Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP

IT Service Centre ISC-FDJP
Post and Telecommunications Surveillance Service

Guidelines for Lawful Interception of Telecommunication Traffic

Technical Requirements for Telecommunication Surveillance (TR TS)

Date: November 23, 2011

Version 3.0

Address and contact:

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

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

Table of contents

1. Scope of the Document

This document describes the technical requirements for the interfaces between the equipment of Communication Service Providers and the equipment of the governmental service PTSS (Post and Telecommunications Surveillance Service) for the provision of lawful interception. It specifies how the respective ETSI standards apply for the purpose of lawful interception in Switzerland.

Organisational and Administrative requirements and compliance testing aspects are not part of this specification and are treated separately in [3].

2. Legal Notice

This document specifies the technical requirements for the implementation of lawful interception of telecommunication traffic. It replaces the technical requirements previously published by PTSS as listed in section 15.

PTSS has the competence to publish technical and administrative guidelines in accordance to article 33 par. 1bis of “Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11)”.

3. Abbreviations

3GPP	Third Generation Partnership Project
ASCII	American National Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
BA	Basic Access (ISDN Basic Access)
BC	Bearer Capability
BRAS	Broadband Remote Access Server
BÜPF	“Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1)” Federal Act of 6 October 2000, on Postal and Telecommunications Surveillance
CATV	Cable television
CC	Content of Communication
CD	Call Data
CLIP/R	Calling Line Identification Presentation / Restriction
CMTS	Cable Modem Termination System
COLP/R	Connected Line Identification Presentation / Restriction
CSP	Communications Service Provider
CUG	Closed User Group
DCF77	German longwave time signal and standard-frequency radio station.
DDI	Direct Dialling In
DSS1	Digital Subscriber Signalling System No 1
DTD	Document Type Definition
E.164	International public telecommunication numbering plan defined by ITU-T
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
FOITT	Federal Office of Information Technology, Systems and Telecommunication
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HI	Handover Interface
HLC	High Layer Compatibility
IIF	Internal Interception Function
IMAP	Internet Message Access Protocol
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
INI	Internal Network Interface
IP	Internet Protocol
IRI	Interception Related Information
ISC-FDJP	IT Service Centre Federal Department of Justice and Police
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAN	Local Area Network
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identifier
MAP	Mobile Application Part
MMS	Multimedia Messaging Service
MS	Mobile Station

MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber ISDN Number
MSN	Multiple Subscriber Number
MTA	Mail Transfer Agent
NEID	Network Element Identifier
OFCOM	Federal Office of Communications (Switzerland)
OID	Object Identifier
PDN-GW	Packet Data Network Gateway
POP3	Post Office Protocol – Version 3
PRA	Primary Rate Access
PRS	Premium Rate Services
PSTN	Public Switched Telephone Network
PTSS	Postal and Telecommunications Surveillance Service
PUK	Personal Unblocking Key
S-GW	Serving Gateway
SIP	Session Initiation Protocol
SIM	Subscriber Identity Module
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SN	Subscriber Number
SR	“Systematische Sammlung des Bundesrechts” – Classified Compilation of Federal Legislation
TCE-O	Telecommunications equipment belonging to the obligated party (the CSP)
TCP	Transport Control Protocol
TDM	Time Division Multiplexing
UDP	User Datagram Protocol
UE	User Equipment
UMS	Unified Messaging System
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	8-bit Unicode Transformation Format (RFC 3629, ISO 10646)
UUS	User-to-User Signalling
VMS	Voicemail Service
VoIP	Voice over IP
VPN	Virtual Private Network
VÜPF	„Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11)“ - Ordinance of 31 October 2001 on Postal and Telecommunications Surveillance
WLAN	Wireless Local Area Network
xDSL	Digital subscriber line (x stands for various types)
XML	Extensible Markup Language

4. Terminology

Interception activity
Action (based on the law) of making available certain information and providing that information to the LEMF.

Interception order
A lawful authorization (warrant) sent from PTSS to the CSP for performing an interception activity.

Communications service provider (CSP)
The CSP is intended as the legal entity providing telecommunication services, including network operators, access providers and service providers.

Delivery network
Network infrastructure between the CSP and the LEMF used to transmit the results of interception data. It can support different types of lower communication layers, which should be standard or widely used data communication protocols.

Handover interface (HI) [7] §3.1
Physical and logical interface across which the interception measures are requested from network operator/access provider/service provider, and the results of interception are delivered from a network operator/access provider/service provider to a law enforcement monitoring facility.

Interception Related Information (IRI) [7] §3.1
Collection of information or data associated with telecommunication services involving the target identity, specifically communication associated information or data (including unsuccessful communication attempts), service associated information or data (e.g. service profile management by subscriber) and location information.

Law Enforcement Monitoring Facility (LEMF) [7] §3.1
Designated as the transmission destination for the results of interception relating to a particular interception subject. PTSS operates the LEMF in Switzerland.

Mediation Function (MF) [7] §3.1
Mechanism which passes information between a CSP and a Handover Interface, and information between the Internal Network Interface and the Handover Interface

Result of interception
Information relating to a target service, including the Content of Communication and Interception Related Information, which is passed by a CSP to the LEMF.

Target identity [7] §3.1
Technical identity (e.g. the interception's subject directory number), which uniquely identifies a target of interception. One target may have one or several target identities.

Target service [7] §3.1
Telecommunications service associated with an interception subject and usually specified in a lawful authorization for interception.

5. References

[1]	SR 780.1	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 06. Oktober 2000 - Federal Act of 6 October 2000 on Postal and Telecommunications Surveillance. Latest edition.
[2]	SR 780.11	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) vom 31. Oktober 2001 - Ordinance of 31 October 2001 on Postal and Telecommunications Surveillance. Latest edition.
[3]	OAR	Guidelines for Lawful Interception of Telecommunications Traffic, Organisational and Administrative Requirements
[4]	SR 784.101.1	Verordnung über Fernmeldedienste (FDV) vom 9. März 2007 - Ordinance of 9 March 2007 on Telecommunications Services
[5]	SR 120.4	Verordnung über die Personensicherheitsprüfungen (PSPV) vom 19. Dezember 2001
[6]	SR 235.1	Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 - Federal Act of 19 June 1992 on Data Protection
[7]	ETSI TS 101 671	Telecommunication security; Lawful interception (LI); Handover interface for the lawful interception of telecommunication traffic
[8]	VOID	
[9]	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
[10]	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
[11]	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
[12]	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
[13]	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
[14]	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
[15]	ETSI TS 102 232-7	Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services
[17]	ETSI TR 102 503	Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception and Retained data handling Specifications
[18]	ETSI TS 102 657	Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data

[19]	ETSI TS 133 108	Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI)
[20]	ITU-T X.690	ITU-T Recommendation X.690, 12/97; Data Networks and Open System Communication – OSI networking and system aspects – Abstract Syntax Notation One (ASN.1)
[21]	ETSI EN 300 403	Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signaling network layer for circuit-mode basic call control
[22]	ETSI ETS 300 974	European Telecommunication Standard (ETS) 300 974, 2000-12; GSM – Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification
[23]	ITU-T Q.931	ITU-T Recommendation Q.931, “ISDN user-network interface layer 3specification for basic call control”
[24]	ITU-T Q.763	ITU-T Recommendation Q.763, “Specifications of signalling System No.7; ISDN user part; Formats and codes”
[25]	ITU-T Q.699	ITU-T Recommendation Q.699, “Interworking of Signalling Systems – Interworking between Digital Subscriber Signalling System No. 1 and Signalling System No. 7
[26]	ETSI TS 129 002	Universal Mobile Telecommunications System (UMTS); Mobile Application Part (MAP) specification
[27]	ETSI TS 101 331	Telecommunication security; Lawful interception (LI); Requirements of Law Enforcement Agencies
[28]	ETSI ES 201 158	Telecommunication security; Lawful interception (LI); Requirements for network functions
[29]	RFC 5322	“Internet Message Format”, October 2008
[30]	RFC 2045 - 2049	“Multipurpose Internet Mail Extensions (MIME)”, November 1996
[31]	RFC 2821	“Simple Mail Transfer Protocol”, April 2001
[32]	RFC 2440	“OpenPGP Message Format”, November 1998
[33]	RFC 2279	“UTF-8, a Transformation Format of ISO 10646”, January 1998
[34]	RFC 1305	“Network Time Protocol (Version 3) Specification, Implementation and Analysis”, March 1992
[35]	RFC 4180	Common Format and MIME Type for Comma-Separated Values (CSV) Files
[36]	SR 784.101.113 / 1.7	Technische und administrative Vorschriften betreffend die Identifikation des anrufenden Anschlusses (BAKOM/OFCOM)
[37]	ETSI ES 282 002	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);PSTN/ISDN Emulation Sub-system (PES)
[38]	ITU-T E.164	ITU-T Recommendation E.164, Numbering plan of the international telephone service
[39]	ITU-T E.123	ITU-T Recommendation E.123, Notation for national and international telephone numbers, e-mail addresses and Web addresses
[40]	ITU-T G.711	ITU-T Recommendation G.711, Pulse code modulation (PCM) of voice frequencies
[41]	ITU-T H.248	ITU-T Recommendation H.248, Gateway control protocol
[42]	ITU-T H.323	ITU-T Recommendation H.323, Packet-based multimedia communications systems
[43]	TR TS Roadmap	Technical Requirements for Telecommunication Surveillance Roadmap.

[44]	TR-CS v2.0	Technical Requirements for the Delivery of the results of interception, Circuit Switched Services TR-CS, version2.0, January 1st, 2008
[45]	TR-CS HD v2.0	Technical Requirements for the Delivery of Historical Data Circuit Switched Services, TR-CS-HD, version 2.0, January 1st, 2008
[46]	TR-PS Email v2.0	Technical Requirements for the Delivery of Intercepted Electronic Mail, Packet Switched Services, TR-PS-EMAIL, version 2.0, January 1st, 2008

Notes:
ETSI: For this publication the version according to the list of Object Identifiers are applicable. The choice of the version depends on the service to be intercepted.

IETF RFC: In the case that a referenced RFC has been obsoleted or updated by another RFC this new RFC applies, the choice of the specific RFC depends on the service to be intercepted.

6. Lawful Interception Reference Model

The following figure provides an overview of the entire real-time interception System.

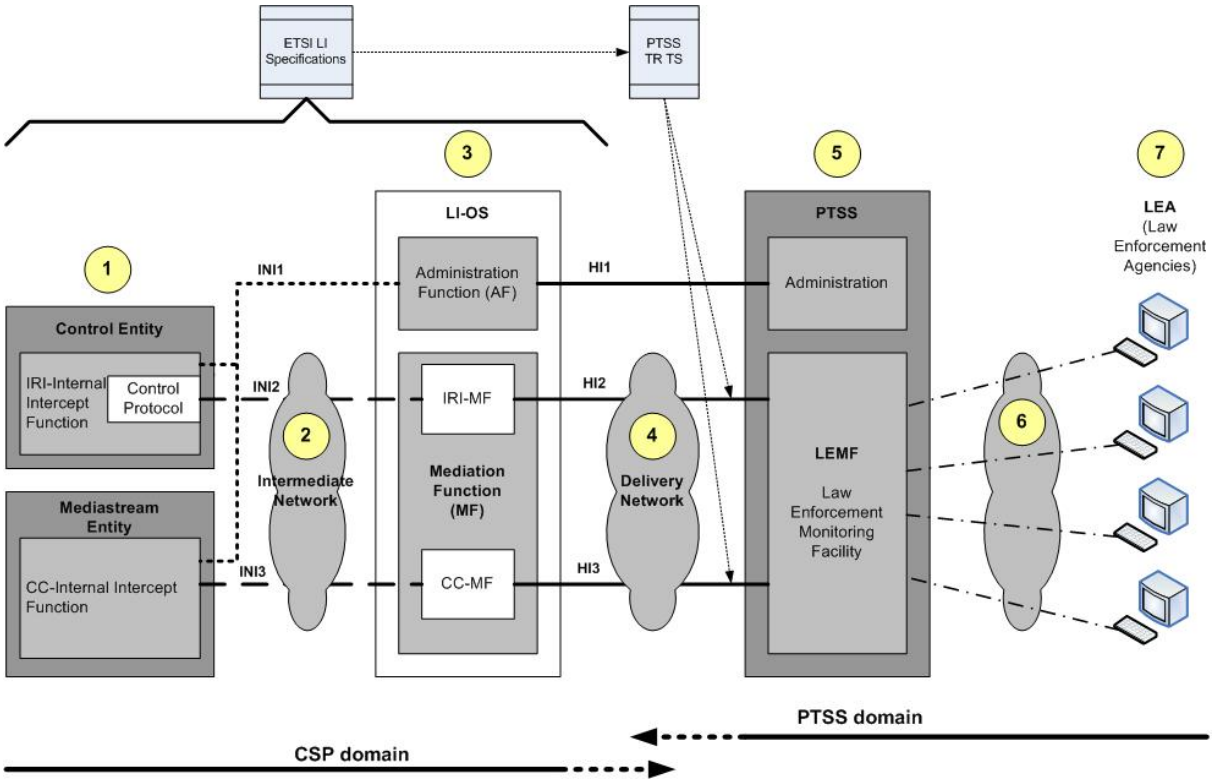

Figure 1: Lawful interception model for real-time interception

IIF: Internal Interception Function
INI: Internal Network Interface
LI-OS: LI Operations System
MF: Mediation Function
AF: Administration Function
LEA: Law Enforcement Agencies
HI1: Handover Interface for administrative information
HI2: Handover Interface for Intercept Related Information
HI3: Handover Interface for Content of Communication

Note: HI1 interface may be established through delivery network ④ in the future as well.

According to the figure above, the “End-to-End System” may be subdivided into 7 sections with the properties described below:

1. The Internal Interception Function (IIF) residing in the platform for replication media stream information (CC-IIF) to be delivered, after some adaptation, as Content of Communication (CC) across HI3. The IIF residing in the platform for replication of control information (IRI-IIF) to be delivered, after some adaptation, as Interception Related Information (IRI) across HI2.
2. The intermediate network supports various Internal Network Interfaces (INI). It conveys the intercepted information from IIFs to Mediation Functions (MF) of the LI-OS (LI Operations System). It also conveys information allowing the Administration Function (AF) of the LI-OS to manage various IIFs.

3. The LI-OS for the purpose of LI-Management consists of the MF and the AF. The MF converts the CC in the format at HI3 (CC-MF), and the IRI in the format at HI2 (IRI-MF), as appropriate (see note below). The AF is used for LI-Administration and also provides to LI-operation staff terminals to the CSP.

   NOTE: It is a matter of LI-architecture and implementation where the MF resides, being a choice of the CSP. It may be co-located with AF in a physical entity, reside in a separate physical entity, or be co-located with IIF.

4. The Delivery Network which delivers the intercepted information to the LEMF.
5. PTSS platform providing services to various Law Enforcement Agencies.
6. The Delivery Network between the LEMF and various Law Enforcement Agencies.
7. The terminal equipment for Law Enforcement Agency organisations.

7. Definition of Target Identities

The definition of target identities is subject to the type of service produced by the CSP and may have many different formats that shall be defined bilaterally between CSP and PTSS.

As guidance, some used and well known target identities are listed in [3] section 6.2

8. Technical Interface HI1

Current technical interface HI1 description is in [3] section 8.

Note: This section may be used in the future to define the technical requirements of the HI1 interface according to the Draft ETSI Draft Technical Report 103 690, also known as “eWarrant”.

9. Dimensioning of Interception Capabilities

9.1. Dimensioning for circuit-switched services interceptions

The minimum number of concurrent interceptions that need to be configurable at the source equipment is as follows:

$$\mathbf{M = 0{,}35 * x^{0{,}45} + p}$$ (**M** shall be rounded up to the next integer value)

where
M = minimum number of concurrent interceptions configurable at the source equipment
x = number of channels potentially subject to interception served by the equipment (for clarification: An ISDN BA consists of two served channels, corresponding to the two B-Channels). In case of a mobile network, the sum of the MSCs is to be regarded as one source switch
p = **30** in case the equipment serves at least one PRA, **0** in case the source equipment does not serve any PA.

This formula is subject to possible future change, based on experience to be gained in the future.

9.2. Dimensioning for packet-switched services interceptions

9.2.1. Dimensioning for mobile data services interceptions

In the context of mobile data services interceptions the dimensioning parameters are set as objectives only, due to the fact that these interceptions types are new and the CSP and PTSS have no experience with the expected traffic patterns. The objectives described below are meant to help CSP and PTSS to initially plan the dimensioning of their respective infrastructure.

The objectives are twofold; a) the minimum number of PDP contexts being intercepted that need to be configurable at the source equipment and b) the maximum aggregated bandwidth of the simultaneous interceptions on the source equipment.

In the context of mobile data services the source equipment is considered to be the entire mobile network. As the IIF instances are distributed through the different network elements, depending on the CSP network configuration.

a) The minimum number of concurrent PDP context interceptions that need to be configurable at the source equipment is as follows:

$$\mathbf{M = c * 0{,}35 * x^{0{,}45}}$$ (**M** shall be rounded up to the next integer value)

where

M = minimum number of concurrent PDP context interceptions configurable at the source equipment
c = factor defining the relationship between the number of PDP context and the number of voice channel (according to section 9.1). Each CSP has to define this value taking into account its own statistics on service offers.
x = the maximum number of channels that can be configured in the source equipment.

b) The source equipment shall be able to support a maximum aggregated bandwidth according to the traffic dispersion evaluated by each CSP in its own network.
As an example the estimation of the used bandwidth can be calculated based on the assumed traffic dispersion according the example below:

Internet [Mb/s]	dispersion * bandwidth * M	[30% * 0.15 Mb/s * M]
DSL Substitution [Mb/s]	dispersion * bandwidth * M	[30% * 0.25 Mb/s * M]
Mobile TV [Mb/s]	dispersion * bandwidth * M	[20% * 0.5 Mb/s * M]
Other [Mb/s]	dispersion * bandwidth * M	[20% * 0.1 Mb/s * M]

These objectives are subject to possible future change, based on experience to be gained in the future.

9.2.2. Dimensioning for email services interceptions

The minimum number of email-boxes being intercepted that needs to be configurable at the source equipment is as follows:

$$M = 0{,}02 * x^{0{,}45}$$ (**M** shall be rounded up to the next integer value.)

where
M = minimum number of mailboxes being intercepted configurable at the source equipment. An email account may include more than one mailbox, depending on the service offered by the CSP.
x = the maximum number of mailboxes that can be configured in the equipment.

This formula is subject to possible future change, based on experience to be gained in the future.

9.2.3. Dimensioning for internet broadband services interceptions

In the context of internet broadband services interceptions the dimensioning parameters are set as objectives only, due to the fact that these interceptions types are new and the CSP and PTSS have no experience with the expected traffic patterns. The objectives described below are meant to help CSP and PTSS to initially plan the dimensioning of their respective infrastructure.

The objectives are twofold; a) the minimum number of IP broadband accounts being intercepted that need to be configurable at the source equipment and b) the maximum aggregated bandwidth of the simultaneous interceptions on the source equipment.

In the context of internet broadband services the source equipment is the network element where the IIF resides (e.g. BRAS, CMTS, IP Services Router)

a) The minimum number of internet broadband accounts being intercepted that needs to be configurable at the source equipment is as follows:

$$M = 0{,}04 * x^{0{,}45}$$ (**M** shall be rounded up to the next integer value.)

where
M = minimum number of internet broadband accounts being intercepted configurable at the source equipment.
x = the maximum number of internet broadband accounts that can be configured in the source equipment.

b) The source equipment IIF shall be able to support a maximum aggregated bandwidth of 100Mbps. If this threshold is exceeded in the source equipment the CSP is not responsible for the potential loss of the intercepted traffic; however, the CSP must notify PTSS in order to address the issue and possibly find a common solution to solve it within the limit of the CSP existing technical and organizational capabilities.

These objectives are subject to possible future change, based on experience to be gained in the future.

9.2.4. Dimensioning for VoIP and other multimedia services

The minimum number of concurrent multimedia interceptions that need to be configurable at the source equipment is as follows:

$$M = 0{,}35 * x^{0{,}45}$$ (**M** shall be rounded up to the next integer value)

where
M = minimum number of concurrent interceptions configurable at the source equipment
x = in multimedia domain:

i) for source equipment for IRI, the maximum number of user accounts that can be handled by the equipment where IIF resides.
ii) for source equipment for CC, the maximum number of concurrent sessions that can be handled by the equipment where IIF resides.

This formula is subject to possible future change, based on experience to be gained in the future.

10. Delivery of Retained and Historical Data and of Technical and Administrative Information

This section covers the general technical requirements that need to be fulfilled by the CSP when providing historical data.

10.1. Delivery of Retained data according to ETSI specification TS 102 657 [Informative]

This section is for further study and will be completed in a future version of TR TS according to the evolution of the legal provisions and LEMF capabilities.
Informative technical description can be found in the document TR TS Roadmap [43].

10.2. Delivery of historical data according to Swiss proprietary mechanism and procedure

10.2.1. Delivery of historical data for the circuit-switched domain

This section specifies a national solution for the delivery of historical data for circuit-switched services.
An implementation which meets the requirements herein is backward compatible to an implementation according to “Technical Requirements for the delivery of Historical Data, Circuit Switched Services, version 2.0”, [45]

10.2.1.1. Target Identities

In case of a fix network target a CSP must be able to deliver historical data and support a target identity as follows:

1. In case of an analog subscriber per individual SN
2. In case of a BA per individual MSN.
3. In case of a PRA per DDI number, if available (i.e. provided by the customer).

In case of a mobile target a CSP must be able to deliver historical data and support a target identity as follows:

1. IMEI
2. IMSI
3. MSISDN

For all the above target identities, historical data interception must be supported and historical data delivered for communication sessions originated, terminated and forwarded by the target.

10.2.1.2. LI identifier

In order to achieve a unique identification of the interception delivery, the lawful interception identifier LIID (specified and delivered by PTSS) is inserted into the information flow from the

CSP to the LEMF. The LIID is a numeric value of up to 15 digits, as described in 11.2.1. The properties of the LIID are described in [7] clause 6.1, while the context in which it is to be used for historical data is specified in section 10.2.1.5

10.2.1.3. Outbound roaming data

Outbound roaming data (calls related to a mobile target roaming abroad) are also within the scope of historical data. The requirements for handling outbound roaming data within the scope of delivery of historical data are defined as follows:

1. Outbound roaming data are to be included and delivered as part of the whole set of historical data. The complete set of interception results has to be processed and delivered by the CSP as defined in the following chapters in this section. The delivery must include the outbound roaming data that is processed within the reaction time of the interception order and that is within the scope of the corresponding interception period.
2. Format, content and delivery method are all the same for the whole set of historical data (including outbound roaming data).
3. The CSP reaction time for historical data interception orders (as in [3]) is not influenced by the outbound roaming data. In case of “high” priority, the focus shall be on fast delivery, rather than outbound roaming data completeness.
4. In exceptional cases, when the authorities issue a second interception order at a later stage in order to complete the outbound roaming data, this second interception order will be a new and independent order to the CSP. There is no requirement for the CSP to avoid duplication of data delivery in such cases.

10.2.1.4. Delivery mechanism

This chapter specifies the mechanisms that are to be put in place for the exchange of historical data, i.e. interception type CS 4 according to [3], between the CSP and PTSS. The delivery mechanism defined herein is thereby similar to the delivery mechanism for electronic mail interception.

10.2.1.4.1. *Transmission medium*

The results of the historical data interception shall be packed into a *MIME-conform* [29, 30] *delivery messages*, which must subsequently be signed and encrypted (see section 10.2.1.6). The resulting container emails must be delivered to the LEMF through the *Internet* according to [31]. For each interception order a specific mailbox is maintained at the LEMF.

Examples of the structure and contents of container emails are given in section 16.3.

10.2.1.4.2. *Container Email size restrictions*

Due to capacity limitations it might be possible that the corresponding container emails are too large for successful delivery. Therefore it is allowed to split the interception results into several container emails.
The following rules apply to the minimum and maximum size of a container email:

1. The size of a container email must not exceed 10 MB.
2. If possible all the interception results should be sent in one single container email.
3. If a single container email would exceed either the CSP internal email size restrictions or the limitation of 10 MB, the interception results have to be split into several container emails.

Each of the resulting container emails should be as large as possible according to the corresponding limitations.

4. The size of the container emails should be configurable at the CSP system to be able to respond to network problems and changes.

10.2.1.4.3. *Creation of multiple Container Emails*

The following rules apply if the results of interception have to be split into several container emails:

1. All the historical communication sessions within a container email have to be complete. A historical communication session must not be split into several container emails.
2. Interception results within a container-email must be presented in the XML document, which is defined by the XML document type definition in section 16.3.
3. Interception results within a container-email must be signed and encrypted according to chapter 10.2.1.6. For all the resulting container emails the same LIID-specific keys will be used.
4. There are no requirements concerning the distribution of historical communication sessions to multiple container emails and the order of historical communication sessions within a container email.

10.2.1.4.4. *Delivery of multiple Container Emails*

The whole series of container emails that belongs to the same interception order must be sent together. The time delays between the sending of the corresponding container emails must be kept as small as possible.

10.2.1.5. Delivery parameters

The contents of the header fields *From*, *To*, and *Subject* of a container email (according to [30]) are defined as follows:

From: *"LI_monitor@" CSP-domain* (denotes the sender's address)
To: *LIID "@" LEMF-domain* (denotes the recipient's address)
Subject: *"CS4_" major-version "." minor-version " " mail-nr "/" number-of-mails*

The variables are defined as follows:

CSP-domain:	The domain name of the CSP.
LIID:	The lawful interception identifier.
LEMF-domain:	The domain name of the LEMF.
major-version:	A single digit representing the major version of the format of the results of interception that are included in the container email. *"1"* is the current major version.
minor-version:	A single digit representing the minor version of the format of the results of interception that are included in the container

email.
"0" is the current minor version.

mail-nr: Current number of container email within the set of multiple container emails.

number-of-mails: Total amount of container emails.

Example: A CSP with the domain name *"examplecom.ch"* having received an interception order with the LIID *"200312310123456"* and sending three container emails containing the results of interception, will configure these emails for the delivery as follows:

From: *"LI_monitor@examplecom.ch"*
To: "200312310123456@" *LEMF-domain*
Subject: "CS4_1.0 1/3"

From: *"LI_monitor@examplecom.ch"*
To: "200312310123456@*" LEMF-domain*
Subject: "CS4_1.0 2/3"

From: *"LI_monitor@examplecom.ch"*
To: "200312310123456@*" LEMF-domain*
Subject: "CS4_1.0 3/3"

10.2.1.6. Security mechanism

For authentication, integrity and confidentiality reasons, the contents of any delivery message must be signed and encrypted using OpenPGP [32].
For each interception order, both the CSP and the LEMF generate a separate pair of LIID-specific public/ private keys. The keys are exchanged and used as follows (see also [3]):

a) The LEMF transmits its LIID-specific public key to the CSP as an attachment to the interception order[1]

b) The CSP transmits its LIID-specific public key to the LEMF as an attachment to the technical confirmation[2]

c) The CSP transmits its results of interception by *signing* the contents with the LIID-specific private key generated by the CSP and *encrypting* the contents with the LIID-specific public key generated by the LEMF

d) The signing and encrypting of the results of interception have to be carried out in two subsequent steps, i.e. first signing then encrypting. Signing and encrypting must not be combined into one single step

[1] Note that for the email exchange on the administrative interface, the requirements according to section 8 apply, including separate PGP-requirements on this interface.
[2] According to [3]

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

f) The MIME entity is signed using the SHA-1 hash algorithm and encrypted applying the Triple-DES algorithm.

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

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

i) The LIID has to be put in the email address field of the LIID-specific keypair generated by the CSP (*LIID@CSP-domain*); this identification is used for correct assignment of the key to the interception order

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

10.2.1.7. Delivery failure

Every container email sent to the LEMF must be confirmed by the LEMF by sending an end-to-end reception confirmation email with the following header fields:

From: *LIID "@" LEMF-domain* (denotes the sender's address)

To: *"LI_monitor@" CSP-domain* (denotes the recipient's address)

Subject: *"Re: " original-subject*

The variables are defined as follows:

LIID:	The lawful interception identifier.
LEMF-domain:	The domain name of the LEMF.
CSP-domain:	The domain name of the CSP.
original-subject:	The subject of the original container email.

If a container email cannot be delivered to the respective recipient mailbox at the LEMF, or in case of a missing reception confirmation, the corresponding container email must be resent periodically by the CSP. If undeliverable or no reception confirmation is received, a bounce must occur latest after 1 working day (24 hours). In this case the CSP contacts the PTSS to negotiate an alternative transmission mechanism.
In any case, the CSP must store any results of interception of historical data until this data is delivered successfully to the LEMF.

10.2.1.8. Data specifications

This section specifies the details of the historical data that needs to be provided by the CSPs.

10.2.1.8.1. *Data format*

The results of interception must be presented in a well-formed, valid XML document. The XML document type definition to be used is given in section 16.3. The complete set of historical data to be delivered is defined within one single XML document type definition.

The characters "<" and "&" must be substituted by their character entities, i.e. *"<"* and *"&"*, respectively.

The XML document containing the results of interception must be included inline in a delivery message as *text/plain* MIME-content type with character set *UTF-8* [33].

10.2.1.8.2. *Data content*

In [2], art. 16 letter d the data to be provided are defined, the details of each are specified below.

10.2.1.8.3. *Address elements*

The following addressing and related information elements need to be provided as available to the CSP for each communication session of the target that took place within the interception period:

Address-information	
Element	Description
calling-number	The number of the party which originates the communication session, that is either the target or a third party. The communication session can thereby be a call, a UUS or an SMS. The calling-number shall meet the following requirements: 1. In case of an SMS terminated at the target, the calling party number shall contain the number conveyed in the field that identifies the originator of the SMS. The number of the SMS-center of the mobile network shall not be delivered in addition[3]. 2. The calling-number shall be delivered in international format for international numbers and in national format for national numbers. If the format is unknown to the CSP, the number shall be delivered as available. 3. For numbers with international format the country code is preceded by "+", for numbers with national format the local area code is preceded by "0" (prefix). 4. The calling-number element must always be transmitted. In case the calling-number is not available, the respective empty XML-element must be provided.
called-number	The number of the party which was originally called by the originator of the communication session, that is either the target or a third party. The communication session can thereby be a call, a UUS or an SMS. The called-number shall meet the following requirements:

[3] If the number of the real originator is not available, the calling-number field shall be left empty. The number of the SMS-center shall only be provided by the CSP if the SMS-centre represents the real originator itself (e.g. SMS information services).

	1. In case of an SMS originated by the target, the called party number shall contain the receiver of the SMS, as supplied by the sender of the SMS. The number of the SMS-center of the mobile network shall not be delivered in addition[4]. 2. The called-number shall be delivered in international format for international numbers and in national format for national numbers. If the format is unknown to the CSP, the number shall be delivered as available. 3. For numbers with international format, the country code is preceded by "+", for numbers with national format the local area code is preceded by "0" (prefix). 4. The called-number element must always be transmitted. In case the called-number is not available, the respective empty XML-element must be provided.
forwarded-to-number	In case of call forwarding, this number denotes the number of the party to whom the called party has forwarded the call. The forwarded-to party is either the target or a third party[5]. Example: If A calls B and the call is forwarded to C, then the number of A is the calling party number, the number of B the called party number, and the number of C the forwarded-to-number. The forwarded-to-number shall meet the following requirements: 1. If a call has been forwarded multiple times, the retrievable forwarded-to-number elements must be delivered in the order of the original forwarding sequence. 2. There is no mandatory requirement to correlate address information created at various switches (and belonging to the same connection). 3. The forwarded-to-number shall be delivered in international format for international numbers and in national format for national numbers. If the format is unknown to the CSP, the number shall be delivered as available. 4. For numbers with international format, the country code is preceded by "+",for numbers with national format the local area code is preceded by "0" (prefix). 5. The forwarded-to-number element must only be transmitted when applicable, i.e. when a call forwarding has actually taken place, and when the number is retrievable. 6. If it is known to the CSP-implementation that a call forwarding

[4] If the number of the real receiver is not available, the called-number field shall be left empty. The number of the SMS-center shall only be provided by the CSP if the SMS-centre represents the real receiver itself.

[5] In general, the party identified by a specific forwarded-to-number may take different positions in relation to the target in the hop-by-hop connection establishment – preceding to the target, the target itself, subsequent to the target

	has taken place, but the forwarded-to-number is not retrievable, the respective empty XML-element must be provided.
csi (attribute)	Communication Session Identifier: This parameter provides supplementary information about the nature of the underlying communication session, see table below. The CSI attribute must always be delivered.

The element *"csi"* can assume several types, each of which describing the particular nature of the communication session. The following table describes the available CSIs:

Communication Session Identifier (csi)		
Type	Syntax	Description
TOC	"toc"	Target Originated Call : A call originated by the target.
TTC	"ttc"	Target Terminated Call: A call terminated by the target.
TFC	"tfc"	Target Forwarded Call: A call forwarded by the target.
TOU	"tou"	Target Originated UUS: A UUS sent by the target.
TTU	"ttu"	Target Terminated UUS: A UUS received by the target.
TOS	"tos"	Target Originated SMS: An SMS sent by the target.
TTS	"tts"	Target Terminated SMS: An SMS received by the target.

10.2.1.8.4. *Mobile parameter elements*

The following parameter element related to mobile networks need to be provided for each mobile communication session of the target that took place within the interception period:

Mobile-parameter-information	
Element	Description
Imei	The IMEI of the target.

Mobile parameter information must only be transmitted when applicable, i.e. when the target is a mobile subscriber. If the target is a mobile subscriber, but the mobile parameter information is not available, the respective empty XML-element must be provided.

10.2.1.8.5. *Mobile location elements*

The following location elements related to mobile networks need to be provided for each mobile communication session of the target that took place within the interception period.

Mobile-location-information	
Element	Description
antenna-coordinates	The coordinates of the cell antenna serving the target, represented as Swissgrid CH1903 coordinates (including x- and y-coordinates).
main-beam	Three-digit representation of the main beam direction of the cell antenna serving the target. The main beam direction refers thereby to the two-dimensional horizontal middle compass angle (in degrees 0-360) of the corresponding cell sector, e.g. *"010"* or *"325"*. In case of an umbrella-sector, the value –1 shall be inserted in this field.
antenna-address	The address of the cell antenna serving the target.

	The address shall be expressed as follows: *street [SP] housenumber ";" [SP] postal-code [SP] locality* The components of these elements are defined as follows: *street*: The name of the street where the antenna is located. *housenumber*: The housenumber where the antenna is located, e.g. *"27"* or *"4a"*. *postal-code*: Four-digit representation of the postal code of the location where the antenna is located, e.g. *"8001"*. *locality:* The name of the city, village or area (as applicable) where the antenna is located. The components are to be inserted as available and applicable. For example, an antenna location in a rural area will contain only the *locality* component, while an antenna on a building will contain the other components as well. If there is only a general location description the corresponding information shall be inserted as available. In case of outbound roaming calls[6] the country name of the corresponding foreign roaming partner must be inserted.
cell-id	The cell ID of the cell antenna serving the target.
Phase (attribute)	This parameter denotes the phase of the communication session the location information relates to. It can be set to either *"begin"* or *"end"*.

Mobile location information must only be delivered for the cell antennas serving the target. They must be delivered for cells serving the target at the beginning and at the end of the communication session.

Mobile location information must only be transmitted when applicable, i.e. when the target is a mobile subscriber. If the target is a mobile subscriber, but the mobile parameter information is not available, the respective empty XML-element must be provided.

10.2.1.8.6. *Duration elements*

For each communication session of the target that took place within the interception period, the duration elements of the underlying communication session shall be delivered as follows:

Duration-information	
Element	Description
start-date-time	The date and time of the beginning of the communication session. This parameter shall be delivered as a timestamp as follows: *year month day [SP] hours ":" minutes ":" seconds [SP] country* The components of this timestamp are defined as follows: year: Four-digit representation of the year month: Two-digit representation of the month, i.e. one of

[6] Calls of a CSP customer roaming abroad

	the following values: *"01", "02", "03", ... , "12"*. day: Two-digit representation of the day of the month, i.e. one of the following values: *"01", "02", "03", ...* , number of the days allowed for the specific month. hours: Two-digit representation of the hours of the time, i.e. one of the following values: *"00", "01", "02", ... , "23"*. minutes: Two-digit representation of the minutes of the time, i.e. one of the following values: *"00", "01", "02", ... , "59"*. seconds: Two-digit representation of the seconds of the time, i.e. one of the following values: *"00", "01", "02", ... , "59".* country: Representation of the country name the time-stamp is related to, e.g.: *"CH", "USA", "AUS-TRIA"*, etc. The exact naming of the country is left to the discretion of the CSP. In case the country name is not known to the CSP, this field shall be filled with the string "UN-KNOWN". In case of a Swiss national call, the time value is to be delivered in terms of Swiss local time. In case of a timestamp from outside Switzerland, the time value is delivered as available from the for-eign partner. This element must always be delivered.
Duration	The duration of the communication session. This parameter shall be expressed in seconds (i.e. one number representing the total amount of seconds of the duration of the communication session). In case of a UUS or an SMS, the respective empty XML-element must be provided, alternatively it can be set to *"0"*, i.e. zero sec-onds. In case of the target having forwarded a call and not being part of the call itself, the respective empty XML-element must be provided. This element must always be delivered.

10.2.2. Delivery of historical data for packet-switched domain according to Swiss national proprietary mechanism.

The delivery of historical data for packet-switched domain is specified in section 12.2.2

11. Circuit-switched Domain Real-Time Interception

This section describes the national requirements of the handover interfaces for circuit-switched real-time interceptions.

Based upon the circuit-switched services provided by the CSP, the lawful interception data shall be carried out on the handover interfaces in conformity with the specifications stated in the following table:

Type	Circuit-switched Services	ETSI Specification	Sections
Fix	PSTN, ISDN	TS 101 671 [7]	11.1, 11.2, 11.3
Mobile	GSM (Phase 1 & 2, Releases 96 to 98)	TS 101 671 [7]	11.1, 11.2, 11.3
Mobile	UMTS 3GPP Releases 99, 4 and 5	TS 101 671 [7]	11.1, 11.2, 11.3
Mobile	UMTS 3GPP from Release 6 and higher	TS 133 108 [19]	11.1, 11.2, 11.4

Note: For UMTS services Third Generation Partnership Project (3GPP), the standards organisation which created the endorsed technical specification ETSI TS 133 108, draws up provisions for this technical specification corresponding to each version of the standard releases which standardise these telecommunications systems.

11.1. Circuit-switched domain: Landline PSTN & ISDN and Mobile Networks (GSM & UMTS) according to ETSI TS 101 671 and UMTS Release 6 and higher according to ETSI TS 133 108

An implementation which meets the requirements herein is backward compatible to an implementation according to “Technical Requirements for the delivery of the results of interception, Circuit-switched Services, version 2.0”, [44]

The general requirements for this section are described in the following sections:

Section	Content
9.1	Dimensioning for circuit-switched services interceptions
16.5	Applicable ETSI Standards and Specifications as well as ASN.1 Modules
13.2	Circuit-switched services interceptions

11.2. Lawful interception identifiers for circuit-switched domain

The following identifiers are inserted into the information flow of both the CC and the IRI data related to circuit-switched domain for achieving a unique identification of the interception target and to correlate CC and IRI data at the LEMF:

11.2.1. LIID

The LIID according to [7] clause 6.1 and [19] clause 5.1 consists of maximum 25 numbered digits (0..9) for the sub-address option according to [7] annex E. LI in Switzerland supports the LLID format for sub-address option according to [7] Annex E, but requires only a maximum of 15 numbered digits (0..9).

Requirements specified by ETSI shall be met as follows:

a) The LIID passed to LEMF when a CC-link is being established shall meet the requirements specified in [7] Annex E, in particular Table E.3.5, where digit 1 is the most significant digit. After the last digit (maximum digit 15), the field separator determines the end of the field. The subsequent field “direction” in table E.3.5 shall be rearranged, i.e. mapped into octet 12, whereas the service octets must still be mapped into octets 19-23.
b) The LIID passed to LEMF when an IRI-Record is being delivered shall meet the requirements specified in [7] Annex D.5. The specification of the IRI-Parameter LawfulInterceptionIdentifier for the sub-address option shall apply using ASCII encoding.

   The specific LIID is provided to the concerned CSP by the PTSS. In case of multiple CSPs intercepting on the same target identity relating to one specific interception order, PTSS assigns the same LIID to be used by these various CSPs for the interception of this target identity.

11.2.2. CID – Network ID

11.2.2.1. OperatorID

The OperatorID in Switzerland has a format of 5 digits. It is issued and provided to the CSP by PTSS and has the following format:

N	N	N	N	N

Requirements specified by ETSI shall be met as follows:

a) For insertion of the OperatorID in the Subaddress field, [7] Annex E applies.
b) For the OperatorID contained within an IRI-Record, [7] Annex D.5 IRI-Parameter operator-Identifier applies.

11.2.2.2. NEID

The network element identifier distinguishes between the various source IIF carrying out the LI operations and thus potentially serving the LEMF. For the NEID, the E.164 number format shall be used and the Numbering Plan Identification shall be “ISDN/telephony numbering plan”.

Requirements specified by ETSI shall be met as follows:

a) For the NEID passed to LEMF within the Calling Party Number information element, the encoding of the NEID according to [7] Annex E, clause E.4.2 applies, with the following clarification: The CSP shall make provision that at the Handover Interface the Calling

Party Number is delivered to the LEMF in one of the formats specified below, the choice (on a call-by-call basis) being a CSP option:

i. national number with Type of Number “unknown” with prefix (in Switzerland the prefix is “0”)
ii. national number with Type of Number “national number”
iii. international number with Type of Number “unknown” with prefix (in Switzerland the prefix is “00”)
iv. international number with Type of Number “international number”

b) For the NEID contained within an IRI-Record, [7] Annex D.5 IRI-Parameter Network-Element-Identifier applies. This IRI-Parameter is always in E.164 international format.

11.2.3. CIN

The communication identity number distinguishes between the various specific communications calls of one certain LI activity. It shall be assigned by the CSP, with a length of between 5 and 8 numbered digits.

Requirements specified by ETSI shall be met as follows:

a) For the format of the CIN conveyed within the Called Party Subaddress when a CC-link is being established, [7] annex E applies with the exception, that the minimum required number of digits is 5.
b) For the format of the CIN conveyed as IRI Parameter communication-Identity-Number, [7] Annex D.5 shall apply, with the CIN being encoded in one of the following formats:
   i. ASCII. In this case the length of the CIN within IRI shall be in the range of 5 up to 8 digits.
   ii. two’s complement according to [20], § 8.3. In this case the length of the CIN-field within IRI shall not exceed 4 bytes.

   The CSP shall indicate to the PTSS which format is supported by which MF.

11.2.4. CCLID

The CCLID shall not be used, as for multiparty calls option A is to be implemented ([7] Annex A.1.1 and A.5.4.2).

11.2.5. Transmission of identifiers

The identifiers are to be transferred as follows:

1. CC link: The identifiers shall be transmitted in the D-Channel (that is, in the D-Channel of the respective CC link of the HI3 interface) when a CC link is established, using a DSS1 SETUP Message, within the Calling Party and Called/Calling Party Subaddress information elements.

   ETSI: Subaddress option according to [7] Annex E applies.
2. IRI link: The identifiers shall be transmitted within every IRI record, to allow correlation at the LEMF.

11.3. Selected and Required Options as well as Extended Technical Requirements according to ETSI specification TS 101 671 (PSTN, ISDN, GSM, UMTS)

Clause TS 101 671	Selection of ETSI options for Switzerland	Additional requirements
5.1	**Manual/Electronic handover interface 1 (HI1)** An electronic handover interface from the LEMF to the obligated party's technical infrastructure for direct administration of interception measures without the involvement of the obligated party is not implemented in Switzerland. Events regarding the management of an interception (e.g. activation and deactivation) and error communication must be delivered.	See section 8
6.2.1	**Network identifier (NID)** The NID is composed of 5 digits: NWO/AP/SvP identifier (Operator identifier). PTSS provides the Operator identifier.	
8.1	**Data transmission protocol** FTP is used for IRI data, HI1 notifications and packetized CC such as SMS and UUS. (see [7] Annex A.4.2. ROSE is not allowed. The FTP connection must be closed immediately after data transmission.	See section 11.3.2
11	**Security aspects** For CC over ISDN, CLIP and COLP services are used.	CUG does not need to be implemented.
Annex A: Circuit switched network handover		
A.1.3	**Usage of identifiers** Options "IRI and CC" and "only IRI" option must be supported. Option "only CC" does not need to be implemented.	
A.3.2.1	**Control information for HI2** The timestamp must include official local time and related DST indication.	
A.4.1	**Delivery of Content of Communication**	

Clause TS 101 671	Selection of ETSI options for Switzerland	Additional requirements
	For relating CC data to other H-Interfaces the subaddress service will be used as specified in [7] Annex E instead of the user-to-user signalling.	CC data must be A-law coded in compliance to ITU-T G.711, i.e. in case of different coding in the original channel (e.g. GSM) the mediation function must ensure conversion to A-law coding. As an alternative to the Bearer Capability (BC) of the value "UDI", the BC can take the value used in the intercepted call, the choice being a CSP option.
A.4.2	**Delivery of packetized Content of Communication** For SMS and UUS Services, CC will be transferred as IRI. For transferring CC data, the ASN.1 module 'HI2Operations' according to annex D.5	
A.4.3	**Control information for circuit switched Content of Communication** The terminal end point of PTSS replies to a SETUP message immediately with a CONNECT message, i.e. without any ALERTING message.	
A.4.5	**Security requirements at the interface port HI3** ISDN Service specifications CLIP and COLP must be used for creating CC links to PTSS.	CUG does not need to be implemented.
A.4.5.3	**Authentication** A special authentication procedure within the ISDN B Channel or within the Subaddress is not used.	
A.5.4	**Multi party calls – general principles** Only option A is available and must be used.	
A.6.3	**Call Hold/Retrieve** If an active call is put on hold, its CC link shall stay intact and the signal from the held party shall be switched through to the LEMF. If the target sets up a new call, while one call is on hold, this call shall be treated as a normal originating call (additional CC link) [7] Annex A.6.3.1 applies. CC links shall stay intact and the signal from the held party shall be switched	

Clause TS 101 671	Selection of ETSI options for Switzerland	Additional requirements
	through.	
A.6.4	**Explicit Call Transfer (ECT)** For explicit call transfer, Option 2 must be implemented. This means, that the transferred call must not be intercepted.	
A.6.16.1.1	**Call Diversion by target, CC links** For CFNR, UDUB, CD and partial rerouting, option 2 (with CONTINUE-Record) must be implemented.	
A.6.22	**User-to-User Signalling (UUS)** UUS service data will be delivered as IRI data.	See point A.4.2 in this Table.
A.8.3	**HI3 (delivery of CC**) SMS service data will be delivered as IRI data. For relating CC to the other H-Interfaces, Subaddress Service described in [7] Annex E must be used. The provider must remove encryption algorithm applied by the CSP internally in the network at the handover interface.	See point A.4.2 in this Table.
Annex C: HI2 Delivery mechanisms and procedures		
C.1 / C.2	**ROSE / FTP** FTP must be used for transferring IRI data over HI2-Interface; ROSE is not allowed.	See point 8.1 in this Table.
C.2.2	**Usage of FTP** For conveying IRI data transmission must be triggered neither by timeout nor by volume. File naming method B must be used. Additionally, section 11.3.2 applies as well.	
Annex D: Structure of data at the Handover Interface		

D.4	`HI1-Operation ::= CHOICE`
	`{`
	`  liActivated`
	`  [1] Notification,`
	`  liDeactivated`
	`  [2] Notification,`
	`  liModified`
	`  [3] Notification,`
	`  alarms-indicator`
	`  [4] Alarm-Indicator,`
	`  ...,`
	`  national-HI1-ASN1parameters`
	`  [5] National-HI1-ASN1parameters`
	`}`
		Implementations at CSP side according to TR-CS v2.0 [44] may support the `li-Activated [1] Notification` only.
		
		It should be noted that national parameters do not apply

Clause TS 101 671	Selection of ETSI options for Switzerland	Additional requirements
D.4 to D.9	**ASN.1 modules** By using FTP for transferring IRI data, the related ROSE operations do not need to be implemented.	
Annex E: Use of sub-address and calling party number to carry correlation information		
E.3.2	**Field order and layout** Parameter assignment for CC in accordance to tables E.3.2 and E.3.4 (and the E.3.4 based example in E.3.6) for the Called Party Subaddress and tables E.3.3 and E.3.8 (and the E.3.5 based example in E.3.7) for the Calling Party Subaddress, make provision to correlate CC with IRI according to [7] Annex A.1.2.	

11.3.1. Subaddress encoding according to ETSI TS 101 671

11.3.1.1. Conventions

[7] clauses E.3.1 and E.3.2 define the coding rules for the various parameters contained in Called and Calling Party Subaddress field. The following rules apply:

a) For numeric values the digit 1 shall be the Most Significant Digit (MSD) while digit n shall be the Least Significant Digit (LSD), see [7] clause E.3.1, last paragraph.

b) All the fields according to [7] Table E.3.2 (refers to Called Party Subaddress) and Table E.3.3 (refers to Calling Party Subaddress) shall be present and appear in the defined order, even if some fields are empty.

c) An empty field shall be indicated by two consecutive Field separators (“FF” hex), see [7] clause E.3.2, first paragraph underneath Table E.3.2 with the following clarification:
An “empty field” appears as “empty field consisting of one field separator” (single half-octet). In this case ONE field separator appear after the field separator of the preceding field, followed by the next field, that could take a value or be empty. For a single (isolated) empty field there are two field separators present in total, one is the field separator of the preceding field and the other is for the empty field; for two (consecutive) empty fields there are three field separators present in total, one is the field separator of the preceding field and the remaining are one for each empty field; for three (consecutive) empty fields there are four field separators present in total, etc...
The format depicted in the figures below illustrates this clarification.

d) The service octets 19 (TMR), 20 (BC octet 3), and 21 (HLC octet 4) shall be present even if a parameter is not available (Note). In the latter case a value “FF” hex shall be entered.

NOTE: The term “available” refers to the presence of a parameter in the signaling messages, i.e. denotes “when provided” by the function that is subject to interception.

11.3.1.2. Format of the Called Party Subaddress Information Element

[7] Table E.3.4 specifies the format of the Called Party Subaddress information element including the Lawful Interception specific parameters to be sent as part of the setup message to LEMF when a CC-link is being established. The format according to [7] Table E.3.4 shall be supported as detailed in the following.

Some of the parameters contained in the Called Party Subaddress are of variable length. Depending on their length they appear in different instances of the Called Party Subaddress while retaining the order.

For the LI specific parameters of the Called Party Subaddress [7] clause E.3 applies with the following clarification:

a) The odd/even indicator defines the number of half-octets up to and including the final Field separator which is either in an odd (final Field separator shall be mapped into bits “4321”) or an even (final Field separator shall be mapped into bits “8765”) position within the half-octet structure. It does not include the spare field, if any, at the end.
b) For parameters with a numeric value that spans more than one half-octet (these are Operator-ID and CIN) the Most Significant Digit (MSD) is the half-octet with the lowest number.
c) The value to be entered into a spare half-octet is undefined in [7]. It shall be set the value of “0000”. At the receiving side spare shall be ignored, i.e. the message containing the Called Party Subaddress shall not be rejected because a spare bit is set to “1”.

Figure 9 depicts the format of the Called Party Subaddress for a five digit CIN.

octet	Bit							
	8	7	6	5	4	3	2	1
1	Called party subaddress information element identifier							
	0	1	1	1	0	0	0	1
2	Length of calling party subaddress contents (9 octets in this case)							
	0	0	0	0	1	0	0	1
3	ext.	Type of subaddress			Odd/even	Spare		
	1	0	1	0	0 (even)	0	0	0
4	Operator-ID				Operator-ID (MSD) NOTE			
	0	0	0	0	1	0	0	1
5	Operator-ID				Operator-ID			
	0	0	0	0	0	0	0	0
6	Field separator				Operator-ID (LSD)			
	1	1	1	1	0	0	0	1
7	CIN				CIN (MSD)			
8	CIN				CIN			
9	Field separator				CIN (LSD)			
	1	1	1	1				
10	Field separator or Spare (IIF implementation option)				Field separator			
	1/0	1/0	1/0	1/0	1	1	1	1

NOTE: In this Called Party Subaddress the Operator-ID value is set as an example to „90001“.

Figure 9: Called Party Subaddress Information Element

The LEMF shall take the parameter “CIN” as the last parameter in the Called Party Subaddress when followed by at least two consecutive Field separators and no further fields other than Field separator or Spare, otherwise the Called Party Subaddress contains a “National parameter” to be treated by LEMF.

11.3.1.3. Format of the Calling Party Subaddress Information Element

[7] Table E.3.5 specifies the format of the Calling Party Subaddress information element including the Lawful Interception specific parameters to be sent as part of the setup message to LEMF when a CC-link is being established. The format according to [7] Table E.3.5 shall be supported as detailed in the following.
Some of the parameters contained in the Calling Party Subaddress are of variable length. Depending on their length they appear in different instances of the Calling Party Subaddress while retaining the order.
For the LI specific parameters of the Calling Party Subaddress [7] clause E.3 applies with the following clarification:

a) The odd/even indicator defines the number of half-octets up to an including the Field separator subsequent to the parameter “Direction” which is either in an odd (Field separator shall be mapped into bits “4321”) or an even (Field separator shall be mapped into bits “8765”) position within the half-octet structure. It does not include the spare field, if any, between the last Field separator and octet 19.
b) For parameters with a numeric value that spans more than one half-octet (this is LIID) the Most Significant Digit (MSD) is the half-octet with the lowest number.
c) The value to be entered into a spare half-octet is undefined in [7]. It shall be set to the value of “0000”. At the receiving side spare shall be ignored, i.e. the message containing the Calling Party Subaddress shall not be rejected because a spare bit is set to “1”.
d) Special rules apply to the Service Octets from 19 through 21 as described in section 11.3.1.4.
e) Depending on the presence of Mobile Bearer Service Code and Mobile Tele-service Code in signaling messages, information shall be provided in octets 22 and 23 as follows:
    1. If both, Mobile Bearer Service Code and Mobile Teleservice Code are provided by signaling, octets 22 AND 23 shall be present.
    2. If Mobile Bearer Service Code is provided by signaling, and Mo-bile Teleservice Code is NOT provided by signaling, octet 22 shall be present.
    3. If Mobile Teleservice Code is provided by signaling, and Mobile Bearer Service Code is NOT provided by signaling, neither octet 22 nor octet 23 shall be present.
    4. If neither Mobile Teleservice Code nor Mobile Bearer Service Code is provided by signaling, neither octet 22 nor octet 23 shall be present.

Figure 10 below depicts the format of the Calling Party Subaddress (example with the defined 15-digit LIID).

octet	bit							
	8	7	6	5	4	3	2	1
1	Calling party subaddress information element identifier							
	0	1	1	0	1	1	0	1
2	Length of calling party subaddress contents							
	0	0	0	1	0	0	1	1
3	ext.	Type of subaddress			Odd/even	Spare		
	1	0	1	0	1 (odd)	0	0	0
4	LIID <2>				LIID <1> (MSD)			
5	LIID <4>				LIID <3>			
6	LIID <6>				LIID <5>			
7	LIID <8>				LIID <7>			
8	LIID <10>				LIID <9>			
9	LIID <12>				LIID <11>			
10	LIID <14>				LIID <13>			
11	Field separator				LIID<15> (LSD)			
12	Field separator				Direction: CC from Target = 1, CC to Target = 2			
	1	1	1	1	1	1	0/1	0/1
13	Spare				Spare			
18	Spare				Spare			
19	Service Parameter “TMR” according to ITU-T Rec. [24] § 3.54							
20	Service Parameter “BC” octet 3 according to ITU-T Rec. [23] § 4.5.5							
	ext	Coding standard		Information transfer capability				
	1	0	0					
21	Service Parameter “HLC” octet 4 according to ITU-T Rec. [23] § 4.5.17							
	ext	High layer characteristics identification						
	0/1							
22	Mobile Bearer Service Code according to [22] § 14.7.10							
	Public Land Mobile Network specific Format							
	Format for other Bearer Service Codes							
	unused	group (see [22] § 14.7.10)				rate (see [22] § 14.7.10)		
	0							
23	Mobile Teleservice Code according to [22] § 14.7.9							
	group (see [22] § 14.7.9)				specific service (see [22] § 14.7.9)			

Figure 10: Calling Party Subaddress Information Element

The Bearer Service Code allows two formats, the choice being a CSP option:

a) the PLMN-specific bearer services, individually defined by each Home Public Land Mobile Network Operator, with codepoint for bits “4321” from 0 through F (Hex) with leading

bits “8765” equal to “1101”, see [22] ASN.1 encoding BearerServiceCode set from allPLMN-specificBS through plmn-specificBS-F.

b) the „rest“ of bearer services with the structure and codepoints defined in [22] ASN.1 encoding BearerServiceCode.

The Teleservice Code allows two formats, the choice being a CSP option:

a) the PLMN-specific teleservices, individually defined by each Home Public Land Mobile Network Operator, with codepoint for bits “4321” from 0 through F (Hex) with leading bits “8765” indicating the group PLMN “1101”, see [22] ASN.1 encoding TeleserviceCode set from allPLMN-specificTS through plmn-specificTS-F.

b) the „rest“ of bearer services with the codepoints for bits „87654321“ defined in [22] ASN.1 encoding TeleserviceCode.

11.3.1.4. Service octets for fix networks

For Fix networks the Calling Party Subaddress contains three parameters that allow identifying the profile of the Content of Communication of the intercepted call. These are:

- Octet 19: The parameter Transmission Medium Requirement (TMR), see [7] Table E.3.5.
- Octet 20: The parameter Bearer Capability (BC), see [7] Table E.3.5.
- Octet 21: The parameter High Layer Compatibility (HLC), see [7] Table E.3.5.

ITU-T Recommendation [25] specifies how, among others, analog signaling, the information elements of DSS1 SETUP, and parameters of ISUP IAM (Initial Address Message) are to be used in specific call scenarios.
The service information available in principle at the Switch where the IIF resides depends on the connection from the calling party (target or third party) to the IIF which could be either ISDN or non-ISDN:

a) For ISDN, [25] § 2.1.1.1, in particular Table 1 in [25] (for TMR), Table 3 in [25] (for User Service Information parameter, USI) and Table 6 in [25] (for User Teleservice Information parameter, UTI) applies.

b) For non-ISDN, including third calling ISDN with intermediate interworking, [25] § 2.2.1.1 applies. In relation to TMR, the value is 3.1 kHz audio. Neither the USI nor the UTI are present.

The following table describes the availability of service information within the switch where the IIF resides for various call scenarios in terms of ISUP parameters (TMR, USI, UTI), and defines the mapping of information contained in the ISUP parameters TMR, USI and UTI into the Calling Party Subaddress to be done by the IIF. It should be noted that the information on the service profile that is provided by the calling party, which could be the target or a third party, and is passed via signaling to the IIF is mainly relevant for the contents of octets 19, 20 and 21 in the Calling Party Subaddress.

In the case that an analog target terminates a call, there are implementation options as follows, the choice being a CSP option:

- Option a.: All parameters available in the switch where the IIF resides are mapped into the octets 19 (TMR), 20 (USI), and 21 (UTI) of the Calling Party Subaddress.
- Option b.: Only TMR is mapped into the octet 19 of the Calling Party Subaddress, while 20 (USI), and 21 (UTI) are set to “FF” (hex).

- Option c.: The octets 19 (TMR), 20 (USI), and 21 (UTI) of the Calling Party Subaddress are set to “FF” (hex).

The IIF shall meet the requirements specified in the following table.

		ISUP parameters according to [25]			Parameters according to [7] Table E.3.5		
Calling	**Called**	**ISUP Transmission Medium Requirement [24] § 3.54**	**ISUP User Service Information octet 1 [24] § 3.57 (coding see [23] § 4.5.5 octet 3)**	**ISUP User Teleservice Information octet 2 [24] § 3.59 (coding see [23] § 4.5.17 octet 4)**	**Service Parameter octet 19 (value "TMR")**	**Service Parameter octet 20 (value "BC" octet 3)**	**Service Parameter octet 21 (value "HLC" octet 4)**
Target ISDN	Third any	speech	speech	not present or telephony	speech or "FF" hex (Note 1)	speech	"FF" hex or telephony (Note 2)
		64 kbit/s unrestricted	unrestricted digital information	not present or value matching BC	UDI or "FF" hex (Note 1)	unrestricted digital information	"FF" hex or value matching BC (Note 2)
		3.1 kHz audio	3.1 kHz audio	not present or value matching BC	3.1 kHz audio or "FF" hex (Note 1)	3.1 kHz audio	"FF" hex or value matching BC (Note 2)
Target analog	Third any	3.1 kHz audio	not present	not present	3.1 kHz audio	"FF" hex	"FF" hex
Third ISDN	Target ISDN	speech	speech	not present or telephony	speech or "FF" hex (Note 1)	speech	"FF" hex or telephony (Note 2)
		64 kbit/s unrestricted	unrestricted digital information	not present or value matching BC	UDI or "FF" hex (Note 1)	unrestricted digital information	"FF" hex or value matching BC (Note 2)
		3.1 kHz audio	3.1 kHz audio	not present or value matching BC	3.1 kHz audio or "FF" hex (Note 1)	3.1 kHz audio	"FF" hex or value matching BC (Note 2)
Third ISDN	Target analog	speech	speech	not present or telephony	OPTION a.: speech or "FF" hex (Note 1)	OPTION a.: speech	OPTION a.: "FF" hex or telephony (Note 2)
					OPTION b.: speech	OPTION b.: "FF" hex	OPTION b.: "FF" hex
					OPTION c.: "FF" hex	OPTION c.: "FF" hex	OPTION c.: "FF" hex
		64 kbit/s unrestricted	unrestricted digital information	not present or value matching BC	No communication between third party and Target takes place with this service profile, since the user destination "analog" is incompatible to the service profile of the offered call. No CC-links are established using this profile, but IRI is sent.		
		3.1 kHz audio	3.1 kHz audio	not present or value matching BC	OPTION a.: 3.1 kHz audio or "FF" hex (Note 1)	OPTION a.: 3.1 kHz audio	OPTION a.: "FF" hex or value matching BC (Note 2)

		ISUP parameters according to [25]			Parameters according to [7] Table E.3.5		
Calling	**Called**	**ISUP Transmission Medium Requirement [24] § 3.54**	**ISUP User Service Information octet 1 [24] § 3.57 (coding see [23] § 4.5.5 octet 3)**	**ISUP User Teleservice Information octet 2 [24] § 3.59 (coding see [23] § 4.5.17 octet 4)**	**Service Parameter octet 19 (value "TMR")**	**Service Parameter octet 20 (value "BC" octet 3)**	**Service Parameter octet 21 (value "HLC" octet 4)**
					OPTION b.: 3.1 kHz audio	OPTION b.: "FF" hex	OPTION b.: "FF" hex
					OPTION c.: "FF" hex	OPTION c.: "FF" hex	OPTION c.: "FF" hex
Third analog or Interworking	Target ISDN	3.1 kHz audio	not present	not present	3.1 kHz audio	"FF" hex	"FF" hex
Third analog or Interworking	Target analog	3.1 kHz audio	not present	not present	OPTION a.: 3.1 kHz audio	OPTION a.: "FF" hex	OPTION a.: "FF" hex
					OPTION b.: 3.1 kHz audio	OPTION b.: "FF" hex	OPTION b.: "FF" hex
					OPTION c.: "FF" hex	OPTION c.: "FF" hex	OPTION c.: "FF" hex

Table Mapping of TMR, USI and UTI at IIF into Calling Party Subaddress service parameters

NOTE 1: Service Parameter octet 19 allows IIF an implementation option in situations where the information is contained in octet 20 thereby LEMF may ignore octet 19.
NOTE 2: Service Parameter octet 21 may deliver "FF" hex, if the optional HLC has not been provided by the calling user.

11.3.2. FTP delivery of IRI according to ETSI TS 101 671

11.3.2.1. File naming

The composition of the filename is based on the file naming method B according to [7] Annex C.2.2

<Filenamestring> of the format ABXYyymmddhhmmsseeeet
Where:
'AB' ASCII letters are assigned by PTSS to the CSP
'XY' ASCII letters can be chosen by the CSP

11.3.2.2. FTP parameters

When transferring data via FTP the systems of the CSP act as sender (i.e. FTP client), and those of PTSS as recipient (i.e. FTP server).

The values of these parameters (e.g. IP address, username and password for the FTP account) are defined during the compliance assessment procedure.

The following rules apply in general:

1. Multiple IRI data sets and, if available, copies of CC data, can be treated as a single file. In case of ASN.1 encoded data, for example, an 'IRI sequence' is used for this.
2. It is possible to transfer one or multiple files in the same communication session if these files are already available at the TCE-O (CSP side). When no further files are available, the communication session must be terminated immediately after file transfer.

The following table contains the definitions for the most important FTP parameters:

Value	**Content**	
Document type	binary	
Filename	length: characters:	21 characters allowed characters: upper case letters A-Z, digits 0-9
CSP username for LEMF FTP server	length: characters:	at least 8 characters lower and upper case letters a-z A-Z, digits 0-9
CSP password for LEMF FTP server	Length: characters:	at least 8 characters lower and upper case letters a-z A-Z, digits 0-9
Directory change	It is not allowed to change the directory in the FTP server.	
Port for data connection	20/TCP (default value)	
Port for control connection	21/TCP (default value)	
Mode	FTP passive mode must be supported.	

11.3.3. Additional information regarding ASN.1 definitions

PTSS informs the CSP about ETSI Specifications including their ASN.1 module. Section 16.5 contains further information about the version requirements for ETSI defined ASN.1 modules.

The ASN.1 descriptions of the different modules for implementation in accordance with this section must be taken from ETSI specifications TS 101 671.

All parameters in the ETSI specification designated as “conditional“ or “optional” must always be transmitted when available and not otherwise specified in section 11.3.

11.4. Selected and Required Options as well as Extended Technical Requirements according to ETSI specification TS 133 108 (UMTS) for 3GPP networks operating Release 6 and higher

Clause TS 133.108	Selection of ETSI options for Switzerland	Additional requirements
4.3	**Functional requirements** Options “IRI and CC” and “only IRI” option must be supported. Option “only CC” does not need to be implemented.	
4.4	**Manual/Electronic handover interface 1 (HI1)** An electronic handover interface from the LEMF to the obligated party’s technical infrastructure for direct administration of interception measures without the involvement of the obligated party is not implemented in Switzerland. Events regarding the management of an interception (e.g. activation and deactivation) and error communication must be delivered.	See section 8
4.5.1	**Data transmission protocol** FTP is used for IRI data. The FTP connection must be closed immediately after data transmission.	See section 11.4.2
Chapter 5: Circuit-switched domain		
5.1.2.1	**Network Identifier (NID)** The NID is composed of 5 digits: NWO/AP/SvP identifier (Operator identifier). PTSS provides the Operator identifier.	
5.2.2.1	**Control information for HI2** The timestamp must include official local time and related DST indication.	
5.3.1	**Delivery of Content of Communication** For relating CC data to other H-Interfaces the subaddress service will be used as specified in [19] Annex J.2 instead of the user-to-user signalling. For SMS and UUS Services, CC will be transferred as IRI. The provider must remove encryption	CC data must be A-law coded in compliance to ITU-T G.711 [40], i.e. in case of different coding in the original channel (e.g. GSM) the mediation function must ensure conversion to A-law coding.

Clause TS 133.108	Selection of ETSI options for Switzerland	Additional requirements
	algorithm applied by the CSP internally in the network at the handover interface.	
5.3.2	**Control information for circuit switched Content of Communication** The terminal end point of PTSS replies to a SETUP message immediately with a CONNECT message, i.e. without any ALERTING message.	
5.3.3	**Security requirements at the interface port HI3** ISDN Service specifications CLIP and COLP must be used for creating CC links to PTSS.	CUG does not need to be implemented.
5.3.3.3	**Authentication** A special authentication procedure within the ISDN B Channel or within the Subaddress is not used.	
5.4.4 5.5.2, 5.5.3, 5.5.11	**Multi party calls – general principles** Only option A is available and must be used.	
5.5.12.1.1	**Call Diversion by target, CC links** For CFNR, UDUB, CD and partial rerouting, option 2 (with CONTINUE-Record) must be implemented.	
5.5.3	**Call Hold/Retrieve** If an active call is put on hold, its CC link shall stay intact and the signal from the held party shall be switched through to the LEMF. If the target sets up a new call, while one call is on hold, this call shall be treated as a normal originating call (additional CC link). [19] clause 5.5.3.1 applies. CC links shall stay intact and the signal from the held party shall be switched through.	
5.5.4.1	**Explicit Call Transfer (ECT)** For explicit call transfer, Option 2 must be implemented. This means, that the transferred call must not be intercepted.	
5.5.15	**User-to-User Signalling (UUS)** UUS service data will be delivered as IRI data.	See points 5.3.1 in this Table.

Clause TS 133.108	Selection of ETSI options for Switzerland	Additional requirements
Annex A: HI2 delivery mechanisms and procedures		
A	**ROSE/FTP** FTP must be used for transferring IRI data over HI2-interface; ROSE is not allowed.	
A.2	**Usage of FTP for conveying IRI data**. File naming method B must be used according to section 11.3.2.1	
Annex J: Use of sub-address and calling party number to carry correlation information		
J.2.3	**Field order and layout** Parameter assignment for CC in accordance to tables J.2.3. and J.2.5 (and the J.2.5 based example in J.2.4A) for the Called Party Subaddress and tables J.2.4 and J.2.6 for the Calling Party Subaddress, make provision to correlate CC with IRI according to [19] Annex J.2.	

11.4.1. Subaddress encoding according to ETSI TS 133 108

11.4.1.1. Conventions

[19] clauses J.2.3.1, J.2.3.2 define the coding rules for the various parameters contained in Called and Calling Party Subaddress field. The following rules apply:

a) For numeric values the digit 1 shall be the Most Significant Digit (MSD) while digit n shall be the Least Significant Digit (LSD), see [19] clause J.2.3.1, last paragraph.

b) All the fields according to [19] Table J.2.3 (refers to Called Party Subaddress) and Table J.2.4 (refers to Calling Party Subaddress) shall be present and appear in the defined order, even if some fields are empty.

c) An empty field shall be indicated by two consecutive Field separators (“FF” hex), see [19] clause J.2.3.2, first paragraph underneath Table J.2.3 with the following clarification:
An “empty field” appears as “empty field consisting of one field separator” (single half-octet). In this case ONE field separator appear after the field separator of the preceding field, followed by the next field, that could take a value or be empty. For a single (isolated) empty field there are two field separators present in total, one is the field separator of the preceding field and the other is for the empty field; for two (consecutive) empty fields there are three field separators present in total, one is the field separator of the preceding field and the remaining are one for each empty field; for three (consecutive) empty fields there are four field separators present in total, etc...
The format depicted in the figures below illustrates this clarification.

d) The service octets 19 (TMR), 20 (BC octet 3), and 21 (HLC octet 4) shall be present even if a parameter is not available (Note). In the latter case a value “FF” hex shall be entered.

NOTE: The term “available” refers to the presence of a parameter in the signaling messages, i.e. denotes “when provided” by the function that is subject to interception.

11.4.1.2. Format of the Called Party Subaddress Information Element

[19] Table J.2.5 specifies the format of the Called Party Subaddress information element including the Lawful Interception specific parameters to be sent as part of the setup message to LEMF when a CC-link is being established. The format according to [19] Table J.2.5 shall be supported as detailed in the following.

Some of the parameters contained in the Called Party Subaddress are of variable length. Depending on their length they appear in different instances of the Called Party Subaddress while retaining the order.

For the LI specific parameters of the Called Party Subaddress [19] clause J.2.3 applies with the following clarification:

a) The odd/even indicator defines the number of half-octets up to and including the final Field separator which is either in an odd (final Field separator shall be mapped into bits “4321”) or an even (final Field separator shall be mapped into bits “8765”) position within the half-octet structure. It does not include the spare field, if any, at the end.
b) For parameters with a numeric value that spans more than one half-octet (these are Operator-ID and CIN) the Most Significant Digit (MSD) is the half-octet with the lowest number.
c) The value to be entered into a spare half-octet is undefined in [19]. It shall be set the value of “0000”. At the receiving side spare shall be ignored, i.e. the message containing the Called Party Subaddress shall not be rejected because a spare bit is set to “1”.

Figure 11 depicts the format of the Called Party Subaddress for a five digit CIN.

octet	bit							
	8	7	6	5	4	3	2	1
1	Called party subaddress information element identifier							
	0	1	1	1	0	0	0	1
2	Length of calling party subaddress contents (9 octets in this case)							
	0	0	0	0	1	0	0	1
3	ext.	Type of subaddress			Odd/even	Spare		
	1	0	1	0	0 (even)	0	0	0
4	Operator-ID				Operator-ID (MSD) NOTE			
	0	0	0	0	1	0	0	1
5	Operator-ID				Operator-ID			
	0	0	0	0	0	0	0	0
6	Field separator				Operator-ID (LSD)			
	1	1	1	1	0	0	0	1
7	CIN				CIN (MSD)			
8	CIN				CIN			
9	Field separator				CIN (LSD)			
	1	1	1	1				
10	Field separator or Spare (IIF implementation option)				Field separator			
	1/0	1/0	1/0	1/0	1	1	1	1

NOTE: In this Called Party Subaddress the Operator-ID value is set as an example to „90001“.

Figure 11: Called Party Subaddress Information Element

The LEMF shall take the parameter “CIN” as the last parameter in the Called Party Subaddress when followed by at least two consecutive Field separators and no further fields other than Field separator or Spare, otherwise the Called Party Subaddress contains a “National parameter” to be treated by LEMF.

11.4.1.3. Format of the Calling Party Subaddress Information Element

[19] Table J.2.6 specifies the format of the Calling Party Subaddress information element including the Lawful Interception specific parameters to be sent as part of the setup message to LEMF when a CC-link is being established. The format according to [19] Table J.2.6 shall be supported as detailed in the following.
Some of the parameters contained in the Calling Party Subaddress are of variable length. Depending on their length they appear in different instances of the Calling Party Subaddress while retaining the order.
For the LI specific parameters of the Calling Party Subaddress [19] clause J.2.3 applies with the following clarification:

a) The odd/even indicator defines the number of half-octets up to an including the Field separator subsequent to the parameter “Direction” which is either in an odd (Field separator shall be mapped into bits “4321”) or an even (Field separator shall be mapped into bits “8765”) position within the half-octet structure. It does not include the spare field, if any, between the last Field separator and octet 19.
b) For parameters with a numeric value that spans more than one half-octet (this is LIID) the Most Significant Digit (MSD) is the half-octet with the lowest number.
c) The value to be entered into a spare half-octet is undefined in [19]. It shall be set to the value of “0000”. At the receiving side spare shall be ignored, i.e. the message containing the Calling Party Subaddress shall not be rejected because a spare bit is set to “1”.
d) Depending on the presence of Mobile Bearer Service Code and Mobile Tele-service Code in signaling messages, information shall be provided in octets 22 and 23 as follows:
    - If both, Mobile Bearer Service Code and Mobile Teleservice Code are provided by signaling, octets 22 AND 23 shall be present.
    - If Mobile Bearer Service Code is provided by signaling, and Mobile Teleservice Code is NOT provided by signaling, octet 22 shall be present.
    - If Mobile Teleservice Code is provided by signaling, and Mobile Bearer Service Code is NOT provided by signaling, neither octet 22 nor octet 23 shall be present.
    - If neither Mobile Teleservice Code nor Mobile Bearer Service Code is provided by signaling, neither octet 22 nor octet 23 shall be present.

Figure 12 depicts the format of the Calling Party Subaddress (example with 15-digit LIID).

octet	bit							
	8	7	6	5	4	3	2	1
1	Calling party subaddress information element identifier							
	0	1	1	0	1	1	0	1
2	Length of calling party subaddress contents							
	0	0	0	1	0	0	1	1
3	ext.	Type of subaddress			Odd/even	Spare		
	1	0	1	0	1 (odd)	0	0	0
4	LIID <2>				LIID <1> (MSD)			
5	LIID <4>				LIID <3>			
6	LIID <6>				LIID <5>			
7	LIID <8>				LIID <7>			
8	LIID <10>				LIID <9>			
9	LIID <12>				LIID <11>			
10	LIID <14>				LIID <13>			
11	Field separator				LIID <15> (LSD			
12	Field separator				Direction: CC from Target = 1, CC to Target = 2			
	1	1	1	1	1	1	1/0	0/1
13	Spare				Spare			
18	Spare				Spare			
19	Service Parameter “TMR” according to ITU-T Rec. [24] § 3.54							
20	Service Parameter “BC” octet 3 according to ITU-T Rec. [23] § 4.5.5							
	ext	Coding standard		Information transfer capability				
	1	0	0					
21	Service Parameter “HLC” octet 4 according to ITU-T Rec. [23] § 4.5.17							
	ext	High layer characteristics identification						
	0/1							
22	Mobile Bearer Service Code according to [26] § 17.7.10							
	Public Land Mobile Network specific Format							
	Format for other Bearer Service Codes							
	unused	group (see [26] § 17.7.10)				rate (see [26] § 17.7.10)		
	0							
23	Mobile Teleservice Code according to [26] § 17.7.9							
	group (see [26] § 17.7.9)				specific service (see [26] § 17.7.9)			

Figure 12: Calling Party Subaddress Information Element

The Bearer Service Code allows two formats, the choice being a CSP option:

a) the PLMN-specific bearer services, individually defined by each Home Public Land Mobile Network Operator, with codepoint for bits “4321” from 0 through F (Hex) with leading bits “8765” equal to “1101”, see [26] ASN.1 encoding BearerServiceCode set from allPLMN-specificBS through plmn-specificBS-F.

b) the „rest“ of bearer services with the structure and codepoints defined in [26] ASN.1 encoding BearerServiceCode.

The Teleservice Code allows two formats, the choice being a CSP option:

a) the PLMN-specific teleservices, individually defined by each Home Public Land Mobile Network Operator, with codepoint for bits “4321” from 0 through F (Hex) with leading bits “8765” indicating the group PLMN “1101”, see [26] ASN.1 encoding TeleserviceCode set from allPLMN-specificTS through plmn-specificTS-F.
b) the „rest“ of bearer services with the codepoints for bits „87654321“ defined in [26] ASN.1 encoding TeleserviceCode.

11.4.2. FTP delivery of IRI according to ETSI TS 133 108

11.4.2.1. File naming

The composition of the filename is based on the file naming method B according to [19] Annex A.2

<Filenamestring> in the format ABXYyymmddhhmmsseeeet
Where:
‘AB’ ASCII letters are assigned by PTSS to the CSP
‘XY’ ASCII letters can be chosen by the CSP

11.4.2.2. FTP Parameters

When transferring data via FTP the systems of the CSP act as sender (i.e. FTP client), and those of PTSS as recipient (i.e. FTP server).

The values of these parameters (e.g. IP address, username and password for the FTP account) are defined during the compliance assessment procedure.
The following rules apply in general:

1. Multiple IRI data sets and, if available, copies of CC data, can be treated as a single file. In case of ASN.1 encoded data, for example, an ‘IRI sequence’ is used for this.
2. It is possible to transfer one or multiple files in the same communication session if these files are already available at the TCE-O (CSP side). When no further files are available, the communication session must be terminated immediately after file transfer.

The following table contains the definitions for the most important FTP parameters:

Value	**Content**	
Document type	binary	
Filename	length: characters:	21 characters allowed characters: upper case letters A-Z, digits 0-9
CSP username for LEMF FTP server	length: characters:	at least 8 characters lower and upper case letters a-z A-Z, digits 0-9

CSP password for LEMF FTP server	Length: at least 8 characters characters: lower and upper case letters a-z A-Z, digits 0-9
Directory change	It is not allowed to change the directory in the FTP server.
Port for data connection	20/TCP (default value)
Port for control connection	21/TCP (default value)
Mode	FTP passive mode must be supported.

11.4.3. Additional Information regarding ASN.1 definitions

PTSS informs the CSP about ETSI Specifications including their ASN.1 module. Section 16.5 contains further information about the version requirements for ETSI defined ASN.1 modules.

The ASN.1 descriptions of the different modules for implementation in accordance with this section must be taken from ETSI specification TS 133 108.

All parameters in the ETSI specification designated as “conditional“ or “optional” must always be transmitted when available and not otherwise specified in section 11.4

11.5. Requirements for the Location Function on Mobile Networks

All information related to the geographical location must be coded in a way that can be directly interpreted by PTSS. In particular, this includes the geographical coordinates of the antennas (e.g. Base Transceiver Station for GSM or Node B for UMTS) as well as their postal addresses, Cell Global Identification (CGI; see ETS 300 523) and the main beam direction. The geographical coordinates must be indicated in accordance with Swissgrid CH1903. The Cell Global Identification (cell ID) values provided to PTSS must be the same as the ones actually used on the Mobile radio interface.
The CSP must deliver the most accurate location concerning the intercepted mobile network connection.

11.6. Provisioning of Cell-ID Correlation Tables

Following contents must be included in the Cell-ID correlation table:

1. Name of operator
2. Date of table delivery
3. Cell-IDs
4. Swissgrid CH1903 coordinates of the antenna locations corresponding to each Cell-ID
5. Direction of the main beam of the antenna corresponding to each Cell-ID: The beam direction angle refers to the mapped 2-dimensional horizontal middle compass angle (in degrees 0-360) of the corresponding cell sector. In case of an umbrella sector, the value –1 must be inserted in this field.
6. Full postal address (if available)

The first row of the table is reserved as follows:

1. Name of operator (1st column)
2. Date of table delivery (2nd column) as follows: ddmmyyyy

Each subsequent row contains a Cell-ID with the corresponding coordinates and beam direction as follows:

1. Cell-ID (1st column)
2. x-Coordinate (2nd column)
3. y-Coordinate (3rd column)
4. Direction of main beam of antenna (4th column)
5. Postal address

The contents of the table must be saved in CSV (Comma Separated Values) format according to [35]. This format separates columns of data by commas and rows by carriage return.

The filename of the table must have the following format (the prefix CM means “Cell-ID Map”): CM_operatorXY_yyyymmdd.csv
where
<operatorXY> Name of the operator providing the table
<yyyymmdd> Date of table delivery
The following example shows the contents of a Cell-ID correlation table in CSV format, mapping two Cell-IDs:

OperatorXY,20101201,,,
228-0X-56F0-B64B,200000,600000,26,Bern Bundesgasse 8
228-0X-57F3-C76A,354678,657891,45,Autobahn A1 KM 555
…

12. Packet-switched Domain Real-Time Interception

This section describes the requirements for the delivery of data for real-time interception of services provided on packet-switched based network. There are four main services:

Service	Specification	Section
Mobile data: Packet-switched networks based on GSM and UMTS, as well as interworking with WLAN [Informative]	TS 101 671 [7] TS 133 108 [19]	12.1
Email: CSP providing email services	TS 102 232-1 [9] TS 102 232-2 [10] Swiss national proprietary mechanism	12.2
Internet access: Fix network layer 2 and layer 3 internet access technologies. [Informative]	TS 102 232-1 [9] TS 102 232-3 [11] TS 102 232-4 [12]	12.3
VoIP and Multimedia: VoIP/multimedia services and emulated PSTN/ISDN services according to ETSI Standard ES 282 002 [37]	TS 102 232-1 [9] TS 102 232-5 [13] TS 102 232-6 [14]	12.4

12.1. Mobile Data Delivery for GPRS and UMTS Networks

This section describes the requirements for the handover interface for mobile data networks such as GPRS and UMTS networks according to ETSI specifications TS 101 671 [7] and TS 133 108 [19]. These specifications provide the technical description for the delivery of mobile packet-switched networks.

Section 7 describes the identifiers that are required for lawful interception. Whenever the target identifier is an IMEI, the intercepted data must be identified by both IMEI and corresponding MSISDN parameters.
The general requirements for this section are described in the following sections:

Section	Content
9.2.1	Dimensioning for mobile data services interceptions
16.5	Applicable ETSI Standards and Specifications as well as ASN.1 Modules
13.3	Packet-switched services interceptions

12.1.1. Specific lawful interception identifiers for mobile packet-switched domain

12.1.1.1. Correlation number

The Correlation Number as specific LI identifier for packet switched networks is defined in [7] Annex B.1 for GPRS, respectively in [19] clauses 6.1.3, 8.1.4 and 9.1.4. for UMTS.

The Correlation Number is unique per PDP context and is used for the following purposes:
• correlate CC with IRI;
• correlate different IRI records within one PDP context.

12.1.2. Selected and required options as well as extended technical requirements for GPRS according to ETSI specification TS 101 671

Clause TS 101 671	Selection of ETSI options for Switzerland	Additional requirements
5.1	**Manual/Electronic handover interface 1 (HI1)** An electronic handover interface from the LEMF to the obligated party's technical infrastructure for direct administration of interception measures without the involvement of the obligated party is not implemented in Switzerland. Events regarding the management of an interception (e.g. activation and deactivation) and error communication must be delivered.	See section 8
6.2.1	**Network identifier (NID)** The NID is composed of 5 digits: NWO/AP/SvP identifier (Operator identifier). PTSS provides the Operator identifier.	
8.1	**Data transmission protocol** FTP is used for IRI data, HI1 notifications and packetized CC such as SMS and UUS. ROSE is not allowed. The FTP connection must be closed immediately after data transmission.	See section 11.3.2
10.1	**Timing** Buffering of IRI for the purpose of recovery is required, for instance if the transmission of IRI fails. See also [7] Annex C.2.5	Buffering of IRI data up to 24 hours.
Annex B: GPRS technology annex		
B.5.3	**HI2 (delivery of IRI)**	Because of a lack of a mapping description of GPRS event information (parameter) to the event record (e.g. GPRS attach), the description of the 3GPP specification [19] clause 6.5.1 applies. Events and available parameters are described in [7] Annex B.5.3. The assignment of parameters to events is specified in tables 6.3 – 6.9 of [19]. The interpretation and meaning of these events is assumed to be identical for

Clause TS 101 671	Selection of ETSI options for Switzerland	Additional requirements
		both specifications.
Annex C: HI2 Delivery mechanisms and procedures		
C.1 / C.2	**ROSE / FTP** FTP must be used for transferring IRI data over HI2-Interface; ROSE is not allowed.	See point 8.1in this Table.
C.2.2	**Usage of FTP for conveying IRI data** Transmission must be triggered neither by timeout nor by volume. File naming method B must be used. Additionally, section 11.3.2 of TR TS [43] applies as well.	
Annex D: Structure of data at the Handover Interface		
D.4 to D.9	**ASN.1 modules** By using FTP for transferring IRI data, the related ROSE operations do not need to be implemented.	
Annex F: GPRS HI3 Interface		
F.3	**HI3 Delivery Content of Communication (CC)** GLIC header with TCP/IP as described in Annex F.3.1. is used. The provider must remove encryption algorithm applied by the CSP and used internally in the network at the handover interface.	Using UDP for transferring the header is not allowed (for both GLIC and ULIC).
F.3.1.3	**Exceptional procedures** TCP must be used to deliver HI3-GPRS information.	
F.3.2.2	**Usage of FTP** FTP for conveying CC data is not supported.	

12.1.2.1. Additional Information regarding ASN.1 definitions

PTSS informs the CSP about ETSI and 3GPP-Standards and Specifications including its ASN.1 module. Section 16.5 contains further information about the version requirements for ETSI defined ASN.1 modules.

The explanations of ASN.1 in this section are based on the ETSI specification TS 101 671.

All parameters in the ETSI specification designated as “conditional“ or “optional” must always be transmitted when available and not otherwise specified in section 12.1.2

12.1.3. Selected and required options as well as extended technical requirements for UMTS data according to ETSI specification TS 133 108

Clause TS 133.108	Selection of ETSI options for Switzerland	Additional requirements
4.4	**Manual/Electronic Handover Interface 1 (HI1)** An electronic handover interface from the LEMF to the obligated party's technical infrastructure for direct administration of interception measures without the involvement of the obligated party is not implemented in Switzerland. Events regarding the management of an interception (e.g. activation and deactivation) and error communication must be delivered.	See section 8
4.5	**HI2: Interface port for intercept related information** Buffering of IRI for the purpose of recovery is required, for instance if the transmission of IRI fails.	Buffering of IRI data up to 24 hours
4.5.1	**Data transmission protocol** FTP is used for IRI The FTP connection must be closed immediately after data transmission.	See section 11.4.2
6.5.1.1	**REPORT record information** Record shall be triggered: - when the SGSN receives the SMS-MO from the target MS. - when the SGSN receives the SMS-MT from the SMS-Centre	
7	**Multi-media domain** The provision of the lawful interception of services supported by the IP Multimedia Core Network Subsystem (IMS) shall be carried out in conformity with the provisions of the technical specification corresponding to RELEASE 7 or higher, according to the releases in which the telecommunications services in question are found at each time.	
7.1	**Identifiers** Interception is performed on an IMS identifier(s) associated with the intercept subject including identifier types such as SIP-URI and Tel-URI	

Clause TS 133.108	Selection of ETSI options for Switzerland	Additional requirements
7.1.2	**Network identifier** Providing the Network Element IDentifier (NEID) parameter is mandatory.	
8	**3GPP WLAN interworking** The provision of the lawful interception of services supported by the IP Multimedia Core Network Subsystem (IMS) shall be carried out in conformity with the provisions of the technical specification corresponding to RELEASE 7 or higher, according to the releases in which the telecommunications services in question are found at each time.	
8.1.3	**Network identifier** Providing the Network Element IDentifier (NEID) parameter is mandatory.	
Annex A: HI2 delivery mechanisms and procedures		
A	**ROSE/FTP** FTP must be used for transferring IRI data over HI2-interface; ROSE is not allowed.	
A.2.2	**Usage of FTP for conveying IRI data** File naming method B must be used according to section 11.4.2 of TR TS [43].	
Annex C: UMTS HI3 interface		
C	**UMTS HI3 interface** ULIC header version 0 with TCP/IP as described in Annex C.1.2, or the the ULIC header version 1 with TCP/IP described in Annex C.1.3. is used. The provider must remove internally used encryption algorithm at the handover interface.	ULIC version 1 is preferred.
C.1.1	**Introduction** When using TCP/IP as transfer method, the used destination port will be provided by PTSS.	Using UDP for transferring the ULIC header is not allowed.
C.1.3	**Definition of ULIC header version 1** When using ULIC header version 1, the parameters LIID and timeStamp are mandatory.	

Clause TS 133.108	Selection of ETSI options for Switzer-land	Additional requirements
C.2	**FTP** Usage of FTP for conveying CC data is not supported.	

12.1.3.1. Additional Information regarding ASN.1 definitions

PTSS informs the CSP about ETSI and 3GPP-Standards and Specifications including its ASN.1 module. Section 16.5 contains further information about the version requirements for ETSI defined ASN.1 modules. The explanations of ASN.1 in this section are based on the ETSI specification TS 133 108.

All parameters in the ETSI specification designated as “conditional“ or “optional” must always be transmitted when available and not otherwise specified in section 12.1.3.

12.2. Interception of Email Services

This section covers general technical requirements that need to be fulfilled by the CSP when providing Email services interception data.

One of the two different technical options specified below can be implemented in agreement with PTSS:

1) Delivery of email services interception data according to the ETSI specification TS 102 232-2 [10] as specified in section 12.2.1
2) Delivery of email services interception data according to the Swiss national proprietary delivery mechanism and procedure as specified in 12.2.2

Note: PTSS recommends adopting option 1 as option 2 will be discontinued.

12.2.1. Delivery of email services data according to ETSI TS 102 232-2

This section describes the handover interface for email services as specified in [10].

12.2.1.1. Definitions and general requirements

Section	Content
9.2.2	Dimensioning for email services interceptions
16.5	Applicable ETSI Standards and Specifications as well as ASN.1 Modules
13.1	Historical Data and email interceptions

Email server	All kinds of service that stores or relays email messages, independently of the access possibilities of the user, e.g. SMTP, POP3, IMAP, Web or WAP.
Email address	Address according to RFC 5322
Mailbox	The part of an email system that is assigned to a specific user (here: the target of an interception measure). Here, both send and received messages are stored. A mailbox can be used for several email addresses.
Login	Procedure for authorizing a user to access a specific mailbox.

If a full copy of a given message has already been transferred to PTSS, only IRI data needs to be sent in case of further events according to [10] clause 6; e.g. in case of later download of the message. In such cases, a unique identifier must be provided in the designated data field so that PTSS can correlate the relevant events.

12.2.1.2. Selected and required options as well as extended technical requirements according to ETSI TS 102 232-1

The following table describes the selected options related to ETSI specification TS 102 232-1.

Clause TS 102 232-1	Selection of ETSI options for Swiss applications	Additional requirements or specifications
5.2.1	**Version** Because an OID is used in the ASN.1 description, a separate parameter is not necessary.	
5.2.2	**LIID** A unique value is assigned by PTSS via the HI1 interface using the mechanism specified in 8	
5.2.3	**Authorisation country code** 'CH' must be used in Switzerland.	
5.2.4	**Communication identifier** In Switzerland, "CH" must be used as the delivery country code (DCC). The operator identifier (part of NID) is assigned by PTSS.	PTSS provides the OperatorID composed of 5 digits
5.2.5	**Sequence number** The sequence number must already be set where the copy of the intercepted telecommunication was first generated (point of interception).	In some cases this requirement cannot be met. In such cases, the sequence number must be set before or at the delivery function. In any case, the sequence number must reproduce the precise counting method at the place of origin.
5.2.7	**Payload direction** Must be indicated for CC data.	The value is either fromTarget(0), toTarget(1) or unknown.
6.2.2	**Error reporting** .OperatorLeaMessage specified in [9] Annex A.2 must be used.	Related NID must be mentioned in the Transport Related Information (TRI) message.
6.2.3	**Aggregation of payloads** Aggregation of payload shall not be used.	
6.2.5	**Padding data** Padding of data shall not be used.	
6.3.1	**General** TCP/IP must be used.	
6.3.2	**Opening and closing of connections** The described handling of unsuccessful connection establishment must be implemented.	
6.3.4	**Keep-alives** Can optionally be implemented by the CSP.	The use of this option must be agreed with PTSS.

Clause TS 102 232-1	Selection of ETSI options for Swiss applications	Additional requirements or specifications
6.4.2	**TCP settings** The destination TCP port number at PTSS (LEMF) will be provided via HI1.	The port number applies in connection with the use of the service specifications TS 102 232-2, TS 102 232-3, TS 102 232-4, TS 102 232-5 and TS 102 232-6.
7.2	**Security requirements** .	Neither TLS, nor signatures, nor hash codes must be used.
7.3.2	**Timeliness**	The possible use of separate managed networks must be agreed with PTSS.

12.2.1.3. Selected and required options as well as extended technical requirements according to ETSI TS 102 232-2

Note: The ETSI technical specifications TS 102 232-2 [10] specified in this section use the same options of TS 102 232-1 [9] as TS 102 232-5 [13] and TS 102 232-6 [14]

Clause TS 102 232-2	Available options for Swiss applications	Additional requirements or specifications
6.2.3	**Email send IR**I IRI data according to table 1 for the event “Email send” must always be transferred.	
6.3.3	**Email receive IRI** IRI data according to table 2 for the event “Email receive” must always be transferred.	
6.4.3	**Email download IRI** IRI data according to table 3 for the event ”Email download” must always be transferred.	

12.2.1.4. Explanations regarding the ASN.1 descriptions

PTSS informs the CSP about ETSI Specifications including their ASN.1 module. Section 16.5 contains further information about the version requirements for ETSI defined ASN.1 modules.

The ASN.1 descriptions of the different modules for implementation in accordance with this section must be taken from ETSI specifications TS 102 232-1 and TS 102 232-2.

All parameters in the ETSI specification designated as “conditional“ or “optional” must always be transmitted when available and not otherwise specified in sections 12.2.1.2 and 12.2.1.3

12.2.2. Delivery of email services and internet access data according to Swiss proprietary mechanism and procedure

This section specifies a national solution for the delivery of the results of email services real-time interception and historical data for email services and internet access.

An implementation which meets the requirements herein is backward compatible to an implementation according to “Technical Requirements for the Delivery of Intercepted Electronic Mail, Version 2.0”, [46]

12.2.2.1. Definitions

Container email	Signed and encrypted delivery message transmitted by the CSP to the LEMF
Delivery message	MIME-conform message containing results of interception in clear.

12.2.2.2. Delivery mechanism for the results of interception

Any result of interception must be packed into a MIME-conform [29, 30] *delivery message*, which must subsequently be signed and encrypted. The resulting *container email* must be delivered to the LEMF through the Internet according to [31]. For each surveillance case a specific mailbox is maintained at the LEMF. The following sections define the generic format of the delivery message and the container email, respectively.

12.2.2.2.1. Header fields of the container email

The contents of the header fields *From*, *To*, and *Subject* according to [30] must be composed following the syntax listed below.

From: *“LI_monitor@” CSP-domain* (denotes the sender’s address)
To: *LIID “@” LEMF-domain* (denotes the recipient’s address)
Subject: *interception-type “_” major-version “.” minor-version*

The variables are defined as follows:

CSP-domain = Domain name of the CSP.

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

LEMF-domain = Domain name of the receiving LEMF.

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

Interception type code	Representation
"00"	Is reserved for administrative emails
"01"	Real-time delivery of an email incoming to the target identifier mailbox (according to chapter 12.2.2.4)
"02"	Real-time delivery of an email sent by the target identifier (according to chapter 12.2.2.4)
"03"	Delivery of a list containing actual SMTP envelope information of emails incoming to the target identifier mailbox (see chapter 12.2.2.5.2)
"04"	Delivery of a list containing actual mailbox access information of the target identifier (see chapter 12.2.2.5.4)
"05"	Delivery of a list containing SMTP actual envelope information of emails sent by the target identifier (see chapter 12.2.2.5.3)
"06"	Delivery of a list containing historical internet access information of the target identifier (see chapter 12.2.2.5.5)
"07"	Delivery of a list containing historical SMTP envelope information of emails sent and received by the target identifier (see chapter 12.2.2.5.2 and 12.2.2.5.3)

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

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

minor-version = Single digit representing the minor version of the format the results of interception are presented in the container email. Find following a table with the current minor version for each *interception type*.

Interception type code	Current minor version
"00"	*"0"*
"01"	*"0"*
"02"	*"0"*
"03"	*"0"*
"04"	*"0"*
"05"	*"0"*
"06"	*"1"*
"07"	*"0"*

12.2.2.2.2. Security mechanisms

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

For authentication, integrity and confidentiality reasons, the contents of any delivery message must be signed and encrypted using OpenPGP [32].

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

The key pair type is Diffie-Hellman/DSS and its size is 2048/1024 bits. The key pairs expire after 3 years. In cases where an interception period exceeds 3 years, new key pairs must be generated, replacing the old key pairs. The PTSS contacts the CSP at least one month before the expiration of the keys in order to agree and define a bilateral key renewal process.

The CSP must perform for each container email to be delivered to the LEMF the following signing and encrypting procedure:

1) The MIME entity of the delivery message is created according to the rules described in chapter 12.2.2.4.1 and 12.2.2.5.1.
2) The whole MIME entity, including its body and set of content headers and the boundaries, is signed using the SHA-1 hash algorithm and subsequently encrypted applying the Triple-DES algorithm.
3) The output of the encryption procedure is encoded into ASCII Armor.
4) New MIME content headers are generated:
   Content-Type: text/plain
   Content-Transfer-Encoding: 7bit
5) The resulting container email is delivered to the LEMF according to section 12.2.2.2

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

12.2.2.2.3. Delivery failure

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

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

12.2.2.3. Date and time specifications

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

12.2.2.3.1. Timestamp syntax

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

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

The components of a timestamp are defined as follows:

year = Four-digit representation of the actual year

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

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

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

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

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

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

12.2.2.3.2. Synchronization

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

The following server is defined as the reference time base:

NTP (stratum 2) time server: ntp.metas.ch

It is proposed to use the Network Time Protocol (NTP) [34] for synchronization, but any other system (e.g. DCF77, GPS, etc.) may also be used as long as the offset from the reference time base remains within the range of +/- 5 seconds.

12.2.2.4. Interception of email contents

The interception of email contents is related to a specific email address serving as target identifier. Any email either received or sent by the target identifier mailbox must be intercepted, copied and forwarded to the LEMF in real-time. Consider that all three addressing possibilities, *"TO", "CC", "BCC"*, are of equal importance and have to be intercepted. This implies that for any email exchange in which the target is involved, all three email receivers concerned (*"TO", "CC", "BCC"*) have to be delivered.

This section defines the data structure and the delivery specifications for intercepting email both for "incoming" and "outgoing" emails according to the article 24a, letters c and d of [2].

12.2.2.4.1. Data structure

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

12.2.2.4.2. Delivery specifications

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

12.2.2.5. Interception of telecommunication parameters

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

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

Events are commonly recorded by the CSP in log-files, from which particular data related to the given target identifier must be filtered out, formatted according to the rules described in section 12.2.2.5.1, and sent as container email to the LEMF.

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

This section defines the data structure and the delivery specifications for intercepting communications parameters both for real-time and historical data according to the article 24a letters b, c and d and art. 24b letters a and b of [2].

12.2.2.5.1. Data structure

The results of interception must be presented in a well-formed, valid XML document. The XML document type to be used is determined by the event type. The respective document type definitions are given in the section 16.4. A XML document containing the results of interception may consist of none, one or several events of the same type. If data of an event is missing, the respective empty XML element must be provided.

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

The characters *"<"* and *"&"* must be substituted by their character entities, i.e. *"<"* and *"&"*, respectively.

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

The XML documents containing the results of interception must be included inline in a delivery message as *text/plain* MIME-content type with character set *UTF-8* [33].

12.2.2.5.2. Data structure for incoming email

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

timestamp =	timestamp denoting the date and time the email has been delivered to the mailbox. The format of the timestamp is according to its definition in section 12.2.2.3.1
mail-from =	The email address of the sender is displayed as *mailbox* defined in [31]: *local-part "@" domain* .
rcpt-to =	The email address of the recipient is displayed as *mailbox* defined in [31]: *local-part "@" domain* .
original-log =	Original event log of the SMTP envelope information. The data must be plain text, UTF-8 encoded.
ip-address =	The IP-address of the sending unit is given in IPv4 or IPv6 format.

For each recipient of the email, a *rcpt-to* element is created. The document type definition and example are listed in section 16.4.1

12.2.2.5.3. Data structure for relayed email

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

For a single event the following XML elements are defined:

timestamp = timestamp denoting date and time of receiving the email at the mail server (for event type *"mail-server_in"*) or of transferring the email to the MTA (for event type *"mail-server_out"*). The format of the timestamp is according to its definition in section 12.2.2.3.1.

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

mail-from, rcpt-to, and *original-log* are used with the same format and meaning as described in chapter 12.2.2.5.2. For each recipient of the email, an element *rcpt-to* is created. The document type definition and example are is listed in section 16.4.2

12.2.2.5.4. Data structure for mailbox access

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

timestamp = timestamp denoting date and time the mailbox has been accessed. The format of the timestamp is according to its definition in section 12.2.2.3.1.

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

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

The document type definitions and example are listed in section 16.4.3.

12.2.2.5.5. Data structure for Internet access

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

start-time = timestamp denoting the date and time a modem session is initiated (login at the CSP) or an IP-address is allocated. The

format of the timestamp is according to its definition in section 12.2.2.3.1.

stop-time = timestamp denoting the date and time a modem session is closed or an IP-address is released. The format of the timestamp is according to its definition in section 12.2.2.3.1.

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

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

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

The format of the *calling number* is either national or international. Local calling numbers must not be used. For the international format there are two alternatives: The country code is either preceded by *"00"* or by "+"[7].

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

users-lastname = Last name of the user associated with the above mentioned login-name.

users-firstname = First name of the user associated with the above mentioned login-name.

users-address = Address (street and number) of the user associated with the above mentioned login-name.

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

users-zip =	ZIP= code of the user associated with the above mentioned login-name.
users-city =	City of the user associated with the above mentioned login-name.
users-profession =	Profession of the user associated with the above mentioned login-name.

All user-related variables have to be added, if they exist in the CSP customer database.

The document type definitions are listed in section 16.4.4

The provided Internet access information must cover the whole specified period of time. When an Internet service attach or detach timestamp is not within the period of time specified in the inquiry the respective timestamp element need not to be provided. The Internet access event itself, however, has to be reported in any case. Typically, the bureaus of investigations are interested in identifying the subscriber that has been using a specific IP-address at a given point in time or a short time period. Therefore, in case that no service attach/detach timestamps fall into this time period, but a dynamic IP-address was indeed allocated before and released after the specified period of time, the event "*event_internet-access*" must nevertheless be reported, only the start-time and stop-time indication may be omitted as the respective timestamps are not within the specified period of time.

12.2.2.6. Delivery period

12.2.2.6.1. Actual data fetched in real-time

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

12.2.2.6.2. Historical data

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

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

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

12.3. Requirements for Internet Access according to ETSI Specifications TS 102 232-3 and TS 102 232-4

This section describes the handover interface for telecommunication technologies that are used for direct subscriber-related access to the Internet (e.g. xDSL, CATV, WLAN, but excluding dial-up access according to [11] clause 5.1.1) in accordance with ETSI specifications TS 102 232-3 and TS 102 232-4. These ETSI specifications use the general IP handover interface as described in the ETSI specification TS 102 232-1 and specified in the section 12.2.1.2.

In addition to the requirements of the present section, the following sections also apply:

Section	Content
9.2.3	Dimensioning for internet broadband services interceptions
16.5	Applicable ETSI Standards and Specifications as well as ASN.1 Modules
13.3	Packet-switched services interceptions

12.3.1. Selected and required options as well as additional technical requirements according to ETSI TS 102 232-3

The following table describes the available options related to ETSI specification TS 102 232-3 for internet access services.

Clause TS 102 232-3	Selection of ETSI options for Swiss applications	Additional requirements or specifications
4.3.1	**Target identity** See section 7	When a cable modem identifier is used for intercepting internet cable access, the modem change or move must be considered.
5.1.1	**Dial Up Access** This type of Internet access is not covered by this section.	
6.1	**IRI events** The events and HI2 attributes from [11] version 1.4.1 and onwards shall be used.	In version 1.4.1 the event ‘startOfInterceptionWithSessionActive’ was added.

12.3.2. Selected and required options as well as additional technical requirements according to ETSI TS 102 232-4

The following table describes the available options related to ETSI specification TS 102 232-4 for Layer 2 services.

Clause TS 102 232-4	Selection of ETSI options for Swiss applications	Additional requirements or specifications
4.2.1	**Target Identity** See section 7	For example, the change or move of a modem must be considered when a cable modem identifier is used for intercepting Internet cable access.
6.1	**IRI events** The events and HI2 attributes of [11] version 1.3.1 and onwards shall be used.	Version 1.3.1 abolished the event 'endOfInterceptionSessionActive'.

12.3.3. Explanations regarding the ASN.1 descriptions

PTSS informs the CSP about ETSI Specifications including their ASN.1 module. Section 16.5 contains further information about the version requirements for ETSI defined ASN.1 modules.

The ASN.1 descriptions of the different modules for implementation in accordance with this section must be taken from ETSI specifications TS 102 232-1, TS 102 232-3 and TS 102 232-4.

All parameters in the ETSI specification designated as “conditional“ or “optional” must always be transmitted when available and not otherwise specified in sections 12.3.1 and 12.3.2.

12.4. Requirements for Voice over IP and Other Multimedia Services according to ETSI Specifications TS 102 232-5 and TS 102 232-6

This section describes the handover interface for IP multimedia services according to ETSI specifications TS 102 232-5 and for emulated PSTN/ISDN services according to TS 102 232-6. These ETSI specifications use the general IP-based handover interface as described in the TS 102 232-1 specification and specified in this document in section 12.2.1.2.

In addition to the requirements of the present section, the following sections also apply:

Section	Content
9.2.4	Dimensioning for VoIP and other multimedia services
16.5	Applicable ETSI Standards and Specifications as well as ASN.1 Modules
13.3	Packet-switched services interceptions

12.4.1. General Requirements

ETSI specification TS 102 232-5 describes a handover interface for Voice over IP (VoIP) and other multimedia services that are based on the Session Initiation Protocol (SIP), the ITU-T Recommendations H.323 [42] and H.248 [41], the Real-time Transport Protocol (RTP) and the Real-time Transport Control Protocol (RTCP).

ETSI specification TS 102 232-6 allows the use of an IP-based handover interface for emulated PSTN and ISDN services. Here, a copy of the telecommunication data will be transferred as RTP stream via the general IP-based handover interface according to ETSI specification TS 102 232-1. Additionally, IRI data encoded within the module 'HI2Operations' according to section 11 will be transferred as well; the FTP transfer method according to section 11 shall not be implemented.

12.4.1.1. Terminology

Multimedia server (VoIP server) and involved network elements	Telecommunication installations that are involved in the provision of VoIP or other multimedia services that are based on SIP, H.323 or H.248 in combination with the media stream (e.g. RTP).
VoIP identifier	The VoIP identifier is an identifier for the communication to be intercepted. It is used in this context as representative for the various types of possible identifiers.
VoIP account	A user account created for the joint organisation of multiple VoIP identifiers. A VoIP account subject to interception may comprise multiple VoIP identifiers.
Login	The event at which the authorization of a user with regard to the access to a VoIP account is checked. The login name used as part of the user identification is also an identifier for the intercepted communication.

Note: If H.248 is in used according to [13] Annex A by a CSP it shall be addressed bilaterally between PTSS and CSP

12.4.1.2. Preliminaries

The technical attribute in a communication interception order can be specified as

1. a VoIP identifier
2. the user identification (login name without password) of the VoIP account

In order to allow for an interception of the complete telecommunication that is performed with a given VoIP identifier, it must be guaranteed by suitable authentication methods that the intercepted communication can be correctly assigned to the target. For example, this protects against cases where the communication cannot be effectively intercepted because of source address manipulation by the user.

If this requirement cannot be met for an interception order relating to a VoIP identifier (e.g. because of improper authentication methods), the fallback is an interception order for the complete VoIP account, i.e. the interception of communication of any VoIP identifier of the corresponding account.

12.4.1.3. Completeness of IRI Data

In order to prevent redundant capture of signal information, i.e. capturing more information without yielding additional details with regard to IRI (e.g. identifiers, used services), the num-

ber of used interception points should be reduced to the required minimum. For example, this should help to prevent multiple captures of INVITE messages of different hops within the network in which only the hop information is updated. However, dedicated filter logic for pre-processing of data collected at the interception points is not required.

12.4.1.4. Completeness of CC Data

Complete interception of CC data is required, particularly when CC data is transmitted separately – and sometimes even across different networks – from IRI data.

If routing changes must be performed in order to capture CC data, it is important that such changes are not visible to subscribers.

12.4.2. Selected and required options as well as additional technical requirements according to ETSI TS 102 232-5

The following table describes the available options related to ETSI specification TS 102 232-5 [13].

Clause TS 102 232-5	Selection of ETSI options for Swiss applications	Additional requirements or specifications
4.3	**General Requirements** 3) Generally, copies of signal information (e.g. SIP messages) are transferred as IRI data.	The documentation of the VoIP provider must explain the parameters and/or message combinations used for the various services (e.g. basic call, call forwarding) at the use of examples. Services that are controlled by end devices (clients) of subscribers must be described – if known – with regard to changes to signalling or RTP streams (e.g. simultaneous RTP streams in the case of conferences).
	5) IRI data that is not part of the signal must be transferred as well.	Module 'HI2Operations' described in [7] Annex D.5 must be used for handing over IRI data. A separate parameter may be used for SIP messages. The module itself should be transmitted in accordance with the requirements of [9] Annex A.2
	6) No national option is mandated.	

Clause TS 102 232-5	Selection of ETSI options for Swiss applications	Additional requirements or specifications
5.3	**Assigning a value to the CIN** Generally, for new sessions, the CIN is assigned at the first IRI or CC information. If a session already exists at the time of activation of an interception measure, the CIN must be generated at the first IRI or CC message.	If a connection already exists at the time of activation of an interception measure, a copy of IRI and CC data must be captured and provided starting from the point in time when the first IRI event is detected.
5.3.1	**Assigning a CIN value to SIP related IRI** The description assumes the use of the Call ID and the „o" field of the SDP for generating a single CIN for the entire call.	Despite of the known ETSI issue with multiple CIN, the generation of a single CIN for the various individual communication sessions is still an objective.
5.5	**Interception of Content of Communication** At the point of handover the VoIP provider must remove any service coding and/or encryption that have been applied to the data on his part. This includes any proprietary encodings.	This requirement also applies if the provider supports peer-to-peer communication by providing the key while the encryption itself is performed outside the provider's network.

12.4.3. Selected and required options as well as additional technical requirements according to ETSI TS 102 232-6

The following table describes the available options related to ETSI specification TS 102 232-6 [14].

Clause TS 102 232-6	Selection of ETSI options for Swiss applications	Additional requirements or specifications
5.2	**Structures** IRI is encoded with module HI2Operations according to [7] Annex D.5 and transferred directly by [9] Annex A.2 via the parameter ETSI671IRI.	

Clause TS 102 232-6	Selection of ETSI options for Swiss applications	Additional requirements or specifications
6.2	**CC format** The copy of content of communication (CC) is transferred as RTP packets with UDP and IP headers by [9] via the parameter PstnIsdnCC through [14]. The information required for interpreting the RTP packets are also transferred by [9] via the parameter PstnIsdnIRI through [14]. At the point of handover the VoIP provider must remove any service coding and/or encryption that have been applied to the data on his part.	This requirement also applies if the provider supports peer-to-peer communication by providing the key while the encryption itself is performed outside the provider's network.
6.2, 6.3.2	**Supplementary information** G.711 A-law must be used by default (mediaAttributes = "8"). The field copyofSDPMessage must always include a copy of the full SDP message (mandatory).	By transferring the full SDP message, PTSS receives a full copy of the communication.

12.4.4. Additional Information about ASN.1 definitions

PTSS informs the CSP about ETSI Specifications including their ASN.1 module. Section 16.5 contains further information about the version requirements for ETSI defined ASN.1 modules.

The ASN.1 descriptions of the different modules for implementation in accordance with this section must be taken from ETSI specifications TS 102 232-1, TS 102 232-5 and TS 102 232-6.

All parameters in the ETSI specification designated as “conditional“ or “optional” must always be transmitted when available and not otherwise specified in section 12.4.2 and 12.4.3

13. Error Handling when Transmitting Interception and Historical Data to the LEMF

Identified problems which impair the telecommunication interception or transmission must be sent and immediately reported to PTSS according [3] section 10.1

13.1. Historical Data and email interceptions

If it appears to be temporarily impossible to deliver a copy of the historical data or email interceptions to the LEMF (e.g. as a result of a network overload or of a malfunction in the CSP equipment or PTSS LEMF), all historical data or email must be temporarily buffered and completely transmitted afterwards.

The connection attempts for sending the copy of the intercepted telecommunication must be automatically reinitiated, unless otherwise agreed with PTSS for the specific incident.

13.2. Circuit-switched services interceptions

13.2.1. IRI data for circuit-switched services

If it appears to be temporarily impossible to deliver to the LEMF a copy of the IRI data related to circuit-switched services, IRI data shall be temporarily buffered and new transmission attempts must be initiated every 30 minutes for a period of 24 hours.

IRI data shall temporarily be stored for a maximum period of 24 hours.

If the failure to deliver lasts longer CSP and PTSS must agree on an alternative medium of transport of the IRI data related to the circuit-switched services.

13.2.2. CC data for circuit-switched services

If a problem occurs when transmitting the copy of the content of communication (CC) intercepted telecommunication, further connection attempts must be done automatically according to [7] Annex A.4.4.1.

Content of communication (CC) shall not be stored.

13.3. Packet-switched services interceptions

13.3.1. IRI data for packet-switched services

IRI data shall not be stored. However, in order to accommodate proper delivery to the LEMF the CSP mediation function/delivery function shall support the minimum buffering requirements specified in [9] Clause 6.3.3.

13.3.2. CC data for packet-switched services

Content of communication (CC) shall not be stored. However, in order to accommodate proper delivery to the LEMF the CSP mediation function/delivery function shall support the minimum buffering requirements specified in [9] Clause 6.3.3.

14. Security

14.1. Communication across HI1

For communication aspects, following security mechanisms apply, as described in [3] section 8:

1. Personal communication over telephone, fax or email is carried out only by pre-defined personnel.
2. When communicating via email, OpenPGP must be used.

14.2. Data Protection

To ensure confidentiality of data the federal requirements of “Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (SR 235.1)” [6] apply for both PTSS and the CSP.

14.3. Hardware Security

The CSP and PTSS must provide for prevention of unauthorized access to the functionality of all the systems involved in lawful interception.

14.4. Personnel Security Aspects

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

15. Final Provisions

The technical requirements mentioned in the following table are repealed:

Document	Version	Date
Technical Requirements for the Delivery of the results of interception Circuit Switched Services TR-CS	Version 2.0	January 1st, 2008
Technical Requirements for the Delivery of Historical Data Circuit Switched Services TR-CS-HD	Version 2.0	January 1st, 2008
Technical Requirements for the Delivery of Intercepted Electronic Mail Packet Switched Services TR-PS-EMAIL	Version 2.0	January 1st, 2008
Technical Guideline for the implementation of lawful measures for monitoring telecommunications Swiss Designation: TR TS (Technical Requirements for Telecommunication Surveillance)	Version 1.0	August 1st, 2009

The utilization of the handover interfaces specified in the sections enumerated in the table below requires the operation of the new LEMF “ISS”. PTSS will notify the CSP accordingly:

Section #	Title
11.4	Selected and Required Options as well as Extended Technical Requirements according to ETSI specification TS 133 108 (UMTS) for 3GPP networks operating Release 6 and higher
12.1	Mobile Data Delivery for GPRS and UMTS Networks
12.2.1	Delivery of email services data according to ETSI TS 102 232-2
12.3	Requirements for Internet Access according to ETSI Specifications TS 102 232-3 and TS 102 232-4
12.4	Requirements for Voice over IP and Other Multimedia Services according to ETSI Specifications TS 102 232-5 and TS 102 232-6

According to article 15 of [1] and articles 18 and 26 of [2], a CSP has to be able to perform the interception types which are defined in [2] and must deliver the results of interception to the LEMF of PTSS in compliance with this Guidelines document.

This document comes into force January 1, 2012.

3003 Berne, November 23, 2011

Post and Telecommunications Surveillance Service PTSS

sig

René Koch

Head of PTSS

16. Appendices

16.1. National Format for XML DTD for Orders

```
<!-- 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) #RE-
QUIRED>
<!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) #REQUIRED>
<!ELEMENT modification (interception-type+)>
```

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, are be included in the order. None of these two elements 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 “PTSS”.
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.

Elements definition:

comment optional comment
target-identity based on the target type:

Target type	**Identifier meaning and format**
fixnet-call-number	Fixnet number in international format
msisdn	MSISDN in international format
imei	IMEI (15 digits)
imsi	IMSI (15 digits)
voice mail identifier	Voice mail identifier, e.g. E.164 number
email address	Email address
ip-address	IP address in either IPv4 or IPv6 format
login-name	Login-name for the service accessed
mac-address	MAC-address of the accessing unit. The MAC-address is presented as a hexadecimal 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 elements date-of-order, date-of-execution, from and to are defined as follows:
year month day [SP] hours ":" minutes ":" seconds

where
year Four-digit representation of the year
month Two-digit representation of the month
day Two-digit representation of the day of the month
hours Two-digit representation of the hours
minutes Two-digit representation of the minutes
seconds Two-digit representation of the seconds

16.1.1. 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>
```

16.1.2. 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>
```

16.1.3. Example for a deactivation order

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE order SYSTEM "order.dtd">

<order order-type="deactivation" prior-
ity="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>
```

16.2. National Format for XML DTD for Requests

The meanings of the XML elements correspond to the definition in section 8. The same formats of the elements as described in section 16 hold.

```
<!-- 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>
```

16.2.1. 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>
```

16.3. National Format for XML DTD for Historical Data of circuit-switched services

```
<!-- CS_4.dtd -->

<!ELEMENT hist-data (communication-session*)>
<!ELEMENT communication-session (address-information, mobile-parameter-
information?, mobile-location-information*, duration-information)>
<!ATTLIST communication-session csi (toc|ttc|tfc|tou|ttu|tos|tts) #RE-
QUIRED>

<!ELEMENT address-information (calling-number, called-number, forwarded-to-
number*)>
<!ELEMENT calling-number (#PCDATA)>
<!ELEMENT called-number (#PCDATA)>
<!ELEMENT forwarded-to-number (#PCDATA)>

<!ELEMENT mobile-parameter-information (imei)>
<!ELEMENT imei (#PCDATA)>

<!ELEMENT mobile-location-information (antenna-coordinates, main-beam, an-
tenna-address, cell-id)>
<!ATTLIST mobile-location-information phase (begin|end) #REQUIRED>
<!ELEMENT antenna-coordinates (x-coordinate, y-coordinate)>
<!ELEMENT x-coordinate (#PCDATA)>
<!ELEMENT y-coordinate (#PCDATA)>
<!ELEMENT main-beam (#PCDATA)>
<!ELEMENT antenna-address (#PCDATA)>
<!ELEMENT cell-id (#PCDATA)>

<!ELEMENT duration-information (start-date-time, duration)>
<!ELEMENT start-date-time (#PCDATA)>

<!ELEMENT duration (#PCDATA)>
```

16.3.1. XML examples

The following informative example contains results of interception as follows:

- The intercepted target identity (mobile) is the MSISDN 075 111 22 33.
- There are three communication sessions reported.
- The communication sessions are:

    - A telephone call originated by the target. The called party number is a fixnet number 01 333 22 11.
    - A forwarded call. The target (075 111 22 33) is being called by the fixnet number 01 333 22 11 and forwards this call to the mobile number 074 222 33 11.
    - An SMS terminated at the target. The number of the SMS sender is 074 222 33 11.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE hist-data SYSTEM "test.dtd">
<hist-data>
      <communication-session csi="toc">
            <address-information>
                  <calling-number>0751112233</calling-number>
                  <called-number>013332211</called-number>
            </address-information>
            <mobile-parameter-information>
                  <imei>123456789012345</imei>
            </mobile-parameter-information>
            <mobile-location-information phase="begin">
                  <antenna-coordinates>
                        <x-coordinate>001001</x-coordinate>
                        <y-coordinate>002002</y-coordinate>
                  </antenna-coordinates>
                  <main-beam>010</main-beam>
                  <antenna-address>musterstrasse 54; 8001 zuerich</antenna-
address>
                  <cell-id>22F89123456789</cell-id>
            </mobile-location-information>
            <mobile-location-information phase="end">
                  <antenna-coordinates>
                        <x-coordinate>500500</x-coordinate>
                        <y-coordinate>600600</y-coordinate>
                  </antenna-coordinates>
                  <main-beam>320</main-beam>
                  <antenna-address>beispielstrasse 123; 8002 zue-
rich</antenna-address>
                  <cell-id>22F89123123123</cell-id>
            </mobile-location-information>
            <duration-information>
                  <start-date-time>20031027 12:00:00 CH</start-date-time>
                  <duration>205</duration>
            </duration-information>
      </communication-session>
      <communication-session csi="tfc">
            <address-information>
                  <calling-number>013332211</calling-number>
                  <called-number>0751112233</called-number>
                  <forwarded-to-number>0742223311</forwarded-to-number>
            </address-information>
            <mobile-parameter-information>
                  <imei>123456789012345</imei>
            </mobile-parameter-information>
            <mobile-location-information phase="begin">
                  <antenna-coordinates>
                        <x-coordinate>001001</x-coordinate>
                        <y-coordinate>002002</y-coordinate>
                  </antenna-coordinates>
                  <main-beam>010</main-beam>
                  <antenna-address>musterstrasse 54; 8001 zuerich</antenna-
address>
                  <cell-id>22F89123456789</cell-id>
```

```
            </mobile-location-information>
            <mobile-location-information phase="end">
                  <antenna-coordinates>
                        <x-coordinate>001001</x-coordinate>
                        <y-coordinate>002002</y-coordinate>
                  </antenna-coordinates>
                  <main-beam>010</main-beam>
                  <antenna-address>musterstrasse 54; 8001 zuerich</antenna-
address>
                  <cell-id>22F89123456789</cell-id>
            </mobile-location-information>
            <duration-information>
                  <start-date-time>20031028 21:03:54 CH</start-date-time>
                  <duration>100</duration>
            </duration-information>
      </communication-session>
      <communication-session csi="tts">
            <address-information>
                  <calling-number>0742223311</calling-number>
                  <called-number>0751112233</called-number>
            </address-information>
            <mobile-parameter-information>
                  <imei>123456789012345</imei>
            </mobile-parameter-information>
            <mobile-location-information phase="begin">
                  <antenna-coordinates>
                        <x-coordinate>111222</x-coordinate>
                        <y-coordinate>222111</y-coordinate>
                  </antenna-coordinates>
                  <main-beam>010</main-beam>
                  <antenna-address>unterbeispieltal</antenna-address>
                  <cell-id>22F89987654321</cell-id>
            </mobile-location-information>
            <mobile-location-information phase="end">
                  <antenna-coordinates>
                        <x-coordinate>222333</x-coordinate>
                        <y-coordinate>333222</y-coordinate>
                  </antenna-coordinates>
                  <main-beam>010</main-beam>
                  <antenna-address>oberbeispieltal</antenna-address>
                  <cell-id>22F89987987987</cell-id>
            </mobile-location-information>
            <duration-information>
                  <start-date-time>20031029 08:32:06 CH</start-date-time>
                  <duration></duration>
            </duration-information>
      </communication-session>
</hist-data>
```

16.4. National Format for XML DTD for Email services

16.4.1. Incoming email

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

Example: (the original event log is not included)

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

16.4.2. Relayed email

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

Example: (the original event log is not included)

```
<?xml version="1.0"?>
<!DOCTYPE relayed-email SYSTEM "relayed_email.dtd">
<relayed-email>
      <event_relayed-email subtype="mail-server_in">
```

```
            <timestamp>20011217 16:25:37 +0100</timestamp>
            <mail-from>xy@example.com</mail-from>
            <rcpt-to>muster@example.net</rcpt-to>
            <rcpt-to>sample@example.org</rcpt-to>
            <original-log>
                  ……
            </original-log>
            <ip-address>192.0.2.110</ip-address>
      </event_relayed-email>
      <event_relayed-email subtype="mail-server_out">
            <timestamp>20011217 16:34:14 +0100</timestamp>
            <mail-from>xy@example.com</mail-from>
            <rcpt-to>muster@example.net</rcpt-to>
            <original-log>
            ……
            </original-log>
            <ip-address>192.0.2.24</ip-address>
      </event_relayed-email>
      <event_relayed-email subtype="mail-server_out">
            <timestamp>20011217 16:38:37 +0100</timestamp>
            <mail-from>xy@example.com</mail-from>
            <rcpt-to>sample@example.org </rcpt-to>
            <original-log>
            ……
            </original-log>
            <ip-address>192.0.2.178</ip-address>
      </event_relayed-email>
</relayed-email>
```

16.4.3. Mailbox access

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

Example:

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

16.4.4. Internet access

```
<!-- internet-access.dtd -->
<!ELEMENT internet-access (event_internet-access*)>
<!ELEMENT event_internet-access (start-time?, stop-time?, ip-address, ac-
cess, login-name, users-lastname?, users-firstname?, users-address?, users-
zip?, users-city?, users-profession?)>
<!ELEMENT start-time (#PCDATA)>
<!ELEMENT stop-time (#PCDATA)>
<!ELEMENT ip-address (#PCDATA)>
<!ELEMENT access (#PCDATA)>
<!ATTLIST access type (PSTN|Cable|xDSL|LAN|Mobile_PS) #REQUIRED>
<!ELEMENT login-name (#PCDATA)>
<!ELEMENT users-lastname (#PCDATA)>
<!ELEMENT users-firstname (#PCDATA)>
<!ELEMENT users-address (#PCDATA)>
<!ELEMENT users-zip (#PCDATA)>
<!ELEMENT users-city (#PCDATA)>
<!ELEMENT users-profession (#PCDATA)>
```

Example:

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

16.5. Applicable ETSI Standards and Specifications as well as ASN.1 Modules

Please note that the table below is showing the applicable version of each related specification.

Any superior version can be adopted from the CSP for better performances. This must be agreed by PTSS for guaranteeing the compatibility with the actual PTSS LEMF systems, and will require a new compliance assessment.
Any existing syntax errors in the ASN.1 modules should be corrected. Use the correct object identifier (OID) and the correct version number.

Applicable ASN.1 Module	OID versions ETSI TR 102 503	Requirement or instruction for application
ETSI TS 101 671 [7] Circuit-switched services (section 11.3)		
HI1NotificationOperations	{0.4.0.2.2.0.1.2} to {0.4.0.2.2.0.1.6}	For the purpose of compatibility with existing implementations version 2 is supported.
HI2Operations,	{0.4.0.2.2.1.2} to {0.4.0.2.2.1.15}	For the purpose of compatibility with existing implementations version 2 is supported.
ETSI TS 101 671 [7] GPRS Packet-switched services (section 12.1.2)		
HI1NotificationOperations	{0.4.0.2.2.0.1.5} to {0.4.0.2.2.0.1.6	
HI2Operations	{0.4.0.2.2.1.10} to {0.4.0.2.2.1.15}	For transmission of HI2
Gprs-HI3-PS from version 3	{0.4.0.2.2.2.3.3}	For transmission of HI3 PS
ETSI TS 133.108 [19] UMTS Circuit-switched (section 11.4)		
UmtsCS-HI2Operations	{0.4.0.2.2.4.3.7.1}	Only valid for 3G networks operating Release 6 and above
UMTS-HI3CircuitLIOperation	{0.4.0.2.2.4.4.7.0}	Only valid for 3G networks operating Release 6 and above
ETSI TS 133.108 [19] UMTS Packet-switched (section 12.1.3)		
UmtsHI2Operations,	{0.4.0.2.2.4.1.7.3} to {0.4.0.2.2.4.1.10.3}	For transmission of HI2
Umts-HI3-PS, up to version 1	{0.4.0.2.2.4.2.7.0}	For transmission of HI3 PS
IWLANUmtsHI2Operations	{0.4.0.2.2.4.6.8.1}	For transmission of HI2 I-WLAN interworking
ETSI TS 102 232-1 [9] (section 12.2.1)		
LI-PS-PDU	{0.4.0.2.2.5.1.2} to {0.4.0.2.2.5.1.9}	Generic header ETSI TS 102 232-1 v1.2.1 ETSI TS 102 232-1 v2.4.1

ETSI TS 102 232-2 [10] (section 12.2.1)		
Email PDU, version 4	{0.4.0.2.2.5.2.3} to {0.4.0.2.2.5.2.4}	Email services ETSI TS 102 232-2 v2.2.1 ETSI TS 102 232-2 v2.4.1
ETSI TS 102 232-3 [11] (section 12.3.1)		
IPAccess PDU	{0.4.0.2.2.5.3.1} to {0.4.0.2.2.5.3.6}	Internet access services ETSI TS 102 232-3 v1.2.1 ETSI TS 102 232-3 v2.2.1
ETSI TS 102 232-4 [12] (section 12.3.2)		
L2AccessPDU	{0.4.0.2.2.5.4.4}	Layer 2 services ETSI TS 102 232-4 v2.2.1
ETSI TS 102 232-5 [13] (section 12.4.2)		
IPMultimediaPDU	{0.4.0.2.2.5.5.1} to {0.4.0.2.2.5.5.3}	IP multimedia services ETSI TS 102 232-5 v2.1.1 ETSI TS 102 232-5 v2.3.2
ETSI TS 102 232-6 [14] (section 12.4.3)		
PstnIsdnPDU	{0.4.0.2.2.5.6.2} to {0.4.0.2.2.5.6.3}	PSTN/ISDN services ETSI TS 102 232-6 v2.2.1 ETSI TS 102 232-6 v2.3.1

16.6. Delivery network specifications

16.6.1. Circuit-switched ISDN delivery network [Informative]

The ISDN delivery network provides access to the HI3 interface of the LEMF for the delivery of content of communication (CC) related to the circuit-switched telephony services can be performed through the public switched network via the universal service provider by means of the DSS1 protocol [21] through ISDN primary rate access or basic rate access. Note that the content of communication of interception of VoIP services can also be delivered like circuit-switched telephony services.

The usual interconnection agreements apply. There are no specific LI-related requirements for the ISDN-based network for the circuit-switched domain.

The LEMF E.164 address is communicated by PTSS to the CSP in a confidential document.

16.6.1.1. Attachment requirements for the ISDN delivery network

CSP have to meet attachment requirements according to the interconnection technical specifications provided by the universal service licensee [4] designated by the Federal Office of Communications.

16.6.2. Packet-switched IP-based delivery network

PTSS operates and maintains several infrastructures that allow CSP to deliver interception results in a packet-switched IP-based form:

i)	PTSS-WAN data network general description		16.6.2.1
		PTSS-WAN for large CSP	16.6.2.2
		PTSS-WAN for small CSP	16.6.2.3
ii)	OpenVPN		16.6.2.4
iii)	Direct connection to ISC-FDJP		16.6.2.5

16.6.2.1. PTSS-WAN data network general description

PTSS operates a legacy data network called PTSS-WAN that is IP-based. Its main purpose is to transmit the IRI data by means of the FTP protocol.
There are two different implementations, one for large CSP and one for small CSP, whereby the categorisation into large and small CSP is made by the PTSS according to the number of simultaneous interceptions carried out by the CSP.

The detailed specifications and requirements are as follows.

16.6.2.2. PTSS-WAN for large CSP

For large CSP, dedicated network links to the LEMF are used. These are referred to hereafter as “PTSS-WAN”. It is an IP based network with VPN connections, which lies in the responsibility of the PTSS.

16.6.2.2.1. *PTSS-WAN infrastructure*

All large CSP as well as the PTSS get network access via CPE (Customer Premises Equipment) router belonging to the provider of the VPN.

For the connection of the internal network of the CSP to the CPE-router an Ethernet interface is provided in the CPE-router, as follows:

- 10Base-T/100Base-TX interface
- Full-duplex transmission
- RJ-45 connector

16.6.2.2.2. *PTSS-WAN addressing*

The following addressing guidelines apply to the PTSS-WAN:

1. The CSP are responsible for the IP-addressing within their own network, including the IP-address of their FTP-client, up to the CSP-router connecting to the CPE-router (see also Figure 4).
2. The IP-addresses of the TSP-router-interface connected to the CPE-router and of the CPE-router itself are assigned by the VPN provider. The VPN provider assigns an IP-subnet for this purpose (the remaining IP-addresses within this subnet may be used internally by the CSP).
3. The FTP-client must be equipped with a public IP-address. The CSP might also use NAT (Network Address Translation) within his own network.
4. Static routing is applied in the PTSS-WAN.

16.6.2.2.3. *PTSS-WAN security*

The following security guidelines apply to the PTSS-WAN:

1. *Encryption*: For secure transmission of IRI data, IPSec VPN is applied in the PTSS-WAN, as in Figure 3. A gateway-to-gateway tunnel is being established between the CPE-router and the PTSS. The protocols IKE (UDP port 500) and ESP (IP protocol 50) of the IPSec protocol suite are being used.
2. *Authentication*: Authentication within the VPN is carried out by the VPN provider. There is no manual interaction required for VPN authentication purposes.
3. *Redundancy* (CSP option): As a redundancy option (backup), each large CSP is assigned an ISDN dial-up account by the VPN provider (in analogy to the solution for small CSP, see below). This dial-up account may be optionally used by the CSP in case of failure of the PTSS-WAN.
4. *Internal CSP-network*: The CSP are responsible for secure transmission of the IRI data within their own network (i.e. up to the CPE-router), see also Figure 3.

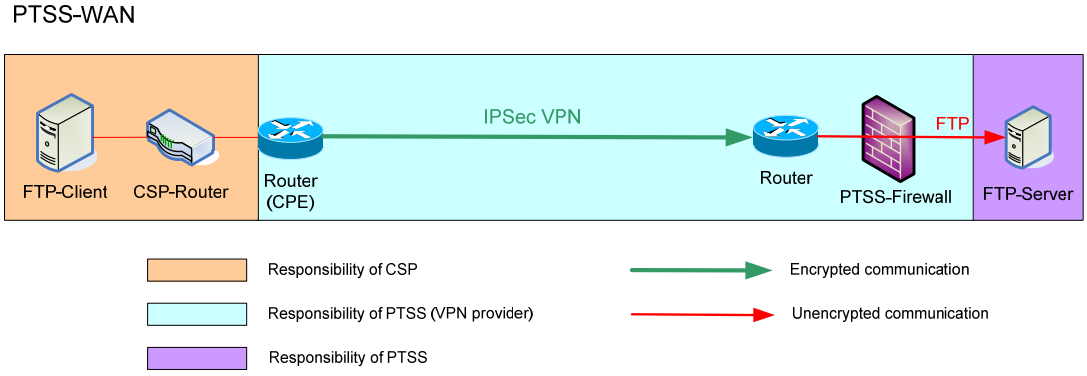

Figure 13: PTSS-WAN responsibilities

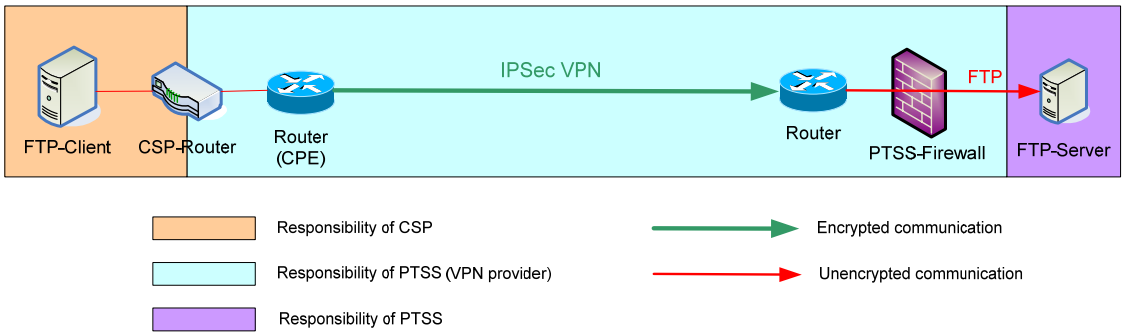

Figure 14: PTSS-WAN IP Addressing

16.6.2.2.4. *PTSS-WAN service and support*

The PTSS-WAN is built up and run under the responsibility of PTSS. PTSS chooses the provider of the VPN. There is only one provider at a time.

The CPE-router belongs to and is supported by the VPN provider. For installation and service purposes, the VPN provider has to be granted access to the CSP premises where the CPE-router resides.

16.6.2.3. PTSS-WAN for small CSP

For small providers, an ISDN dial-up alternative solution is available. No dedicated network links are installed.

The CSP dial into the dial-up RAS (toll-free number) of the VPN provider, where an account is defined for each CSP. Authentication is carried out through exchange of username and password. Subsequent to authentication an IPSec VPN link from the CSP to the firewall of the LEMF is established.

For the VPN a dedicated VPN client product[8] is supplied to the CSP by the VPN provider. In case a CSP has no ability to use this product, it is in his responsibility to acquire an alternative VPN solution which is compatible with the PTSS firewall[9] at the LEMF side.

Figure 16 provides an overview of the dial-up solution.

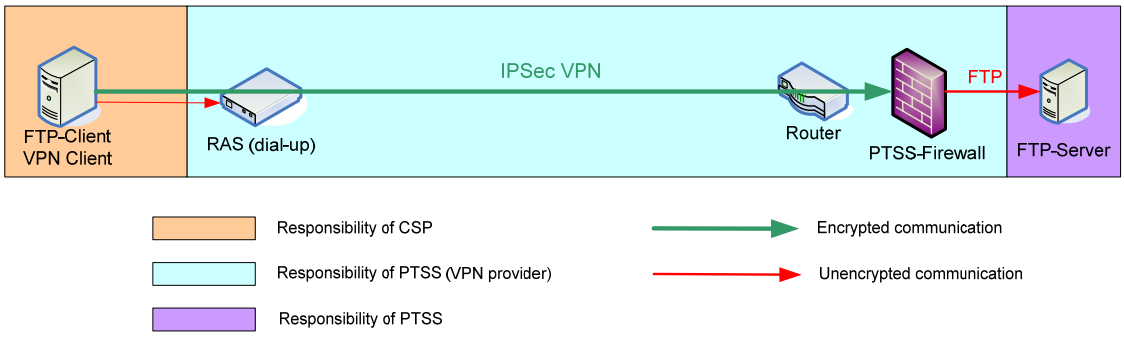

Figure 16: PTSS-WAN Dial-up solution

[8] At this stage “SecureClient” from CheckPoint. This product is compatible with Windows platforms only

[9] CheckPoint firewall

16.6.2.4. OpenVPN [Informative]

The FOITT (AS33845) is the provider of the IP Delivery Network. The CSP can use Internet upstream, private or public peering with the FOITT. In order to reduce the risk of interruptions, the connections of the CSP with the Delivery Network provider shall provide failover redundancy. The CSP manages the connections with the FOITT and arranges for the required service level through Service Level Agreements (SLA) with its peering partner (FOITT or IX) or upstream provider.

Data transmission across public networks has to be secured through encryption. OpenVPN has been chosen as the basic principle. The CSP are not obliged to choose a particular product or vendor as OpenVPN is available as an Open Source software solution.

The PTSS operates the VPN servers. PTSS is responsible for the connection between the Delivery Network provider (FOITT) and the LEMF. The VPN keys and certificates are managed and assigned by the PTSS as certification authority (CA).

The CSP sets up one or more individual OpenVPN tunnels with the ISC-FDJP. The CSP acquires and operates its VPN clients under its own responsibility.

The technical details regarding the supported protocol options if required and addressing schemes are provided by PTSS to the CSP on a bilateral basis.

16.6.2.4.1. *VPN Tunnel CSP - LEMF*

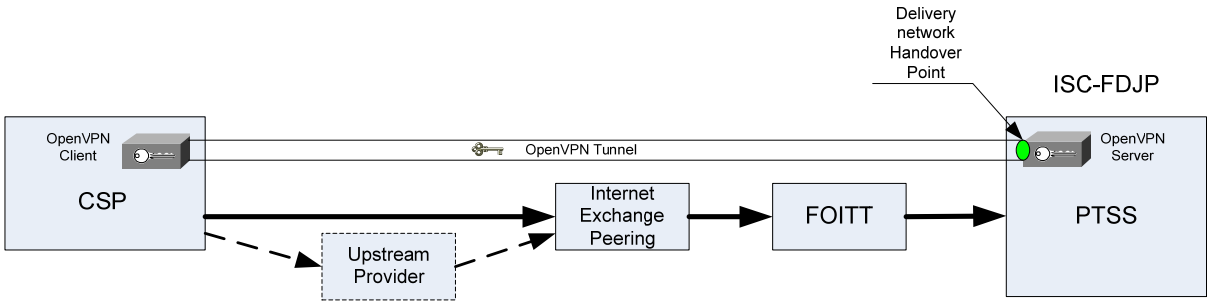

Figure 17: Schematic view of the OpenVPN delivery network

The PTSS is the single point of contact (SPOC) for the CSP.

16.6.2.5. Direct connection to ISC-FDJP [Informative]

The handover points of the CSP reside in the premises of the ISC-FDJP near the LEMF.. The ISC-FDJP provides in its premises a shared co-location for CSP. Each CSP is responsible for the installation and operation of its network termination equipment inside the co-location. The Delivery Network Handover Point between the CSP and the LEMF is the Ethernet port of the network termination equipment of the CSP. The interception data has to be handed over non-encrypted. The CSP is responsible for the data delivery up to the Delivery Network Handover Point.

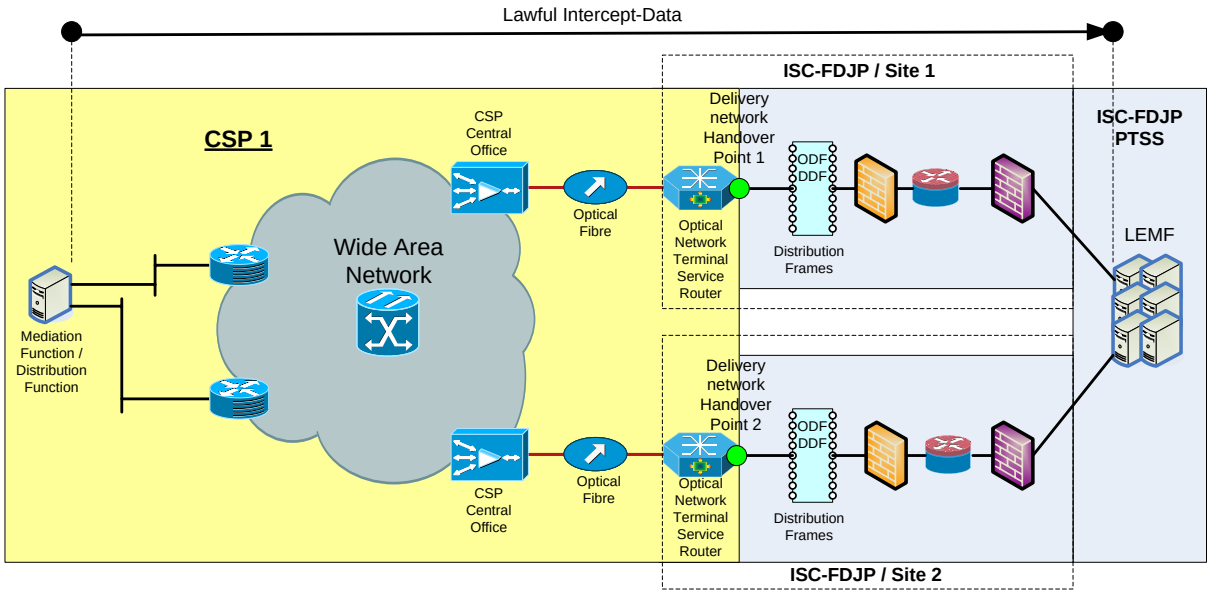

Figure 18: Schematic view of the direct connection to ISC-FDJP

The direct connection to ISC-FDJP must be redundant with disjoint paths and have a failover capability.

The implementation of the direct connection to ISC-FDJP must be agreed with PTSS. The technical details regarding the housing of equipment in the co-location premises as well as the supported protocol stacks and addressing schemes are provided by PTSS to the CSP on a bilateral basis.

16.6.2.5.1. *Attachment requirements for the IP-based delivery network for direct connection to ISC-FDJP*

The protocol stack for the IP delivery network connection is shown in the table below:

NETWORK	IP v4 according to IETF RFC 791
MAC-Frame	MAC Frame Format according to IEEE 802.3
PHYSICAL	Electrical or optical interface according to IEEE 802.3 1000BASE-T or 1000BASE-SX Connector: Electrical RJ-45 or optical LC.

17. Status and History of the Document

Version	Date	Comments & Remarks
	08.04.2011	TR TS Initial document for consultation
1.0	16.06.2011	TR TS (after consultation period of April-May 2011)
2.0	01.07.2011	TR TS after meeting of 24.06.2011 with CSP and authorities. - Change version number from 1.0 to 2.0 - Added definition of integer for the dimensioning formula in sections 9.1, 9.2.2 and 9.2.4 - Remove exception regarding Annex G in section 15
3.0	23.11.2011	TR TS after addition of fix internet and mobile data interceptions requirements. - Completion of dimensioning sections 9.2.1 and 9.2.3 - Mobile data delivery in section 12.1 - Internet broadband delivery in section 12.3 - Completion of ASN.1 table in section 16.5 - Corrections to XML DTD in sections 16.1 and 16.2 - Added section 16.6 Delivery network specifications Adapted references to new VÜPF version