Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP

IT Service Center ISC-FDJP
Postal Service and Telecommunications Surveillance PSTS

Lawful Interception of telecommunications traffic

Organisational and administrative requirements (OAR)

Date: May 19th, 2009

Version: 2.10

Confidential

Contents

Document History

Version	Date	Status	Remarks
0.1	06.05.02	Draft	First draft
0.2	31.05.02	Draft	• Work Items updated • Removal of exception handling chapter
0.3	21.06.02	Draft	• Work Items updated
0.4	12.07.02	Final draft	• Work Items updated • 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	15.02.2009	Draft	• Appendices corrected (Syntax correction)
2.10	19.05.2009	Draft	• Add-ons for broadband Internet access surveillance

1. Scope

This document provides the organisational and administrative requirements for interfacing the telecommunication service providers with the governmental PSTS, concerning the issues of lawful interception[1].

The specifications made in this document build 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 circuit switched services (as in [3]), for electronic mail,(as in [4]) and for Internet Acces route (e.g. xDSL,, CATV, WLAN), as in [15][2].

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] and [11]. References to the respective ETSI specifications are made where applicable.

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

This document is classified as confidential and shall be handled correspondingly.

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]	[TR CS]	Technical requirements for the delivery of the results of interception
[4]	[TR PS]	Technical requirements for the delivery of intercepted electronic mail
[5]	[CCIS]	Call Center Information system (CCIS); Regulatorische Aspekte
[6]	SR 172.015	Verordnung über die Klassifizierung und Behandlung von Informationen im zivilen Verwaltungsbereich vom 10. Dezember 1990
[7]	SR 120.4	Verordnung über die Personensicherheitsprüfungen (PSPV) vom 19. Dezember 2001
[8]	SR 235.1	Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992
[9]	ETSI ES 201 671	Telecommunication security; Lawful interception (LI); Handover interface for the lawful interception of telecommunication traffic
[10]	ETSI TS 101 331	Telecommunication security; Lawful interception (LI); Requirements of Law Enforcement Agencies

[1] New content according to Version 2.10, May 19th, 2009

[2] New content according to Version 2.10, May 19th, 2009

[11]	ETSI ES 201 158	Telecommunication security; Lawful interception (LI); Requirements for network functions
[12]	SR 784.101.113 / 1.7	Technische und administrative Vorschriften betreffend die Identifikation des anrufenden Anschlusses (BAKOM/OFCOM)
[13]	[TR HD]	Technical requirements for the delivery of historical data
[14]	SR 780.115.1	Verordnung vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs
[3][15]	[TR TS, Annexe G]	Technical Requirements for Telecommunication Surveillance, Annex G
[4][16]	ETSI TS 102 232-3	Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services

3. Abbreviations

BA	Basic Access interface
CC	Content of Communication
CCIS	Call Center Information system
CLIP	Calling Line Identification Presentation
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
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
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identifier
MF	Mediation Function
MSISDN	Mobile Subscriber ISDN number
MSN	Multiple Subscriber Number
PA	Primary Access interface
PGP	Pretty Good Privacy
POTS	Plain Old Telephony System
PRS	Premium Rate Service
PSTN	Public Switched Telephone Network
PSTS	Postal Service and Telecommunications Surveillance
SIM	Subscriber Identity Module
SMS	Short Messages Service
SN	Subscriber Number

[3] New content according to Version 2.10, May 19th, 2009

[4] New content according to Version 2.10, May 19th, 2009

SPOC	Single Point Of Contact
TISP	Telecommunications *or* Internet Service Provider
TSP	Telecommunications Service Provider
TTI	Test Target Identity
UMTS	Universal Mobile Telecommunications System
UUS	User-User Signaling
VNO	Virtual Network Operator
VoIP	Voice over IP

4. Definitions

Handover interface	See [9], clause 3
Intercept related information	See [9], clause 3
Interception order	An order sent from the PSTS to a TISP for setting up an interception activity
Internet Service Provider	The legal entity providing internet/e-mail services to the intercepted subject
Law Enforcement Monitoring Facility	See [9], clause 3 This is at the same time the data center of the PSTS
Mediation function	See [9], clause 3
PSTS [5]	Postal Service and Telecommunications Surveillance 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 PSTS to initiate an interception activity
Target identity	See [9], clause 3
Target service	See [9], clause 3
Telecommunications Service Provider	The legal entity providing telecommunications services to the intercepted person (denoted as “NWO/AP/SvP” in [9]). This includes also VoIP-services. I.e. that requirements that are listed for TSP's in this document apply also for all providers of VoIP-services.

5. Responsibilities

The responsibilities for interception are defined as follows:

1. A TISP 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 PSTS, in compliance with the requirements in [2], [3] and [4] for telecommunication service data being under control of the TISP. Subcontractors are obliged to assist the TISP in the fulfilment of the above duties.

   A “subcontractor” is defined hereafter as any 3rd party TISP having a contractual agreement with the 1st party TISP to perform telecommunication/internet services on the 1st party TISP’s behalf in Switzerland.
2. A TISP being ordered with an interception order is not responsible for delivery or interpretation of interception data accruing beyond its own or its subcontractors’ network/systems.
3. The HI1 interface must be implemented by all TISP's.
4. In case of a TSP being subject to an interception order, interception results based on the technical interfaces HI2 and HI3 must be delivered in the following cases:
   a. The TSP acts as an access provider to the interception target
   b. The TSP acts as a value added service provider for the following services: Call content (HI3) processing (e.g. Voice Mail); number translation (e.g. 0800 Numbers)

   This implies particularly that TSP's not falling under these conditions do not need to implement HI2 and HI3 interfaces. Information delivery concerning IRI parameters (the pa-

[5] New content according to Version 2.10, May 19th, 2009

rameters are defined in [3]) will in that case be handled over the technical medium underlying the logical handover interface HI1.

5. In case of an ISP, interception results must be delivered according to the specific scenarios denoted in [2], Art. 24.a-h, whereby these apply only to public e-mail and Internet access services
6. If the target uses an access arrangement “Multiple-Access” according to [12], the TSP (being ordered with an interception order) whose access supports the specific communication is responsible for the delivery of the interception results.
7. Upon introduction of a new service being subject to LI requirements according to [2], [3] and [4], the TISP concerned is responsible to ensure, to its best effort and knowledge, proper functioning of its handover interface for this new service, from the date the new service is put into operation.
8. TSP's which provide for their subscribers a VoIP-solution that uses an E.164-Number, derived from the BAKOM numbering-range, as addressing element, are obliged to intercept the complete realtime traffic based on the technical requirements defined in [3], and to store and deliver the complete historical data based on the technical requirements defined in [13], for the target represented by this E.164-Number. The deliveries of the interception results correspond at this stage exactly to the interfaces described in [3] and [13], all requirements of [3] and [13] apply.
9. For a target abroad, the communication traffic into and from the TSP's network in Switzerland must be interceptable. This is valid for real time interception as well as for historical data. This means that target outgoing calls into the TSP's network in Switzerland and target incoming calls from the TSP's network in Switzerland must be interceptable and stored. The delivery of the real time and historical data corresponds exactly to the circuit-switched interfaces described in [3] and [13]. All requirements of [3] and [13] 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 TISP's.

6.1.1. Circuit switched services

The following interception types are defined according to [2] (this includes also VoIP-interception at this stage):

Type	Explanation
CS_1	Content of Communication (CC), as in [2], Art. 16.a. This includes CC as defined in [3]: 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 services available for the concerning target identity must be intercepted.
CS_2	Location information for mobile targets, as in [2], Art. 16.b.
CS_3	Intercept Related Information (IRI), as in [2], Art. 16.c. This includes IRI as defined in [3], 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 addressing elements of the underlying call).
CS_4	Historical data, as in [2], Art. 16.d. The parameters contained in that paragraph (16.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 mecha-

	nisms for transmission of these data to the LEMF will be defined in a separate document.

Table 1: Interception type's circuit switched services

The following combinations are possible when combining 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
5. CS_4

6.1.2. Packet switched services

The following interception types are defined and can be ordered for e-mail services as in [2] or Internet Acces route as in [1]:

Type	Explanation
PS_1	Contents of incoming e-mails, as in [2], Art. 24.a. The parameters contained in that paragraph are to be ordered as a package and cannot be split into further subsets of parameters.
PS_2	Telecommunication parameters of incoming e-mails, as in [2], Art. 24.b. The parameters contained in that paragraph are to be ordered as a package and cannot be split into further subsets of parameters.
PS_3	Telecommunication parameters of mailbox accesses, as in [2], Art. 24.c. The parameters contained in that paragraph are to be ordered as a package and cannot be split into further subsets of parameters.
PS_4	Contents of outgoing e-mails, as in [2], Art. 24.d. The parameters contained in that paragraph are to be ordered as a package and cannot be split into further subsets of parameters.
PS_5	Telecommunication parameters of outgoing e-mails, as in [2], Art. 24.e. The parameters contained in that paragraph are to be ordered as a package and cannot be split into further subsets of parameters.
PS_6	Historical data relating to dynamic allocation of IP-addresses, as in [2], Art. 24.f. The parameters contained in that paragraph are to be ordered as a package and cannot be split into further subsets of parameters.
PS_7	Historical data relating to internet access information, as in [2], Art. 24.g. The parameters contained in that paragraph are to be ordered as a package and cannot be split into further subsets of parameters.
PS_8	Historical data relating to incoming and outgoing e-mails, as in [2], Art. 24.h. The parameters contained in that paragraph are to be ordered as a package and cannot be split into further subsets of parameters.
PS_10[6]	Internet Access route: Real-time delivery of the complete communication of the Broadband Internet Access as in [1], Art. 15. This includes content of communication (CC) and the intercept related information (IRI) of the broadband internet access.

Table 2: Interception types packet switched services

[6] New content according to Version 2.10, May 19th, 2009

An interception order can contain one or multiple real-time interception types (PS_1 until PS_5 and PS_10) or one historical interception type (PS_6 until PS_8)[7].

6.1.3. Emergency Paging

Based on existing practice of the PSTS, as well as on Art. 3.a in [1] (enforced as of April 1st, 2007) the interception types for emergency paging are defined as follows:

N_1	**Location Determination:** 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	**Active Location Determination:** The Active Location Determination N_2 is performed in the same way as N_1. For TSP's which are already connected to the LIS, N_2 interceptions can only be activated with the LIS. In that case, the latest location information and communication related information is captured and stored in the LIS. It is the responsibility of the LEA to ensure their access to the LIS. For the technical feasibility of N_2 interceptions, CS_2 and CS_3 have to be activated preliminary on the LIS.
N_3	**Historical Location Determination** 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.

6.2. Activation bases

The activation bases for interception orders, i.e. the definition of the possible target identities, are defined in [3], [4] and [15]:

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 “CC” and the target identity has a voice-mail service attached, the interception of the voice-mail communication shall be activated as well[8].
2. Packet switched services:
    a. Identifier of the associated telephone line
    b. E-mail address
    c. IP-address
    d. Login-name
    e. MAC-address
    f. Calling number
    g. User identifier assigned to the internet access route
    h. Dial -up access according to ETSI TS 102 232-3 [16] section 5.1.1
    i. xDSL access according to ETSI TS 102 232-3 [16] section 5.1.2
    j. Cable modem access according to ETSI TS 102 232-3 [16] section 5.1.3
    k. WLAN access according to ETSI TS 102 232-3 [16] section 5.1.4

[7] New content according to Version 2.10, May 19th, 2009

[8] New content according to Version 2.10, May 19th, 2009

l. LAN access
m. Other designation for the transmission route
n. Undefined access: The use of this type has to be agreed by PSTS [9].

6.3. Recipients of interception orders

6.3.1. Assigning target identities to TISP's

Upon receipt of a surveillance order from the LEA the PSTS will contact the appropriate TISP which has to carry out the interception activity.

6.3.2. Multiple TISP involvement

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

1. A TISP being selected as in chapter 6.3.1 acts as SPOC (Single Point Of Contact) to the PSTS. This means in particular, that the selected TISP will delegate interception requests to subcontractors if necessary, in order to comply fully with the requirements of delivery of the results of lawful interception as in [2], [3] and [4] and as per the responsibilities defined in chapter 5 above.
2. The PSTS may submit an information request, in compliance with [2] and as specified in chapter 7, to the selected TISP in order to obtain official stored (static) information available at the TISP about other TISP's the target is subscribed to (e.g. through preselection contracts).

6.4. Activation procedure

The activation procedure contains three steps:

1. The PSTS sends an interception order to the TISP
2. The TISP activates the required interception activity
3. The TISP sends a confirmation of the activation to the PSTS

6.4.1. Step one – Initiation

When requesting the activation of an interception activity, the PSTS sends an interception order to the TISP concerned, providing the following information within the interception order form:

1. Form header

   This contains several administrative information elements, including:
   a. TISP name
   b. Priority: This denotes the priority level assigned to this interception order. The priority levels are defined in chapter 9.2.1 and chapter 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 explicitly by which date and time the activation is required to be in place.
   c. File number: File number of form for storage purposes
   d. Lawful Interception Identifier (LIID): Unique identifier of interception order, consisting of 15 numbered digits (the details of which are described in [3])
   e. Reference name: Identifier for referencing the surveillance order
   f. Date: Date of commissioning of interception order
2. Target identity

   This contains the target identity of the interception, as in chapter 6.2.
3. Interception types

[9] New content according to Version 2.10, May 19th, 2009

This contains the various interception types to be delivered to the LEMF, see chapter 6.1.

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 to be delivered.

5. Delivery address

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

6. PSTS signature

Interception order forms are available in the three Swiss national languages (German, French and Italian) as well as in English. The TISP chooses by which of those languages it wants to be contacted.

6.4.2. Step two – Activation

This step is subject to the TISP's internal processes.
Note: For historical data, activation denotes the provision of the data concerned to the destination address.

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

6.4.3. Step three - Confirmation

Upon successful activation of the surveillance case in the switch, the TISP confirms the activation to the PSTS both administratively and technically.

6.4.3.1. Administrative confirmation

The TISP provides to the PSTS the following information within the confirmation form:

1. Form header

   This contains the administrative information elements, including:
   a. TISP name
   b. File number: Same as in the corresponding interception order
   c. LIID: Same as in the corresponding interception order
   d. Reference name: Same as in the corresponding interception order
   e. Date: Date of sending of confirmation

2. Target identity

   This contains the target identity the interception has been activated 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 TISP contact person

The PSTS provides a template of the confirmation form to be used by the TISP for confirmations.

6.4.3.2. Technical confirmation

In addition to the official administrative confirmation, the PSTS also needs to verify the proper functioning of the technical interfaces as in [3] and [4][10].

For this purpose, the TISP concerned sends *to the LEMF* upon successful activation of the interception at his site:

1. For circuit switched services: A confirmation IRI in accordance with [9], annex D.4 (sending of tag *liActivated*).
2. For e-mail services: A confirmation e-mail (whereby the interception type for administrative e-mails is inserted in the subject field, see [4]). 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 [4], chapter 6.2.1. The public ISP 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 PSTS key to be used for the underlying interception activity (see chapter 8).
3. For Broadband Internet Access: a confirmation e-mail (encrypted) or a Fax with the activation details must be send to the PSTS[11].

6.5. Modification procedures

The modification procedure contains three steps:

1. The PSTS sends a modification order to the TISP
2. The TISP undertakes the required modifications to the interception activity
3. The TISP sends a confirmation of the modifications to the PSTS

6.5.1. Step one – Initiation

When requesting the modification of an existing interception activity, the PSTS sends a modification order to the TISP concerned, providing the following information within the modification order form:

1. Form header

   This contains several administrative information elements, including:
   a. TISP name
   b. Priority: This denotes 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 explicitly by which date and time the modification is required to be in place.
   c. File number (same as the one of the underlying interception order)
   d. LIID (same as the one of the underlying interception order)
   e. Reference name (same as the one of the underlying interception order)
   f. Date: Date of commissioning of modification order
2. Target identity

   This contains the target identity of the interception, as in chapter 6.2.
3. Interception modification

   This contains the modification of the interception types combination to be delivered to the LEMF, see chapter 6.1. The modification order can contain the addition or removal of any of the interception types defined in chapter 6.1.
4. PSTS signature

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

[11] New content according to Version 2.10, May 19th, 2009

Modification order forms are available in the three Swiss national languages (German, French and Italian) as well as in English. The TISP chooses by which of those languages it wants to be contacted.

6.5.2. Step two – Modification

This step is subject to the TISP's internal processes.
If any of the required modifications requested in the modification order cannot be carried out, the TISP reports this immediately to the PSTS (see also chapter 8). The official confirmation is carried out as described below.

6.5.3. Step three - Confirmation

Upon successful modification, the TISP confirms the modification to the PSTS, providing the following information within the confirmation form:

1. TISP name
2. Form header

   This contains the administrative information elements, including:
   a. File number: Same as in the corresponding modification order
   b. LIID: Same as in the corresponding modification order
   c. Reference name: Same as in the corresponding modification order
   d. Date: Date of sending of confirmation
3. Target identity

   This contains the target identity upon which the modification has been taken place.
4. Interception modification

   If certain modifications required in the interception order could not be carried out, the reason here fore is to be provided.
5. Date and time of modification
6. Name of TISP contact person

The PSTS provides a template of the confirmation form to be used by the TISP for confirmations.

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 contains three steps:

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

6.6.1. Step one – Initiation

Deactivation orders are only sent within operating hours. When requesting the deactivation of an interception activity, the PSTS sends a deactivation order to the TISP concerned, providing the following information within the deactivation order form:

1. Form header

   This contains several administrative information elements, including:
   a. TISP name
   b. File number (same as the one of the underlying interception order)
   c. LIID (same as the one of the underlying interception order)

   d. Reference name (same as the one of the underlying interception order)
   e. Date: Date of commissioning of deactivation order
2. Target identity

   This contains the target identity of the interception to be deactivated, as in chapter 6.2.
3. Date and time of deactivation (which must not be before date and time of the sending of the deactivation order)
4. PSTS signature

Deactivation order forms are available in the three Swiss national languages (German, French and Italian) as well as in English. The TISP chooses by which of those languages it wants to be contacted.

6.6.2. Step two – Deactivation

This step is subject to the TISP's internal processes.

6.6.3. Step three - Confirmation

Upon successful deactivation, the TISP confirms the deactivation to the PSTS, providing the following information within the confirmation form:

1. Form header

   This contains the administrative information elements, including:
   a. TISP name
   b. File number: Same as in the corresponding deactivation order
   c. LIID: Same as in the corresponding deactivation order
   d. Reference name: Same as in the corresponding deactivation order
   e. Date: Date of sending of confirmation
2. Target identity

   This contains the target identity the deactivation has been undertaken on.
3. Date and time of deactivation
4. Name of TISP contact person

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

6.7. Cancellation of orders

The PSTS may cancel an interception order that has been delivered already to the TISP, as long as the PSTS has not received yet the administrative confirmation of the activation of the surveillance case by the TISP. The administrative confirmation has only to be sent to the PSTS, when the surveillance is activated in the switch (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. As soon as the administrative confirmation has been received at the PSTS, a cancellation is not possible anymore.
Upon cancellation of an interception order, the TISP is entitled to remuneration for the work being carried out so far in relation to the cancelled interception order.

6.7.1. Step one - Initiation

The PSTS sends the cancellation order to the TISP, providing the following information within the cancellation form:

1. Form header

This contains several administrative information elements, including:

a. TISP name
b. File number
c. LIID (same as the one of the underlying ordered interception activity)
d. Reference name (same as the one of the underlying ordered interception activity)
e. Date: Date and time of sending of the cancellation form

2. Target identity

   This contains the target identity of the underlying ordered interception activity
3. Cancelled file number (same as the one of the underlying ordered interception activity)
4. Description: Short description of the cancellation order
5. PSTS signature

Cancellation forms are available in the three Swiss national languages (German, French and Italian) as well as in English. The TISP chooses by which of those languages it wants to be contacted.

6.7.2. Step two - Confirmation

The TISP confirms the cancellation to the PSTS, providing the following information within the confirmation form:

1. Form header

   This contains the administrative information elements, including:

   a. TISP name
   b. File number (same as the one of the cancellation order)
   c. LIID (same as the one of the underlying ordered interception activity)
   d. Reference name (same as the one of the underlying ordered interception activity)
   e. Date: Date and time of sending of the confirmation
2. Target identity

   This contains the target identity of the underlying ordered interception activity
3. Name of TISP contact person

The PSTS provides a template of the confirmation form to be used by the TISP for confirmations.

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, as in the following table:

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 3: 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 experience of combinations which have been requested in the past. For further information requests which are not covered

in chapter 14.1, the PSTS will agree on a case-by-case basis with the TISP concerned about the conditions of delivery.

7.1. Information request procedure

The information request procedure contains three steps:

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

7.1.1. Request

The PSTS sends an information request to the TISP concerned, providing the following information within the information request form:

1. Form header

   This contains several administrative information elements, including:
   a. TISP 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 information request
   e. Reference name
   f. Date: Date of sending of information request
2. Information type category: This denotes the category as in Table 3.
3. Known information
4. Requested information
5. Delivery address

   This denotes the destination address for delivery of the information response.
6. PSTS signature

Interception request forms are available in the three Swiss national languages (German, French and Italian) as well as in English. The TISP chooses by which of those languages it wants to be contacted.

7.1.2. Response

This process is internal to the TISP. The response is being sent to the destination address denoted in the information request form.

7.1.3. Confirmation

The TISP sends an information confirmation to the PSTS, providing the following information within the form:

1. Form header

   This contains several administrative information elements, including:
   a. TISP name
   b. File number (same as in the corresponding information request)
   c. Order number (same as in the corresponding information request)
   d. Reference name (same as in the corresponding information request)
   e. Date: Date of sending of information confirmation
2. Date of sending of response
3. Transfer medium used for response
4. Name of TISP contact person

The PSTS provides initially a template of the confirmation form to be used by the TISP for confirmations.

8. Technical interface (HI1)

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

1. E-mail

   The following requirements apply for e-mail communication:

   a. All e-mail communications must employ OpenPGP signing and encryption for:
      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 contact persons concerned have a validity period of 1 year, after which the keys have to be renewed. The PSTS contacts the TISP's to renew the keys.
   d. The public keys must employ the following naming convention:

   `TISP.asc`

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

   e. For ISPs, the public keys belonging to the specific interception order (see [4]) are exchanged as follows:
      1. The PSTS sends its public key to the ISP as attachment to the interception order
      2. The ISP sends its public key to the PSTS as part of the technical confirmation (see 6.4.3.2)
      3. The public keys must employ the following naming convention:

   `ISP_LIID.asc`

   Whereby `ISP` denotes the name of the ISP and `LIID` is substituted by 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 TISP (LIID@TISP-domain).

   The ISPs’ private keys belonging to a specific interception order are to be stored at the ISP concerned 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	PSTS	E-mail	Fax[12]
Interception confirmation	6.4.3	TISP	E-mail	Fax
Emergency response (interception not possible)	6.4.2	TISP	Telephone	-
Modification order	6.5.1	PSTS	E-mail	Fax
Modification confirmation	6.5.3	TISP	E-mail	Fax
Emergency response (modification not possible)	6.5.2	TISP	Telephone	-
Deactivation order	6.6.1	PSTS	E-mail	Fax
Deactivation confirmation	6.6.3	TISP	E-mail	Fax
Emergency response (deactivation not possible)	6.6.2	TISP	Telephone	-
Cancellation order	6.7.1	PSTS	E-mail	Fax
Cancellation confirmation	6.7.2	TISP	E-mail	Fax
Information request	7.1.1	PSTS	E-mail	Fax
Information confirmation	7.1.3	TISP	E-mail	Fax
Error notification	10.1.1	PSTS/TISP	E-mail[13]	Fax
Out-Of-Service notification	10.1.2	PSTS/TISP	E-mail[13]	Fax
System update notification	10.1.3	PSTS/TISP	E-mail[13]	Fax
Document update notification	10.1.4	PSTS	E-mail	Fax
New services notification	10.1.5	TISP	E-mail	E-mail, delayed[14]
Cell-ID table	10.2	TSP	E-mail	Electronic storage media
MF-Type table	10.2	TSP	E-mail	Fax

[12] For ISPs, the alternative medium of exchange for the PSTS public key belonging to the specific interception order may be agreed on a case-by-case basis between the PSTS and the ISP concerned.

[13] 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 "LIS Support".

[14] The sending of the service notification shall 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*
Interception order outside operating hours	6.4.1 / 6.5.1	PSTS	E-mail	Telephone[15]

Table 4: Media of communication exchange

The contents of the e-mails are included as follows:

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 the annex, see chapter 14.2) 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 PSTS sends a corresponding confirmation form template as attachment. The confirmation template (sent by the PSTS to the TISP) as well as the filled out forms (sent by the TISP to the PSTS) 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 follows:

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 [4], chapter 6.1.1
   - "1.0" denotes the version of this document, currently 1.0
   - "file number" denotes the file-number/order-identifier of the underlying interception order
2. Notifications: Notification type, as in chapter 10.1
3. Tables: Table type, as in chapter 10.2

For any document or information that needs to be exchanged between the PSTS and the TISP's and which is not mentioned within this document, the PSTS will agree with the TISP concerned on a case-by-case basis about the appropriate medium of exchange.
When document or information exchange over the particular medium reserved herefore (including the alternative medium) is temporarily not possible, the PSTS will agree with the TISP concerned on a case-by-case basis about the appropriate medium of exchange. In any case, written confirmations are mandatory for the documents and information exchanges contained in Table 4.

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

1. Name
2. Telephone and fax-number
3. E-mail address

[15] With written confirmation from the PSTS on the next working day

4. Communication function (e.g. recipient of interception orders, etc.). For the exchange of orders and confirmation documents, only one single contact address shall be defined.

The lists must be updated in case of changes.

9. Timing Issues

9.1. Operating hours

The operating hours for both TISP's and PSTS are specified as follows: Monday to Friday, 8.00-17.00.

During these hours both parties (TISP and PSTS) ensure normal operation, whereby normal operation 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 TISP has to ensure a 24h stand-by-for-emergency duties or at least 24h availability. Only activations or modifications of real time interception orders are subject to emergency duties. The PSTS receives from the TISP a list of the telephone numbers for contacting outside the operating hours.

The following hours and days are considered to be outside the operating hours:

1. Every day after 17.00 until 08.00 on the next 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 TSP's and ISPs as a general rule for normal operations[16] 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 the following tables 5 (real-time interception) and 7 (historical data interception). This implies particularly, that regardless whether the provider is a TSP or an ISP, tables 5 and 7 (TSP-tables) apply for VoIP services.

9.2.1.1. Real-time interception

Priority	*Reaction time during operating hours*	*Reaction time outside operating hours*
"High"	1h	3h
"Normal"	2h	-
"Required by date & time"[17]	Specified in interception order	Specified in interception order

Table 5: Interception order reaction times - *TSP's*

[16] Normal operations are referring here to an average number of orders and an average proportion of normal and high priority orders.

[17] New content according to Version 2.10, May 19th, 2009

Priority	*Reaction time during operating hours*	*Reaction time outside operating hours*
E-Mail Interception: "High"	2h	5h
E-Mail Interception: "Normal"	3h	-
E-Mail Interception: "Required by date & time"[18]	Specified in interception order	Specified in interception order
"Broadband Internet Interception: Required by date & time"[19]	Reaction time for Broadband Internet Interception: Starting with July 1st, 2010 activation must be completed as soon as possible, with a maximum of 7 calendar-days.	

Table 6: Interception order reaction times - *ISPs*

The following explanations to the above tables apply:

1. Reaction time: this is defined as the maximum time allowed, elapsing between the interception reception order at the TISP and the date/time of the execution (determined in the received confirmation at the PSTS). In case the order or part of it cannot be implemented by the TISP (e.g. a subset of the required interception types cannot be activated), the TISP informs the PSTS accordingly in the confirmation form (as in chapters 6.4.3.1, 6.5.3 and 6.6.3).

2. During/Outside operating hours: This relates to the time of *commissioning of the interception order* at the TISP[20].

9.2.1.2. Historical data interception

Priority	*Reaction time*
"High"	5 days
"Low"	7 days

Table 7: Interception order reaction times – *TSP's (historical data)*

Delivery time for data stored within the last 30 days	*Delivery time for data stored before the last 30 days*
1 day	5 days

Table 8: Interception order reaction times – *ISPs (historical data)*

[18] New content according to Version 2.10, May 19th, 2009

[19] New content according to Version 2.10, May 19th, 2009

[20] This means, orders arriving at the TISP from 08.00 – 17.00 imply reaction times according to the column "during operating hours" and orders arriving at the TISP from 17.00 – 08.00 imply reaction times according to the column "outside operating hours" in Table 5 and Table 6.

The days are defined as working days.

9.2.2. Information requests

The following response times are defined for information requests as a general rule for normal operations[21]:

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 9: Response times for information requests

The following explanations to Table 9 apply:

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

10. Reporting

This chapter describes the various reports to be exchanged over the administrative interface between the PSTS and the TISP's.
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 10: 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 lie with the TISP or the PSTS.
Typical error events could be (see also [9], annex A.4.4.2)

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

An error notification shall contain:

1. TISP name (or PSTS)

[21] Normal operations are referring here to an average number of requests and an average proportion of normal and high priority requests.

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 TISP'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 impact on the ability to process lawful interception. Typical notifications might be:

- LEMF system will be shut down for a certain period of time
- TISP 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 contain:

1. TISP name (or PSTS)
2. Date and time of sending of notification
3. Date and time of expected occurrence of the event described in the notification (if available)
4. Description of the event underlying the notification, including the impact on the TISP's ability to carry out lawful interception
5. Estimated recovery time (if available and applicable)

Out-Of-Service notifications must be sent in advance to the other party as soon as the TISP (or the PSTS) is aware of the future event causing the notification.
The mechanism for the transmission of Out-Of-Service notifications is described in chapter 8. For the notification text no specific structure is required.

10.1.3. System update

System update notifications inform the other side (TISP or PSTS) about an update or upgrade of the current release of its interface system for delivery of interception results (e.g. IIF).

A system update notification shall contain:

1. TISP name (or PSTS)
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

System update notifications must be sent to the other party as soon as the exact date of the system update is known.
The mechanism for transmission of system update notifications is described in chapter 8. For the notification text no specific structure is required.

10.1.4. Document update

Document update notifications inform the TISP's about a new release of any of the regulatory documents, being under the supervision of the PSTS, on lawful interception. This notification

type has a broadcasting character, in the sense that the PSTS sends this notification to all relevant TISP's.

A document update notification shall contain:
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 to the document text

Document update notifications must be sent to the TISP's as soon as the exact date of the public release of the document is known to the PSTS. The TISP's 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 TISP's, the PSTS may decide to form a new working group with the TISP's.
The mechanism for the transmission of document update notifications is described in chapter 8. For the notification text no specific structure is required.

10.1.5. New services

New service notifications inform the PSTS about new public services the TISP will put into operation. This enables the PSTS to examine the applicability of lawful interception regulations on that service and to take the necessary steps accordingly (e.g. preparing test scenarios).

New service notifications must be sent in the following cases:
1. The TISP introduces newly one of the following services: Access provision, Value-added service provisioning for call-content processing, voice-mail or number translations.
2. The TSP adds to his portfolio a service which impacts on the HI2 interface in that one or more additional IRI parameters (the parameters are defined in [3]) are newly being sent to the LEMF.
3. The TISP introduces a new service which is subject to LI according to [3] or [4] but cannot be delivered according to the specifications defined in [3] or [4].

In the cases 1 and 2 above, the TISP having provided for LI functionality according to [3] and [4] to his best effort and knowledge and having sent the service notification to the PSTS can put the service into operation as planned. In case 3 above, the PSTS will contact the TSP concerned and decide on a case-by-case basis on the actions to be taken.

A new service notification shall contain:
1. TISP name
2. Date and time of sending of the new service notification
3. Date when the new service is planned to be put into operation
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 shall 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 TISP.

The PSTS 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 PSTS in relation to the information included in the service notification, access of this 3rd party organisation to the information included in the service notification is, if requested by the TISP

concerned, subject to a non-disclosure-agreement between the TISP concerned and this 3rd party organisation.

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

10.2. Tables

This type of reporting contains two tables:

1. Cell-ID Table (TSP's only): This table contains a map of all Cell-IDs and their corresponding parameters of the mobile network operators, as defined in [3]. An updated version of this table is to be delivered to the PSTS periodically every two weeks, in the format specified in [3].
2. MF-Type table (TSP's only): This table contains the current versions of the software of the various IIF's of the lawful interception system at the TSP. These are used as parameters of the file name used for the FTP transfer of IRI's to the LEMF, see [3]. The table must contain for each IIF the name of the manufacturer and the version of the SW. An updated version of this table is to be delivered to the PSTS as soon as the manufacturer or SW version of one of the IIF's change.

   The PSTS compiles the two-letter parameter for each IIF to be inserted into the FTP file name out of the MF-type table received from the TSP's.

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 PSTS and at the TISP.

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.

11.2. Data protection

To ensure confidentiality of data, the federal requirements of [6] and [8] apply for both the PSTS and the TISP.

11.3. Hardware security

The TISP's and the PSTS must provide for prevention of 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 PSTS and the TISP's are subject to confidentiality principles. Therefore, each TISP provides the PSTS with a signed confirmation, confirming that all personnel engaged with lawful interception activities at that TISP have been instructed to handle all matters involved in a confidential manner.

12. Acceptance procedure

This chapter specifies the procedures that apply for acceptance by the PSTS of the technical systems for delivery of interception results as in [3] and [4]. 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 TISP's for delivery of interception results as in [3] and [4] requires the following steps:

1. The TISP informs the PSTS about the changes in implementation which affect the HI.

   The PSTS receives notice of planned updates and upgrades *in advance*, as soon as the TISP under concern has knowledge about the exact date of implementation. Equally, when the PSTS is planning an update of its system at the LEMF, it informs the involved TISP's (i.e. those who have installed the delivery interfaces according to [3] and [4]) as soon as it has knowledge about the exact date of implementation.
   Reporting of the notice is carried out according to chapters 8 and 10.1.3.
2. The PSTS sets up a testing procedure for the new implementation.

   As soon as the PSTS has knowledge about the planned implementations, it can start to devise the test cases for this particular scenario. Regular test scenarios, relating in specific 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 smooth processing of testing future implementation changes, there shall be a permanent test environment, described in the subsequent chapter.
3. The PSTS releases the new implementation for putting into operation.

   Upon successful completion of the test cases, the PSTS acknowledges the acceptance of the system to the TISP under concern. The TISP receives a certificate from the PSTS which confirms proper functioning of the TISP’s system in compliance with the Swiss handover interface requirements that are defined in [3] and [4].
4. The certification procedure allows reduced testing for subsequent implementations of the same system. I.e. in case of a TISP implementing the same system for which another TISP has already received a certificate for successful implementation, the TISP and the PSTS can reduce the scope of the tests to a minimum required.

12.2. Permanent test environment

This chapter defines the proposed organisation of permanent testing of the LI interfaces for delivery of interception results as in [3] and [4] and the corresponding requirements.

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

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

1. The PSTS is allowed to perform handover interface tests according to [3] and [4] at any time it wishes to, also after the conclusion of the initial test phase, when the system is put into operation.
2. This implies that the provisions of the TISP's for system testing need to be permanent as well. These include:

a. Provision (by ISPs) of a test e-mail account. If the assigned account changes, the PSTS shall be informed immediately.
b. Provision (by TSP's) of an access to relevant switches that provide for interception (by means of an IIF) in order to allow the PSTS 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, as appropriate. If the assigned TTI changes, the PSTS shall be informed immediately.
    ii. Hosting of the TE(s) with associated TTI(s), if requested by the PSTS.
c. Manual interventions by TISP staff in cases where automated testing is not feasible (after consultation of the TISP by the PSTS).
d. Provision of the delivery of results as in [3] and [4] via handover interface connecting the TTI with the LEMF.

The physical layout of the permanent test environment is dependent on the services under concern (circuit switched services or e-mail services) and is therefore described in detail in the corresponding test documents.

13. Final provisions

According to articles 17 and 25 of [2], the TSP's and ISPs must implement the administrative interface to the PSTS according to these organisational and administrative requirements from the date of putting into operation the technical interfaces according to [3] and [4],

The requirements of this document are valid from [22]August 1st 2009.

3003 Berne, ...

Postal Service and Telecommunications Surveillance PSTS

Partick Schöpf .

[22] New content according to revision of Version 2.10 of May 19th, 2009

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 TISP)	TISP[23]	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 secrete 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 suffices for a unique identification of the card.
A_1.8	IP-address	MAC-address	ISP	

14.1.2. Subscriber information A_2

Nr	Known information (provided by the authorities)	Requested information (provided by the TISP)	TSP	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	

[23] 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 TISP)	Network	Comment
A_3.1	Cell-ID	Location-address of antenna, Coordinates, Main beam	MN	
A_3.2	a) Cell-ID or 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 TISP)	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	

14.2. XML document structures

14.2.1. Data structure for orders

The XML document type definition (DTD) associated with the XML files for activation, modification and deactivation orders is defined as follows:

```
<!-- order.dtd -->
<!ELEMENT order (comment*, date-of-execution?, tisp, file-number,
liid, reference-name, date-of-order, target-identity, (activa-
tion|modification)?)>
     <!ATTLIST order order-type (activation|modification|deactivation)
     #REQUIRED priority
     (high|normal|required_by_date_and_time|emergency) #REQUIRED>
     <!ELEMENT date-of-execution (#PCDATA)>
     <!ELEMENT comment (#PCDATA)>
```

```
<!ELEMENT tisp (#PCDATA)>
<!ELEMENT file-number (#PCDATA)>
<!ELEMENT liid (#PCDATA)>
<!ELEMENT reference-name (#PCDATA)>
<!ELEMENT date-of-order (#PCDATA)>
<!ELEMENT target-identity (#PCDATA)>
     <!ATTLIST target-identity target-type (fixnet-call-number|
     msisdn|imei|imsi|voice-mail-identifier|e-mail-address|ip-
     address|login-name|mac-address) #REQUIRED>
<!ELEMENT activation (interception-type+, interception-period?,
address)>
     <!ELEMENT interception-type (#PCDATA)>
     <!ELEMENT interception-period (from?, to)>
          <!ELEMENT from (#PCDATA)>
          <!ELEMENT to (#PCDATA)>
     <!ELEMENT address (#PCDATA)>
          <!ATTLIST address destination (external| PSTS) #RE-
QUIRED>
<!ELEMENT modification (interception-type+)>
```

The meanings of the XML elements correspond to the definition in chapter 6. The following rules apply:

1. If the `priority` is set to “`required_by_date_and_time`”, the element `date-of-execution` is mandatory.
2. For the activation and modification order, the respective element `activation` and `modification`, respectively, must be included in the order. None of these two elements must appear in a deactivation order.
3. The element `interception-period` is included only for historical data denoting the period of time the results of interception are to be delivered. Hence, both elements, „`from`“ and „`to`“ are necessary
4. For a deactivation order, the `priority` must be set to “`required_by_date_and_time`”.
5. The `address` element must contain the destination address when the attribute `destination` is set to “`external`”. It must be empty when the destination attribute is set to “PSTS”.
6. In case of modifications, the element `interception-type` contains all the types that are valid for the modified interception activity, i.e. including the newly added types and excluding the newly removed types.

The elements `comment`, `target-type`, `date-of-order` and `date-of-execution` are defined as follows:

`comment =`	optional comment
`target-identity =`	The meaning of this identifier and its representation depend on the target type

Target type	Identifier meaning and format
fixnet-call-number	Fixnet number in international format, e.g. +41431234567
msisdn	MSISDN in international format, e.g. +41791234567
imei	IMEI (15 digits)
imsi	IMSI (15 digits)
voice mail identi-fier	Voice mail identifier, e.g. E.164 number in international format, e.g. +41781234567
e-mail address	E-Mail address in standard format accord-ing to RFC2821
ip-address	IP address in either IPv4 or IPv6 standard format
login-name	Login-name for the service accessed
mac-address	MAC-address of the accessing unit. The MAC-address is presented as a hexadeci-mal value (0 – F).

date-of-order = Date and time of commissioning the order

date-of-execution = Date and time the order is to be executed.

from = Date and time the interception has to start.

to = Date and time the interception has to end.

The date and time indications must be composed according to the structure below:

date-of-order = year month day [SP] hours ":" minutes ":" seconds [SP] zone

date-of-execution = year month day [SP] hours ":" minutes ":" seconds [SP] zone

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

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

The components introduced above 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 fol-lowing 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 days allowed for the specific month.
`hours =`	Two-digit representation of the hours of the actual local time, i.e. one of the following values: “00”, “01”, “02”, ... , “23”.
`minutes =`	Two-digit representation of the minutes of the actual local time, i.e. one of the following values: “00”, “01”, “02”, ... , “59”.
`seconds =`	Two-digit representation of the seconds of the actual local time, i.e. one of the following values: “00”, “01”, “02”, ... , “59”.

In the following a few examples are listed:

Example for an activation order:

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE order SYSTEM “order.dtd”>
<order order-type="activation" priority="high">
      <comment>very urgent</comment>
      <tisp>newtelco</tisp>
      <file-number> A.123456.A.01.E </file-number>
      <liid>200206211234567</liid>
      <reference-name>abc</reference-name>
      <date-of-order>20020621 14:25:14</date-of-order>
      <target-identity target-type="msisdn">+41761234567</target-
identity>
      <activation>
            <interception-type>CS_4</interception-type>
            <interception-period>
                  <from>20020322 12:00:00</from>
                  <to>20020622 12:00:00</to>
            </interception-period>
            <address destination="external">
Kantonspolizei Z&#252;rich; Hans Muster; Kasernenstrasse; 8000
Z&#252;rich
            </address>
      </activation>
</order>
```

Example for a modification order:

```
<?xml version="1.0" encoding="UTF-8?>
<!DOCTYPE order SYSTEM "order.dtd">
<order order-type="modification" priority="required_by_date_and_time">
      <date-of-execution>20020626 12:00:00</date-of-execution>
```

```
      <tisp>newtelco</tisp>
      <file-number> A.123456.A.02.M </file-number>
      <liid>200206211234567</liid>
      <reference-name>abc</reference-name>
      <date-of-order>20020621 14:25:14</date-of-order>
      <target-identity target-type="fixnet-call-number">+41431234567
      </target-identity>
      <modification>
            <interception-type>CS_1</interception-type>
            <interception-type>CS_3</interception-type>
      </modification>
</order>
```

Example for a deactivation order:

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE order SYSTEM "order.dtd">
<order order-type="deactivation" priority="required_by_date_and_time">
      <date-of-execution>20020626 12:00:00</date-of-execution>
      <tisp>newtelco</tisp>
      <file-number> A.123456.A.03.A </file-number>
      <liid>200206211234567</liid>
      <reference-name>abc</reference-name>
      <date-of-order>20020621 14:25:14</date-of-order>
      <target-identity target-type="imei">123456789012345</target-
identity>
</order>
```

14.2.2. Data structure for requests

The XML document type definition (DTD) associated with the XML files for information requests is defined as follows:

```
<!-- request.dtd -->
<!ELEMENT request (comment?, date-of-execution?, tisp, file-number,
order-number, reference-name, date-of-order, known-information,
requested-information, address)>
      <!ATTLIST request request-category (1|2|3|4) #REQUIRED priority
      (high|normal|required_by_date_and_time) #REQUIRED>
      <!ELEMENT date-of-execution (#PCDATA)>
      <!ELEMENT comment (#PCDATA)>
      <!ELEMENT tisp (#PCDATA)>
      <!ELEMENT file-number (#PCDATA)>
      <!ELEMENT order-number (#PCDATA)>
      <!ELEMENT reference-name (#PCDATA)>
      <!ELEMENT date-of-order (#PCDATA)>
      <!ELEMENT known-information (#PCDATA)>
      <!ELEMENT requested-information (#PCDATA)>
      <!ELEMENT address (#PCDATA)>
            <!ATTLIST address destination (external|PSTS) #REQUIRED>
```

The meanings of the XML elements correspond to the definition in chapter 7. The same formats of the elements as described in chapter 14.2.1 hold.

Example for an information request:

```
<?xml version="1.0"?>
<!DOCTYPE request SYSTEM “request.dtd”>
<request request-category="1" priority="normal">
      <tisp>newtelco</tisp>
      <file-number>12345</file-number>
      <order-number>R20020621123456</order-number>
      <reference-name>abc</reference-name>
      <date-of-order>20020621 14:25:14</date-of-order>
      <known-information>SIM card number ABC1234567</known-information>
      <requested-information>MSISDN</requested-information>
      <address destination="external">
            Police Cantonale Vaudoise, Mr. Hans Muster, 1052 Le Mont-
            sur-Lausanne
      </address>
</request>
```