Period of interception

   This denotes the time frame for the Historical Data Interception, i.e. start and end date and time of the intercepted data.

5. Delivery address

   This denotes the destination address for the delivery of the intercepted data (Historical Data only).

6. PTSS signature

   Signature of the employee charged with completing and sending the interception order form.

Interception order forms are available in three Swiss national languages (German, French and Italian). The CSP chooses one of the above mentioned languages.

### 6.4.2. Step two – Activation

This step is part of the CSP’s internal processes.
Note: For Historical Data, activation denotes the provision of the data derived from the destination address.

If any of the interception types required in the interception order cannot be activated, the CSP reports this immediately to the PTSS (see also chapter 8). The official confirmation is carried out as described in chapter 6.4.3.

### 6.4.3. Step three - Confirmation

Upon successful technical activation of the surveillance case, the CSP confirms the activation to the PTSS both administratively and technically.

#### 6.4.3.1. Administrative confirmation

The CSP provides to the PTSS the following information:

1. Form header

   This includes the administrative information elements, such as:
   a. CSP name
   b. File number: Identical to the corresponding interception order
   c. LIID: Identical to the corresponding interception order
   d. Reference name: Identical to the corresponding interception order
   e. Date: Date of confirmed activation
2. Target identity

   Target identity which the interception is based on.
3. Interception types activated

   If certain interception types required in the interception order could not be activated, the reason must be stated.
4. Date and time of activation (respectively of data provision for Historical Data Interception)
5. Name of CSP contact person

The PTSS provides a template of the confirmation form to be used by the CSP.

#### 6.4.3.2. Technical confirmation

In addition to the official administrative confirmation, the PTSS also needs to verify the proper functioning of the technical interfaces as defined in [16][1].
For this purpose, the respective CSP sends *to the LEMF* upon successful activation of the interception:

1. For e-mail services according to TR TS [16] section 12.2.2 (Swiss proprietary mechanism and procedure): A confirmation e-mail (whereby the interception type for administrative e-mails is inserted in the subject field, see [16]). The body of the e-mail must contain the date and time of the underlying activation. The date and time shall have the format of the time-stamp as defined in [16] section 6.2.1. The public CSP key to be used for the underlying interception activity must be sent as an attachment to this e-mail. The confirmation e-mail (body and attachment) must be encrypted by the public PTSS key to be used for the underlying interception activity (see chapter 8).
2. If the data type `HI1-Operation` is not available a confirmation e-mail (encrypted) or a fax with the activation details must be sent to the PTSS.
3. For all other cases: A confirmation notification in accordance with [16].

## 6.5. Modification procedures

The modification procedure includes three steps:

1. The PTSS sends a modification order to the CSP
2. The CSP modifies the respective interception functionality
3. The CSP sends a confirmation of the modifications to the PTSS

### 6.5.1. Step one – Initiation

When requesting the modification of an existing interception functionality, the PTSS sends a modification order to the involved CSP, providing the following information:

[1] In case of multiple CSP involvement as in chapter 6.3.2, the technical confirmation must be carried out by the *CSP owning the technical interface facilities*.

1. Form header

   This includes several administrative information elements, such as:
   a. CSP name
   b. Priority: This describes the priority level assigned to this modification order. The priority levels are defined in chapter 9.2.1.1. In case the priority level is set to “required by time and date” (see chapter 9.2.1.1), the form states when (exact date and time) the modification has to be implemented.
   c. File number (identical to the corresponding interception order)
   d. LIID (identical to the corresponding interception order)
   e. Reference name (identical to the corresponding interception order)
   f. Date: Date of modification order
2. Target identity

   The target identity of the interception, as defined in chapter 6.2
3. Interception modification

   Modification of the interception type combination that needs to be delivered to the LEMF, refer to chapter 6.1. The modification order denotes the addition or removal of any of the interception types as defined in chapter 6.1.
4. Signature by the respective employee issuing the order on behalf of the PTSS

Modification order forms are available in three Swiss national languages (German, French and Italian). The CSP chooses one of the above mentioned languages.

### 6.5.2. Step two – Modification

This step is part of the CSP’s internal processes.
If any of the required modifications requested in the modification order cannot be carried out, the CSP reports this immediately to the PTSS (see also chapter 8). The official confirmation is carried out as described in chapter 6.5.3:

### 6.5.3. Step three - Confirmation

Upon successful modification, the CSP confirms the modification to the PTSS, providing the following information:

1. CSP name
2. Form header

   This includes the administrative information elements, such as:
   a. File number: Identical to the corresponding modification order
   b. LIID: Identical to the corresponding modification order
   c. Reference name: Identical to the corresponding modification order
   d. Date: Date of sending of confirmation
3. Target identity

   The target identity of the interception.
4. Interception modification

   If certain modifications required in the interception order could not be carried out, the reason therefore must be stated.
5. Date and time of modification
6. Name of the CSP’s contact person

The PTSS provides a template of the confirmation form to be used by the CSP.

There is no technical confirmation for a modification order.

## 6.6. Deactivation procedures

This procedure is only applicable to Real Time Interception orders (not applicable to interception orders for Historical Data or for Information Requests). The deactivation procedure consists of three steps:

1. The PTSS sends a deactivation order to the CSP
2. The CSP deactivates the interception activity
3. The CSP sends a confirmation of the deactivation to the PTSS

### 6.6.1. Step one – Initiation

Deactivation orders are only sent within operating hours. When requesting the deactivation of an interception activity, the PTSS sends a deactivation order to the involved CSP, providing the following information:

1. Form header

   This includes several administrative information elements, such as:
   a. CSP name
   b. File number (identical to the corresponding interception order)
   c. LIID (identical to the corresponding interception order)
   d. Reference name (identical to the corresponding interception order)
   e. Date: Date of commissioning of deactivation order
2. Target identity

   Target identity of the interception, as defined in chapter 6.2.
3. Date and time of deactivation
4. Signature by the respective employee issuing the order on behalf of the PTSS

Deactivation order forms are available in three Swiss national languages (German, French and Italian) as well as in English. The CSP chooses one of the above mentioned languages.

### 6.6.2. Step two – Deactivation

This step is part of the CSP's internal processes.

### 6.6.3. Step three - Confirmation

Upon successful deactivation, the CSP confirms the deactivation to the PTSS, providing the following information:

1. Form header

   This includes the administrative information elements, such as:
   a. CSP name
   b. File number: Identical to the corresponding deactivation order
   c. LIID: Identical to the corresponding deactivation order
   d. Reference name: Identical to the corresponding deactivation order
   e. Date: Date of sending of confirmation
2. Target identity

   Target identity of the interception, as defined in chapter 6.2
3. Date and time of deactivation
4. Name of CSP's contact person

The PTSS provides a template of the confirmation form to be used by the CSP.
There is no technical confirmation for a deactivation order.

## 6.7. Cancellation of orders

The PTSS may cancel an interception order that has already been sent to the CSP, as long as the PTSS has not yet received the administrative confirmation of the activation. The administrative confirmation only has to be sent to the PTSS, when the surveillance is activated in the network (in case of real-time interceptions). This relates to cancellations of activations, modifications or deactivations of real-time interception orders, as well as to cancellations of activations of historical data interception orders. Upon cancellation of an interception order, the CSP is entitled to remuneration.

### 6.7.1. Step one - Initiation

The PTSS sends the cancellation order to the CSP, providing the following information within the cancellation form:

1. Form header

   This includes several administrative information elements, such as:
   a. CSP name
   b. File number
   c. LIID (identical to the corresponding interception order)
   d. Reference name (identical to the corresponding interception order)
   e. Date: Date and time of sending of the cancellation form
2. Target identity

   Target identity of the interception, as defined in chapter 6.2
3. Cancelled file number (same as the one of the underlying ordered interception activity)
4. Description: Short description of the cancellation order
5. Signature by the respective employee issuing the order on behalf of the PTSS

Cancellation forms are available in three Swiss national languages (German, French and Italian). The CSP chooses one of the above mentioned languages.

### 6.7.2. Step two - Confirmation

The CSP confirms the cancellation to the PTSS, providing the following information within the confirmation form:

1. Form header

   This includes the administrative information elements, such as:
   a. CSP name
   b. File number (identical to the corresponding interception order)
   c. LIID (identical to the corresponding interception order)
   d. Reference name (identical to the corresponding interception order)
   e. Date: Date and time of sending of the confirmation
2. Target identity

   Target identity of the interception, as defined in chapter 6.2
3. Name of CSP’s contact person

The PTSS provides a template of the confirmation form to be used by the CSP.

# 7. Information requests

Information requests are divided into two categories:

1. Requests relating to basic subscriber information. This category is defined and specified in [5].
2. More detailed requests relating to technical and administrative queries. There are four categories defined:

| Category | Information type | Examples |
|---|---|---|
| A_1 | *Target identity information* | MAC-address, PUK, IMSI |
| A_2 | *Subscriber information* | Contract copies, billing information |
| A_3 | *Network information* | Assumed coverage maps |
| A_4 | *Services information* | Fixed redirections, virtual numbers |

**Table 6: Information types**

In the annex (chapter 14.1), the standard combinations of known and requested information are given. Note that this list is not exhaustive but rather represents the combined queries which have been requested in the past. For further information requests which are not covered in chapter 14.1, the PTSS will agree on a case-by-case basis with the respective CSP on the conditions of delivery.

## 7.1. Information request procedure

The information request procedure includes three steps:

1. Sending of information request
2. Responding to the information request
3. Confirmation of the information delivery

### 7.1.1. Request

The PTSS sends an information request to the responsible CSP, providing the following information:

1. Form header

   This includes several administrative information elements, such as:
   a. CSP name
   b. Priority: This denotes the priority level assigned to this information request. The priority levels are defined in chapter 9.2.2.
   c. File number
   d. Order number: Unique identifier of a information request
   e. Reference name
   f. Date: Date of sending of information request
2. Information type category: This is described in Table 6
3. Known information
4. Requested information
5. Delivery address

   This denotes the destination address for delivery of the information response.
6. Signature by the responsible employee issuing the order on behalf of the PTSS

Information request forms are available in three Swiss national languages (German, French and Italian). The CSP chooses one of the above mentioned languages.

### 7.1.2. Response

This step is part of the CSP's internal processes.
The response is being sent to the destination address included in the information request form.

### 7.1.3. Confirmation

The CSP sends an information confirmation to the PTSS, providing the following information:

1. Form header

   This includes several administrative information elements, such as:
   a. CSP name
   b. File number (identical to the corresponding information request)
   c. Order number (identical to the corresponding information request)
   d. Reference name (identical to the corresponding information request)
   e. Date: Date of sending of information confirmation
2. Date of sending of response
3. Transmission medium used for response
4. Name of CSP's contact person

The PTSS provides a template of the confirmation form to be used by the CSP.

# 8. Technical interface (HI1)

For exchange of information for administrative and organisational purposes, as described in this document, the following technical transmission media are used:

1. E-mail

   The following requirements apply for e-mail communication:

   a. All e-mail communications must use OpenPGP [24] encryption and have to be properly signed and then encrypted:
      1. The body of the e-mail
      2. Attachments
   b. Reception of e-mails must be confirmed to the sending party. This can be made via automatic confirmation from the mail server concerned to the sending party. The following rules apply:
      1. The exact content of the body of the received e-mail is replied in the body of the reception confirmation e-mail
      2. No further signing and encryption is necessary (the e-mail is already signed and encrypted)
      3. Attachments are not included in the reply
      4. The subject field shall be encoded as follows:

   `Re: original subject`

   Whereby `original subject` denotes the original subject field inserted in the original e-mail.

   c. The private and public keys of the CSP concerned have a validity period of 5 years, after which the keys have to be renewed. The CSP is responsible for generating its new keys and to inform PTSS at least 30 calendar days before the key's expiration date.
   d. The public keys must employ the following naming convention:

   `CSP.asc`

   Whereby `CSP` denotes the name of the CSP. The CSP shall generate the administrative key pair with the administrative e-mail address `"LI_monitor"@CSP-domain`.

   e. For CSPs, the public keys belonging to the specific interception order (see [16]) are exchanged as follows:
      1. The PTSS sends its public key to the CSP as attachment to the interception order
      2. The CSP sends its public key to the PTSS as part of the technical confirmation (see 6.4.3.2)
      3. The public keys must employ the following naming convention:

   `CSP_LIID.asc`

   Whereby `CSP` denotes the name of the CSP and `LIID` is substituted for the specific LIID belonging to the interception order concerned. The LIID has to be put in the e-mail address of the LIID-specific key pair generated by the CSP (LIID@CSP-domain).

   The CSP's private keys belonging to a specific interception order are to be stored at the respective CSP for ten years.

2. Fax
3. Telephone
4. Electronic storage media, e.g. CD

The following table describes the media to be used for the transfer of the various documents and information data, as well as for each case the alternative communication medium in case the preferred choice is temporarily not available.

| *Data / Document to be sent* | *Reference chapter* | *Sender* | *Preferred medium of exchange* | *Alternative medium of exchange* |
|---|---|---|---|---|
| Interception order | 6.4.1 | PTSS | E-mail | Fax[2] |
| Interception confirmation | 6.4.3 | CSP | E-mail | Fax |
| Emergency response (interception not possible) | 6.4.2 | CSP | Telephone | - |
| Modification order | 6.5.1 | PTSS | E-mail | Fax |
| Modification confirmation | 6.5.3 | CSP | E-mail | Fax |
| Emergency response (modification not possible) | 6.5.2 | CSP | Telephone | - |
| Deactivation order | 6.6.1 | PTSS | E-mail | Fax |
| Deactivation confirmation | 6.6.3 | CSP | E-mail | Fax |
| Emergency response (deactivation not possible) | 6.6.2 | CSP | Telephone | - |
| Cancellation order | 6.7.1 | PTSS | E-mail | Fax |
| Cancellation confirmation | 6.7.2 | CSP | E-mail | Fax |
| Information request | 7.1.1 | PTSS | E-mail | Fax |
| Information confirmation | 7.1.3 | CSP | E-mail | Fax |
| Error notification | 10.1.1 | PTSS/CSP | E-mail[3] | Fax |
| Out-Of-Service notification | 10.1.2 | PTSS/CSP | E-mail[3] | Fax |
| System update notification | 10.1.3 | PTSS/CSP | E-mail[3] | Fax |
| Document update notification | 10.1.4 | PTSS | E-mail | Fax |
| New services notification | 10.1.5 | CSP | E-mail | E-mail, delayed[4] |
| Cell-ID table | 10.2 | CSP | E-mail | Electronic storage media |
| Interception order | 6.4.1 / 6.5.1 | PTSS | E-mail | Telephone[5] |

[2] For CSPs, the alternative medium of exchange for the PTSS public key belonging to the specific interception order may be agreed on a case-by-case basis between the PTSS and the respective CSP.

[3] Documents concerning error notifications, out-of-service notifications and system update notifications have to be sent directly to the responsible position. The corresponding address is the e-mail address of "LEMF-Support".

[4] The sending of the service notification must be delayed until the secure exchange over e-mail is available again

| *Data / Document to be sent* | *Reference chapter* | *Sender* | *Preferred medium of exchange* | *Alternative medium of exchange* |
|---|---|---|---|---|
| outside operating hours | | | | |

**Table 7: Media of communication exchange**

The contents of the e-mails include the following:

1. Order (also request) forms: Orders are sent in duplicate: As PDF-documents in the attachment, and in XML-format in the body (the formatting is specified in [16] sections 16.1 and 16.2) Cancellation orders are sent as PDF-attachments only (no XML-file, empty body). The word "Cancellation" (in the recipients chosen language) is added at the end of the Subject-Field.
2. Confirmation forms: Confirmation forms are sent as attachments. Together with each order (also request) form the PTSS sends a corresponding confirmation form template as attachment. The confirmation template (sent by the PTSS to the CSP) as well as the filled in forms (sent by the CSP to the PTSS) are in RTF-format.
3. Notifications: Notifications are sent in the body of the e-mail
4. Tables: Tables are sent as attachments

The subject fields of the e-mails are encoded as following:

1. Order (also request) forms: "00_1.0" [SP] file number
   where
   - "00" denotes e-mail types used for administrative information exchange, as defined in [16] section 12.2.2.
   - "1.0" denotes the version of this document, currently 1.0
   - "file number" denotes the file-number/order-identifier identical to the interception order
2. Notifications: Notification type, as defined in chapter 10.1
3. Table: Table type, as defined in chapter 10.2

For any document or information that needs to be exchanged between the PTSS and the CSPs not mentioned within this document, the PTSS will agree with the responsible CSP on a case-by-case basis on the appropriate medium of exchange.
When document or information transmission over the defined medium reserved (including the alternative medium) is temporarily not possible, the PTSS will agree with the respective CSP on a case-by-case basis on the appropriate medium of exchange. In any case, written confirmations are mandatory for the documents and information exchanges.

For the purpose of communication the PTSS and the CSPs exchange a list containing all relevant professional contact details of the staff acting as communication partners as well as their substitutes. The list shall contain for each person:

1. Name
2. Telephone and fax-number
3. E-mail address
4. Responsibility (e.g. recipient of interception orders, etc.). For the exchange of orders and confirmation documents, only a single contact address shall be defined.

The lists must be updated in case of changes.

[5] With written confirmation from the PTSS on the next working day

# 9. Timing Issues

## 9.1. Operating hours

The operating hours for both CSPs and PTSS are specified as following: Monday to Friday, 8.00-17.00.
During these hours both parties (CSP and PTSS) ensure normal operation processes, whereby normal operation processes means the ability to exchange documents and information through the mechanisms described in chapters 6.4, 6.5 and 6.6 and 7.1, with response times defined hereafter in chapter 9.2.
Outside the operating hours the CSP has to ensure a 24h stand-by-for-emergency duties or at least a 24h availability. Only activations or modifications of real time interception orders are subjected to emergency duties. The PTSS receives from the CSP a list of the telephone numbers for contacting the responsible Lawful Interception units outside the operating hours.

The following timeframe is considered to be outside normal operating hours:
1. Every day after 17.00 until 08.00 the following day
2. Weekends (Saturdays and Sundays)
3. National and official regional holidays

## 9.2. Delivery times

### 9.2.1. Interception orders

In the following the priority levels for interception orders for CSP as a general rule for normal operations[6] are defined, whereby this includes orders for activation, modification and deactivation (note: Deactivation orders are only sent *within* operating hours).
The reaction times for VoIP-Interception are the same as specified in table 8 (Real-Time Interception) and table 10 (Historical Data Interception). This implies particularly, that regardless whether the provider is a Telecommunication or an Internet Service Provider, tables 8 and 10 apply for VoIP services.

#### 9.2.1.1. Real-Time Interception

The following explanations apply to the tables below:
Execution time: Maximum time allowed, between the reception of the interception order at the CSP and the execution of this order by the CSP (determined by the date/time in the confirmation received by the PTSS). In case the order or part of it cannot be executed by the CSP (e.g. a subset of the required interception types cannot be activated), the CSP informs the PTSS accordingly (refer to chapters 6.4.3.1, 6.5.3 and 6.6.3)[7].

The indicated execution times below do not take into account extraordinary situations. In case a CSP is not able to execute the orders in these defined times for any effective reason (e.g. due to many simultaneous orders or due to technical or organisational limitations), the CSP shall immediately inform PTSS about the expected execution times for the delayed orders.

[6] Normal operations refer to the average proportion of normal and high priority requests.

[7] This means, orders arriving at the CSP from 08.00 – 17.00 imply execution times according to the column “during operating hours” and orders arriving at the CSP from 17.00 – 08.00 imply execution times according to the column “outside operating hours” in Table 8 and 9.

Execution times for Real-Time Interception types: CS_1, CS_2 and CS_3:

| *Priority* | *Execution time during operating hours* | *Execution time outside operating hours* |
|---|---|---|
| “High” | 1 hour | 3 hours |
| “Normal” | 2 hours | Not applicable |
| “Required by date & time” | Specified in interception order (shall be longer than “Normal” execution time) | Not applicable |

Table 8: Interception order execution times – *real-time circuit switched*

Execution times for Real-Time Interception types: PS_1, PS_2, PS_3 and PS_4:

| *Priority* | *Execution time during operating hours* | *Execution time outside operating hours* |
|---|---|---|
| Packet switched access Interception [PS_1 and PS_2]: “High” | 4 hours | 10 hours |
| Packet switched access Interception [PS_1 and PS_2]: “Normal” | 6 hours | Not applicable |
| Packet switched application Interception [PS_3 and PS_4]: “High” | 2 hours | 5 hours |
| Packet switched application Interception [PS_3 and PS_4]: “Normal” | 3 hours | Not applicable |
| All types of packet switched Real-Time Interception orders: Required by date & time” | Specified in interception order (shall be longer than “Normal” execution time) | Not applicable |

**Table 9: Interception order execution times – *real-time packet switched***

### 9.2.1.2. Historical Data Interception

Delivery times for Historical Data Interception types using the shipment method for delivery of information according to TR TS [16] section 10.2.1.4: CS_4, CS_5, CS_6, CS_7

The delivery time consists of the compilation time according to Table 10 plus the shipping time according to Table 11 which depends on the delivery method (postal service or electronic interface).

| *Compilation time for high priority order* | *Compilation time for low priority order* |
|---|---|
| 5 working days | 7 working days |

**Table 10: Interception order compilation time**

| *Shipping method* | *Shipping time* |
|---|---|
| Postal service registered mail | 1 working day<br>Note: Outside of the responsibility of the CSP |
| Electronic interface | 1 hour |

**Table 11: Interception order shipping time**

In case the compilation of the data or part of it cannot be executed by the CSP, the CSP informs the PTSS accordingly (refer to chapters 6.4.3.1, 6.5.3 and 6.6.3).

Delivery times for Historical Data Interception types using the automated method for delivery of information according to TR TS [16] section 10.1: PS_5 and PS_6:

The delivery time consists of the compilation time according to Table 12 plus the shipping time according to Table 13 which depends on the delivery method (postal service or electronic interface).

| *Compilation time for high priority order* | *Compilation time for low priority order* |
|---|---|
| 5 working days | 7 working days |

**Table 12: Interception order compilation time for PS_5 and PS_6**

| *Shipping method* | *Shipping time* |
|---|---|
| Postal service registered mail | 1 working day<br>Note: Outside of the responsibility of the CSP |
| Electronic interface | 1 hour |

**Table 13: Interception order shipping time**

In case the compilation of the data or part of it cannot be executed by the CSP, the CSP informs the PTSS accordingly (refer to chapters 6.4.3.1, 6.5.3 and 6.6.3).

Delivery times for Historical Data Interception types using the manual method for delivery of information according to TR TS [16] section 10.2.3: PS_5:

The delivery time consists of the compilation time according to Table 14 plus the shipping time according to Table 15 which depends on the shipping method (e.g. postal service, electronic).

| *Compilation time for high priority order* | *Compilation time for low priority order* |
|---|---|
| *5 working days* | *7 working days* |

**Table 14: Interception order compilation time**

| *Shipping method* | *Shipping time* |
|---|---|
| Postal service standard mail | 2 working days |
| Postal service priority mail | 1 working day |
| Secure e-mail | 1 hour |
| FTP | 1 hour |
| HI-B | 1 hour |

**Table 15: Interception order shipping time**

### 9.2.2. Information requests

The following response times are defined for information requests as a general rule for normal operations[8]:

| *Priority* | *Target identity information* | *Subscriber information* | *Network information* | *Services information* |
|---|---|---|---|---|
| "High" | 1h | 5 days | 5 days | 5 days |
| "Normal" | 1 day | 7 days | 7 days | 7 days |

**Table 16: Response times for information requests**

The following explanations apply to Table 16:

1. Response time: This is defined as the maximum time allowed between reception of the information request at the CSP and the delivery date/time (determined in the received confirmation by the PTSS).
2. The days are defined as working days.

[8] Normal operations refer to the average proportion of normal and high priority requests.

# 10. Reporting

This chapter describes the various reports to be exchanged over the administrative interface between the PTSS and the CSPs.
There are two types of reports to be exchanged at this stage: Notifications and tables.

## 10.1. Notifications

The following notifications must be reported in a timely manner over the HI1 interface:

| *Notification type* |
|---|
| Error notification |
| Out-Of-Service notification |
| System update notification |
| Document update notification |
| New services notification |

**Table 17: Notification types**

The notification type must be shown in the subject field of the corresponding e-mail.

### 10.1.1. Errors

Error notifications contain information about any failure to deliver interception results to the LEMF. The source of the failure can be traced to the CSP or the PTSS.
Typical errors could be (see also [8], annex A.4.4.2)

- LEMF system is down
- CSP system is down
- Failed authorization of connection (e.g. unauthorized CLIP)
- LEMF is busy
- etc.

An error notification shall include:

1. CSP name (or PTSS)
2. Date and time of sending of notification
3. Date and time of error occurrence (if available)
4. Description of the error (if available), including the impact on the CSP's ability to carry out lawful interception
5. Estimated recovery time (if available)

Error notifications must be sent to the other party as soon as the error has been detected.
The mechanism for the transmission of error notifications is described in chapter 8. For the notification text no specific structure is required.

### 10.1.2. Out-Of-Service

Out-Of-Service notifications include information about future internal events which might have an impact on the ability to carry out lawful interception activities. Examples of typical notifications are:

- LEMF system will be shut down for a certain period of time
- CSP system will be shut down for a certain period of time
- Software update on the system will disable delivery for a certain period of time

An Out-Of-Service notification shall include:
1. CSP name (or PTSS)
2. Date and time of sending of notification
3. Date and time of expected occurrence of the event (if available)
4. Description of the event, including the impact on the CSP's ability to carry out the lawful interception activities
5. Estimated recovery time (if available and applicable)

Out-Of-Service notifications must be sent to the other party as soon as the CSP (or the PTSS) becomes aware of the event or, if the event can be planned, at least 6 working days prior to the future event compromising the ability to carry out lawful interception activities.
The mechanism for the transmission of Out-Of-Service notifications is described in chapter 8. No specific structure is required for the notification text.

### 10.1.3. System update

System update notifications inform the other party (CSP or PTSS) of an update or upgrade of the current release of its interface system for delivery of interception results (e.g. IIF).

A system update notification must include:
1. CSP name (or PTSS)
2. Date and time of sending of system update notification
3. Date and time of system update
4. Duration of system update
5. Version number of the updated system

A system update notification must be sent to the other party as soon as the exact date of the system update is known but at least 6 working days in advance.
The mechanism for transmission of system update notifications is described in chapter 8. No specific structure is required for the notification text.

### 10.1.4. Document update

Document update notifications inform the CSPs about a new release of any of the regulatory documents, being under the supervision of the PTSS, on lawful interception. This notification type has a broadcasting character, in the sense that the PTSS sends this notification to all relevant CSPs.

A document update notification shall include:
1. Date and time of sending of document update notification
2. Date when the updated document will become effective
3. Version number of the updated document
4. Information about the changes and additions applied to the document

Document update notifications must be sent to the CSPs as soon as the exact date of the public release of the document is known to the PTSS. The CSPs must be granted enough time to assess the impacts of the new document and to adapt their systems and processes accordingly. Depending on these impacts and the response statements from the CSPs, the PTSS may decide to form a new working group with the CSPs.
The mechanism for the transmission of document update notifications is described in chapter 8. No specific structure is required for the notification text.

### 10.1.5. New services

New service notifications inform the PTSS about new public services the CSP will implement. This enables the PTSS to examine the applicability of lawful interception regulations on that service and to take the necessary steps (e.g. preparing test scenarios).

New service notifications must be sent in the following cases:

1. The CSP introduces one of the following services: Access provision, Value-added service provisioning for call-content processing, voice-mail or number translations.
2. The CSP adds a new service which has an impact on the HI2 interface by adding new IRI parameters (the parameters are defined in [16]).
3. The CSP introduces a new service which is subject to LI according to [16] but cannot be delivered according to the specifications defined in [16].

In the cases 1 and 2 above, the CSP having provided for LI functionality according to [16] to his best effort and knowledge and having sent the service notification to the PTSS can put the service into operation as planned. In case 3 above, the PTSS will contact the involved CSP and decide on a case-by-case basis which actions need to be taken.

A new service notification shall include:

1. CSP name
2. Date and time of sending of the new service notification
3. Date when the new service is offered to the public
4. Date when the LI interface for the new service is planned to be put into operation, if available
5. Brief description of the new service and its impact on the HI

New service notifications must be sent three months in advance of the introduction of the service, or, if not possible, as soon as the exact introduction time of the service is known to the CSP.

The PTSS has to ensure strict confidentiality of the information provided within a service notification. In case a 3rd party organisation (e.g. a system supplier) needs to be contacted by the PTSS in relation to the information included in the service notification, access of this 3rd party organisation to the information included in the service notification, if requested by the CSP concerned, is subject to a non-disclosure-agreement between the CSP and this 3rd party organisation.

The mechanism for the transmission of new service notifications is described in chapter 8. No specific structure is required for the notification text.

## 10.2. Table

This type of reporting includes one table:

1. Cell-ID Table (CSPs only): This table contains a list of all Cell-IDs and their corresponding parameters of the mobile CSP, as defined in [16]. An updated version of this table is to be delivered to the PTSS periodically at least every two weeks, in the format specified in [16].

The table type shall be denoted in the subject field of the corresponding e-mail.
The delivery medium over HI1 for the tables is specified in chapter 8.

# 11. Security

This chapter describes the security mechanisms that shall apply for the administrative and organisational interface at the PTSS and at the CSP.

## 11.1. Communication

For communication aspects, the following security mechanisms apply, as described in chapter 8:

1. Personal communication over telephone, fax or e-mail is carried out only by pre-defined personnel.
2. When communicating via e-mail, OpenPGP shall be used. For that purpose, personnel at PTSS and CSP may use individual private and public keys to sign and encrypt the messages and/or the attachments. OpenPGP features and options to be used are mentioned in chapter 8.

## 11.2. Data protection

To ensure confidentiality of data, the federal requirements of [7] apply for both the PTSS and the CSP.

## 11.3. Hardware security

The CSPs and the PTSS must prevent unauthorized access to the functionality of all the systems involved in lawful interception.

## 11.4. Personnel security aspects

Staff involved in the technical and administrative operations of the lawful interception systems at the PTSS and the CSPs are subject to confidentiality principles. Therefore, each CSP provides the PTSS with a signed confirmation, confirming that all personnel engaged with lawful interception activities have been instructed to handle all matters in a confidential manner.

# 12. Acceptance procedure

This chapter specifies the procedures that apply for acceptance by the PTSS of the technical systems for delivery of interception results as defined in [16]. It is not constrained to the initial setup of the systems, but applies also for ongoing changes and updates of implementations, which need acceptance as well.

## 12.1. Acceptance

Acceptance of the technical systems of the CSPs for delivery of interception results as defined in [16] and [4] requires the following steps:

1. The CSP informs the PTSS about the implemented changes which affect the HI.

   The PTSS receives notice of planned updates and upgrades *in advance*, or as soon as the CSP has knowledge about the exact date of implementation. Equally, when the PTSS is planning an update of its system at the LEMF, it informs the involved CSPs (i.e. those who have installed the delivery interfaces according to [16]) as soon as it knows the exact date of implementation.

   Reporting of the notice is carried out according to chapters 8 and 10.1.3.
2. The PTSS sets up a testing procedure for the new implementation.

   As soon as the PTSS has knowledge about the planned implementations, it can start to work out the details of the test cases for this particular scenario. Regular test scenarios, relating especially to the initial setup of the systems, are defined in a separate document. However, future upgrades could demand adaptation of certain test cases, which will then be devised on a case-by-case basis.

   In order to enable the testing of future implementation changes, there shall be a permanent test environment, described in the following chapter.
3. The PTSS releases the new implementation.

   Upon successful completion of the test cases, the PTSS acknowledges the acceptance of the system to the CSP. The CSP receives a certificate from the PTSS which confirms proper functioning of the CSP's system in compliance with the Swiss handover interface requirements that are defined in [16].
4. The certification procedure allows reduced testing for subsequent implementations of the same system. I.e. in case of a CSP implementing the identical system for which another CSP has already received a certificate due to successful implementation, the CSP and the PTSS may reduce the scope of the tests to a minimum.

## 12.2. Permanent test environment

This chapter illustrates the organisation of permanent testing of the LI interfaces for delivery of interception results as defined in [16] as well as the corresponding requirements.

Testing facilities are of great importance to the PTSS, as it has the mandate to deliver the results of interception to the final recipients, the LEA. Therefore it is the responsibility of the PTSS to ensure proper and reliable functioning of the LI system, which includes (among others) the handover interface to the CSPs.

The mandatory requirements on the permanent test environment in general are as following:

1. The PTSS is allowed to perform handover interface tests according to [16] at any time, also after the conclusion of the initial test phase, when the system is put into operation.
2. This implies that the provisions of the CSPs for system testing need to be permanent as well. These include:

**Lawful Interception of telecommunication traffic**

a. Provision (by CSPs) of a test e-mail account. If the assigned account changes, the PTSS shall be informed immediately.
b. Provision (by CSPs) of an access to the relevant network element performing the interception (by means of an IIF) in order to allow the PTSS to attach Test Equipment (TE) with Test Target Identities (TTI). This further includes:
    i. Configuration of the TTI(s) associated with the access to this attached TE, or associated with a mobile station. If the assigned TTI changes, the PTSS shall be informed immediately.
    ii. Hosting of the TE(s) with associated TTI(s), if requested by the PTSS.
c. Manual interventions by CSP staff in cases where automated testing is not feasible (after consultation of the CSP by the PTSS).
d. Provision of the delivery of results as defined in [16] via handover interfaces connecting the TTI with the LEMF.

The physical layout of the permanent test environment depends on the respective services (circuit switched or packet switched services) and is therefore described in detail in the corresponding test documents.

# 13. Final provisions

According to articles 17 and 25 of [2], the CSPs must implement the administrative interface to the PTSS in compliance with the organisational and administrative requirements from the date of operating the technical interfaces according to [16],

This document comes into force January 1, 2013

3003 Berne, November 9, 2012

Post and Telecommunications Surveillance Service PTSS

sig

René Koch

Head of PTSS

# 14. Annex

## 14.1. Information type request combinations

The following tables depict the standard types of information requests. Each request consists of a combination of known information and corresponding requested information.

### 14.1.1. Target identity information A_1

| Nr | Known information (provided by the authorities) | Requested information (provided by the CSP) | CSP[9] | Comment |
|---|---|---|---|---|
| A_1.1 | IMSI | MSISDN | MN | |
| A_1.2 | MSISDN or IMSI | SIM | MN | |
| A_1.3 | MSISDN or SIM | IMSI | MN | |
| A_1.4 | IMEI | MSISDN, SIM, IMSI | MN | (up to 6 months back) |
| A_1.5 | MSISDN or SIM or IMSI | IMEI | MN | (up to 6 months back) |
| A_1.6 | SIM or MSISDN | PUK | MN | |
| A_1.7 | Refill-Card-Number or secret code | MSISDN, Date & Time of refill, Amount of refill | MN | The two numbers might be partly scratched out or blurred. In this case, as much information as possible is to be handed out. If both numbers are complete, one of them will do for a unique identification of the card. |
| A_1.8 | IP-address | MAC-address | CSP | |

### 14.1.2. Subscriber information A_2

| Nr | Known information (provided by the authorities) | Requested information (provided by the CSP) | CSP | Comment |
|---|---|---|---|---|
| A_2.1 | Telephone number & time period | Contract copy | MN / FN | |
| A_2.2 | Telephone number & time period | Copy of invoice | MN / FN | |
| A_2.3 | Telephone number & time period | Customer correspondence | MN / FN | |
| A_2.4 | Telephone number | Activation date, deactivation date | MN / FN | Last date per default |
| A_2.5 | SIM & time period | Contract copy | MN | |
| A_2.6 | SIM & time period | Copy of invoice | MN | |

[9] MN: Mobile Network, FN: Fixnet Network, ISP: Internet Service Provider

| | | | | |
|---|---|---|---|---|
| A_2.7 | SIM | Name, address, point of sale for prepaid / postpaid cards | MN | |
| A_2.8 | Customer-number | Name, address | MN / FN | Name and address of the owner of the customer-number |

### 14.1.3. Network information A_3

| Nr | Known information (provided by the authorities) | Requested information (provided by the CSP) | Network | Comment |
|---|---|---|---|---|
| A_3.1 | Cell-ID | Location-address of antenna,<br>Coordinates,<br>Main beam | MN | |
| A_3.2 | a) Cell-ID or<br>b) location name & MSISDN & timestamp of communication start | Assumed coverage of the cell concerned | MN | |

### 14.1.4. Service information A_4

| Nr | Known information (provided by the authorities) | Requested information (provided by the CSP) | Network | Comment |
|---|---|---|---|---|
| A_4.1 | PRS-number | Name, Address | MN / FN | |
| A_4.2 | PRS-number | Destination number | FN | |
| A_4.3 | PRS-number | PRS-turnover | MN / FN | |
| A_4.4 | PRS-number | Contract copy | MN / FN | |
| A_4.5 | PRS-number | Copy of invoice | MN / FN | |
| A_4.6 | PRS-number | Customer correspondence | MN / FN | |
| A_4.7 | Name & address | PRS-number | MN / FN | |