Technical Guideline for the implementation of lawful measures for monitoring telecommunications

Swiss Designation: TR TS (Technical Requirements for Telecommunication Surveillance)

Version 0.2 Ready for Review

Limited to Annex G (Broadband Internet Access Monitoring)

Confidential

May 2009

This document follows the Technical Guideline for the Implementation of Legal Measures for Monitoring telecommunications created by European Telecommunications Standards Institute (ETSI).

The present technical regulation has been customized following the actual Swiss Surveillance Act and the related guidelines. It applies to every telecommunication provider operating in Switzerland or offering services to customers geographically based in Switzerland or abroad.

Contents

Document History

Version	**Date**	**Status**	**Remarks**
0.1	**April 2009**	**Draft**	A first draft was developed and presented to the parties.
0.2	**Mai 2009**	**Draft**	A pre-definitive version, ready for review.

Chapter 1 Regulatory scope of the Technical Guideline

This Technical Guideline (TR TS), in accordance with the general purpose described in Art. 15 of the Federal Act of 6 October 2000 on the Surveillance of Post and Telecommunications (SPTA) prescribes the technical rules in connection with the monitoring equipment and the necessary technical properties of the recording connections.

It also establishes the types of identifiers for which, in certain types of telecommunications equipment in addition to the destination and origin addresses used therein, additional measures are to be taken for the technical implementation of monitoring operations on the basis of the acts governing the monitoring of telecommunications.

Where technical progress has not yet been taken into account in the actual TR TS, the obligated parties must agree on the design of their monitoring equipment with the Postal Service and Telecommunication Surveillance (PSTS).

Chapter 2 TR TS in General

2.1 Chapter definition

General requirements are defined in the first section of this technical regulation.

The equipment and the related service specific requirements are described in separate annexes, contained in the second section which can be used together with the basic requirements and other requirements as stand-alone descriptions of the requirement for a specific handover interface:

- **Basic requirements (Chapter 5)**
  Basic requirements shall apply equally to all handover interfaces and are presented in Chapters 5 and 6. Delivery Point is also intended as basic requirement, described into Annex A; its handover interface is located at the PSTS.
- **Other requirements (Chapter 6)**
  Where necessary, the other regulatory areas in addition to the basic requirements may also be included into Chapter 6 of the present regulation.
- **Equipment- and service-specific requirements (Annex A, Annex G)**
  Specific requirements with regards to equipment its services are described into different related Annexes. Annex A in particular contains provisions about the allowed transmission methods. Annexe G contains the specification regarding Interception of Broadband Internet traffic.

Informative part (Annex X4, Annex X6)
Annex X4 contains a list of minimal required version of the ETSI specifications to be used in relationship with the present Swiss technical regulation.

Annex X6 corrects the ASN.1 module related to the TS 101 909-20-2 Technical Specification, witch is used in combination with Annex G.1.4.

2.2 Overview of the equipment- and service-specific annexes and the informative part - Actual situation in Switzerland

Annex A	Annex A describes the allowed transmission methods and the Delivery Network between Provider and PSTS.	
Annex A.1	Annex A.1 Delivery Network for Interception related information of Circuit Switched Interceptions	**TR CS** regulation is actually the official technical regulation exclusively covering this issue in Switzerland.
Annex A.2	Delivery Network between Provider and PSTS for Broadband Internet Surveillance	**Description in Annex A.2**
Annex A.3	Transmission of HI1 events and additional events	**OAR** regulation is actually the official technical regulation exclusively covering this issue in Switzerland
Annex A.4	Troubleshoots by transmitting interception data to the PSTS terminals for Broadband Internet Surveillance	**Description in Annex A.4**
Annex A.5	Annex A.5 Delivery Network for Call Content of Circuit Switched Interceptions	**TR CS** regulation is actually the official technical regulation exclusively covering this issue in Switzerland.

Annex B	Handover interface for circuit-switched networks (PSTN, ISDN and GSM). These national requirements were laid down before a corresponding ETSI standard was adopted and can now only be used for extensions to existing circuit-switched networks. The descriptions in Annex C shall apply to new circuit-switched networks.	**TR CS** regulation is actually the official technical regulation exclusively covering this issue in Switzerland.
Annex C	Provisions for **circuit-switched fixed and mobile radio networks** (PSTN and GSM) **and for GPRS** in accordance with ETSI standard ES 201 671 or ETSI specification TS 101 671 [22].	**TR CS** regulation is actually the official technical regulation exclusively covering this issue in Switzerland. GPRS related issues are actually not defined.
Annex D	Provisions for **UMTS networks** in accordance with 3GPP specification TS 33.108 [23].	**TR CS** regulation is actually the official technical regulation exclusively covering this issue in Switzerland. UMTS rules are actually defined for voice data only.
Annex E	Provisions for **storage devices** (**UMS**, **VMS** etc.) for voice, fax, SMS, MMS etc. As these types of systems are not taken into account in the provisions in Annexes A to D, these requirements may also need to be taken into account.	**TR CS** regulation is actually the official technical regulation exclusively covering this issue in Switzerland. Only Voicemail, FAX, SMS are actually defined.
Annex F	Provisions for the e-mail service in accordance with national requirements or ETSI specification **TS 102 232-02** [30]	**TR for the delivery of intercepted electronic mail (Packet Switched Service) regulation** is actually the official technical regulation exclusively covering this issue in Switzerland.
Annex G	Provisions for **direct subscriber-based access to the Internet** in accordance with ETSI specification TS 102 232-03 [31], TS 102 232-04 [32] or TS 101 909-20-2 [33]	**Description in Annex G**
Annex H	Provisions for VoIP and multimedia services which [lacuna] on SIP, RTP or H.323 and H.248 and for emulated PSTN/ISDN services in accordance with ETSI specifications TS 102 232-05 [34], TS 102 232-06 [35] and TS 101 909-20-1 [36]	**OAR** regulation is actually the official technical regulation exclusively covering this issue in Switzerland. Only TSP which provide for their subscribers a VoIP-solution that uses an E.164-Number, derived from the OFCOM numbering-range, as addressing element, are actually defined in this regulation.

Annex X.4	Table of applicable ETSI-Standards and specifications as well as the ASN.1 module	**Description in Annex X.4**
Annex X.6	Correction of the ASN.1 module of the TS 101 909-20-2 Technical Specification, used in Annex G1.4	**Description in Annex X.6**

Chapter 3 Reference standards

The following table contains the standards referring to Swiss technical regulations:

SPTA	Surveillance of Post and Telecommunications Act
SPTO	Ordinance of 31 October 2001 on the Surveillance of Post and Telecommunications
ES 201 671/ TS 101 671	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
ITU-T G.711	Pulse Code Modulation (PCM) of Voice Frequencies
RFC 2822	Internet Message Format

Chapter 4 Definitions and Abbreviations

4.1 Definitions

Content of Communication (CC)

The part of the telecommunication to be monitored which contains the information exchanged between the participants or their terminal equipment.

Copy of the monitored telecommunication

The copy of the monitored telecommunication consists of Content of Communication and Intercept Related Information, to be delivered to the lawful enforcement monitoring facility (LEMF).

Event data (Intercept Related Information or IRI)

The call data (known as Intercept Related Information or IRI in Europe and Call Data or CD in the US) consists of information about the targeted communications, like destination of a voice call (e.g., called party’s telephone number), source of a call (caller’s phone number), time of the call, duration and other similar related information.

IRI information is also generally related to all other telecommunication session made from any telecommunication device, with exception for the content of the communication.

Internet access route

The transmission route the Internet subscriber uses for Internet access other than the one made over the telephony network, by using analogical or digital modems.

Telecommunications equipment-O (TCE-O)

In general, the Telecommunications equipment belonging to the Obligated party (the Telecommunication Service Provider), where a monitored telecommunication line or identifier sends outgoing traffic or receives incoming traffic.

Transit network

The network used for sending the copy of the monitored telecommunication traffic (CC and IRI).

The content coming from TCE-O is effectively delivered to the lawful enforcement monitoring facility (LEMF).

4.2 Abbreviations

The following abbreviations are used in the TR TS:

ASCII	American National Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
BA	ISDN Basic Access
BC	Bearer Capability
CC	Content of Communication
CLIP/R	Calling Line Identification Presentation / Restriction
COLP/R	Connected Line Identification Presentation / Restriction
CUG	Closed User Group
DCF77	DCF77 stands for D=*Deutschland* (Germany), C=long wave signal, F=Frankfurt, 77=frequency: 77.5 Khz. It is a 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
ERMES	European Radio Message System
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HI	Handover Interface
HLC	High Layer Compatibility
IMAP	Internet Message Access Protocol
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agencies
LEMF	Lawful Enforcement Monitoring Facility
LI	Lawful Interception
LLID	Lawful Interception Identifier
MAP	Mobile Application Part
MMS	Multimedia Messaging Service
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber ISDN Number
MSN	Multiple Subscriber Number
NEID	Network Element Identifier
OID	Object Identifier
POP3	Post Office Protocol – Version 3
PSTN	Public Switched Telephone Network
PSTS	Postal Service and Telecommunications Surveillance

SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPTA	Surveillance of Post and Telecommunications Act
SPTO	Ordinance of 31 October 2001 on the Surveillance of Post and Telecommunications
Target	Line or identifier that is to be monitored
TCE-O	Telecommunications equipment belonging to the obligated party (the TSP)
TCP	Transport Control Protocol
TSP	Telecommunications Service Provider
UDI	Unrestricted digital information
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	8-bit Unicode Transformation Format (RFC 3629, ISO 10646)
VoIP	Voice Mail System
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
XML	Extensible Markup Language

Chapter 5 Basic requirements

Technical Guidelines for monitoring and configuring the handover interface to the PSTS.

5.1 Copy transmission of monitored telecommunication

Monitored telecommunications copies are composed of communication content and event data.

Rerouted or forwarded communications shall be part of the monitored copy transmission.

The event data in principle has to be immediately generated after the occurrence of the corresponding event (e.g. invocation, cancellation or activation of a service or supplementary service, use of a supplementary service for data transmission). This has to be sent to the PSTS.

An event data set containing relevant data shall be transmitted at the beginning and at the end of the monitored telecommunication. In addition, event data shall be also delivered during the telecommunication session every time activities should appear (e.g. service activation).

During the transmission, content of communication (CC) and associated event data (IRI) must be clearly identifiable and logically associable. For this purpose, each monitoring operation receives a reference number (LIID).

5.2 General requirements pertaining to circuit-switched networks (PSTN and GSM)

All telecommunication surveillance guidelines regarding circuit switched network operated by PSTN, GSM, UMTS technology are described in the external TR CS Document.

All packet based services on GSM- and UMTS-Networks are not yet part of the actual Swiss telecommunication surveillance measures.

5.3 General requirements for the Email service

All telecommunication surveillance guidelines regarding E-Mail-Services are described in the external “Technical Requirement for the delivery of intercepted Electronic Mail” document.

5.4 General requirements for the Internet access route

In accordance with Article 15 BÜPF, operators of transmission routes providing direct user-based Internet access (e.g. Internet access routes via xDSL, CATV, WLAN) are committed to take measures for monitoring the whole IP-traffic.

Annex G contains three different ETSI specific possibilities for exporting monitored packet switched traffic on layer 3, layer 2 or based on a IPCablecom architecture.

5.5 Requirements for VoIP using E. 164 ITU-T

TSP must be able to activate an interception activity for VoIP targets using E.164 call identity number.
All telecommunication surveillance guidelines regarding the actual VoIP interception are described in the external TR-CS document.

Chapter 6 Other requirements

The present chapter contains additional mandatory provisions, for implementing target identities for the interception of the Internet access route.

Please refer to the external OAR document for the defined target identities.

Chapter 7 Certification

Every TSP shall follow a predefined certification procedure, provided for a specific telecommunication type. The single certification procedures are described in the external “Certification Procedures for TSP” document.

Every TSP which has to be registered by OFCOM shall obtain the proper certification from the PSTS. If a registered provider doesn’t follow the certification procedures and conditions, he will be forced to immediately install the necessary equipment, whenever a surveillance measure with regards to its customers should appear. This immediate and specific procedure will be ordered from the TSPS and will be mandatory for the TSP.

Chapter 8 Final provisions

According to article 15 SPTA, TSP must deliver the results of interception by following the present technical regulation and all other annexed or referred document.

This technical regulation comes into force on August 1st 2009.

A period of transition is provided and will last 11 month, from August 1st 2009 expiring on June 30 2010.

After the transition period all officially registered providers shall be certified from PSTS.

3003 Bern, ...

Postal Service and Telecommunications Surveillance PSTS

René Koch

Head of Business Unit PSTS

Annex A

Annex A describes the transmission methods, the delivery network between Provider and PSTS, troubleshoots by transmitting interception data and the transmission of HI1 events and additional.

Annex A.1 Delivery Network for Interception related information of Circuit Switched Interceptions

TR CS regulation is actually the official technical regulation exclusively covering this issue in Switzerland

Annex A.2 Delivery Network between Provider and PSTS for Broad-band Internet Surveillance

General Information

Delivery Network has to be able to handle multiple parallel interceptions and use a strong encryption method.

There are two possibilities for the delivery Network between the TSP and the PSTS:

1. the Internet connection to the PSTS (usual case)

2. a redundant fiber optic connection.

   The use of any fiber optic connection must be planned and agreed in every case with the PSTS.
   The detailed solution shall be presented in the Declaration of Compliance.

1. Internet connection

For the Internet connection to the PSTS a redundant Open VPN solution is provided by the PSTS. The providers can connect themselves with their Open VPN compatible product of their choice to the VPN server.
For compatibility assurance reason the PSTS recommend to implement Open-VPN SW also at the Provider side.
The transition point for the lawful interception data is a virtual IP-address, which is provided by the Open VPN solution.

VPN-Connection Test

PSTS provides monitor facilities at disposal to every TSP for checking the Internet Access and the VPN Servers connections.

Connection Concept

Every TSP can choose its own technical implementation. This has to be specified in the Declaration of Compliance which will be verified and agreed by the PSTS. The PSTS can give recommendations regarding the proposed delivery network solution.
PSTS will provide the needed certificate for a strong encryption and a short configuration guide for the setup of the recommended Open-VPN SW at the Provider side.
For quality assurance reasons the used transmission method of the LI related data within the provider network shall be presented in the Declaration of Compliance.

Annex A.4 shall be applied for assuring the lossless Lawful Interception Data transmission.

The table below indicates the actually used PSTS side encryption software solution. The following software is recommended for ensuring a maximal compatibility degree between TSP and PSTS.

No.	Manufacturer	Product name	Contact
1	Open-VPN	Open Source	http://openvpn.net/

2 Redundant Fiber optic connection

This type of delivery Network must be planned and agreed with the PSTS.
For the fiber optic connection the provider shall install a VPN box of his own choice at the two PSTS locations. A remote access to the box can be realized with an ISDN basic access. The transition point for the lawful interception data is located at the output of the VPN box (clear text Ethernet port).

Connection Concept

Every TSP can choose its own technical implementation. For the redundant fiber optic connection: a failover concept (e.g. with VRRP or a similar technology) and the specification for the used VPN technology has to be specified in the “Declaration of Compliance” which will be verified and agreed by the PSTS. The PSTS can give recommendations regarding the proposed delivery network solution.
For quality assurance reasons the used transmission method of the LI related data within the provider network shall be presented in the Declaration of Compliance.

On the first of January 2011 the PSTS will be equipped with a redundant LEMF (lawful enforcement monitoring facility). From this date on, providers using the Internet connection have to implement redundant equipments and connections.

The concept described in the Annex A.4 combined with the high availability of the delivery network must ensure the transmission of the Lawful Interception Data without any loss.

Annex A.3 Transmission of HI1 events and additional events

OAR regulation is actually the official technical regulation exclusively covering this issue in Switzerland

Annex A.4 Troubleshoots by transmitting interception data to the PSTS terminals for Broadband Internet Surveillance

Principles

If it appears to be temporarily impossible to deliver a copy of the monitored telecommunication to the PSTS (e.g. as a result of a malfunction in the transmitting equipment of the TCE-O or by encountering network overload), all data sets must be temporarily buffered and completely transmitted afterwards.

The call attempts for sending the copy of the monitored telecommunication shall be automatically reinitiated, unless otherwise agreed with the PSTS for the specific trouble.

Technical implementation

Initial repeated attempts to establish a connection

If a trouble appears by transmitting the copy of the monitored telecommunication, further connection attempts shall automatically be done.

Those first reconnect attempts should be done at least 5 times and should occur at least every 5 to 10 seconds.

If the connection to the PSTS can be re-established, all the event data and the copy of the content of communication shall be transmitted until the buffer is emptied.

If the copy of the monitored telecommunication cannot be sent to the PSTS, even after the above mentioned attempting procedure, the event data and CC must be physically stored for a later transmission.

Further attempts at establishing a connection

After the initial five repeated attempts, other recursive attempts shall be made every minute for a period of 24 hours.

If however the transmission has not been re-established, the following two options can be adopted:

OPTION 1

Event data (IRI) and Call Content (CC) shall be saved to another standard storage medium (DVD or Harddisk) and sent to the PSTS by appropriate means by fast and reliable logistics service. Event data may also be sent by secure e-mail on request.

After formal confirmation from PSTS, the original stored (buffered) data contained into the TCE-O can be deleted.

The PSTS can extend the attempts period till 1 week, if a trouble solution guarantees the right delivery of CC and IRI Data within this extension period.

In case of emergency, the temporary storage solution shall be delivered every 12 hours or as reasonably requested from the PSTS.

OPTION 2

TSPS can declare the circumstances as not urgent; in this case the TSP will receive instruction for waiting until the connection will be re-established and transmit the stored data. The TSP shall use their due diligence for ensuring the full recording of the monitored data on the TCE-O.

Detected troubles which impair the telecommunication monitoring or transmission shall be sent and immediately reported to the PSTS. An IRI Alarm Report is set

In case of IRI failure, the Alarm Report must nevertheless be generated and transmitted by using encrypted Email, FAX or mail.

Annex A.5 Delivery Network for Call Content of Circuit Switched Interceptions

TR CS regulation is actually the official technical regulation exclusively covering this issue in Switzerland

Annex G Provisions for the Internet access route in accordance with ETSI specifications TS 102 232-03, TS 102 232-04 and TS 101 909-20-2 in conjunction with TS 102 232-01

Preliminary remarks

This Annex describes the conditions for the handover interface in accordance with ETSI specifications TS 102 232-03, TS 102 232-04 and TS 101 909-20-2 for those transmission routes (e.g. xDSL, CATV, WLAN) that are used for direct subscriber-related access to the Internet.

These ETSI specifications use the general IP-based handover interface as described in the TS 102 232-01 specification.

Annex G contains specific details with regards to the national specification as well as additional technical requirements.

If, in addition to Internet access service, broadcasting services or other public services (e.g. IP-TV, video on demand) are also provided, the Internet Traffic only shall be intercepted, without interfering with other content transmission.

Point to Point broadcasting services must be fully monitored (e.g. home user streaming, closed group data transmission).

In addition to the requirements in Chapters 5 and 6, the following annexes also apply:

Annex	Contents
Annex A.2	Delivery Network between Provider and PSTS for Broadband Internet Surveillance The copy of the monitored telecommunication is transmitted via TCP/IP over the Delivery Network between Provider and PSTS.
Annex A.3	OAR is actually the official technical regulation exclusively covering this issue in Switzerland.
Annex A.4	Troubleshoots by transmitting interception data to the PSTS terminals for Broadband Internet Surveillance
Annex X.4	Table of applicable ETSI/3GPP standards and specifications as well as the ASN.1 module
Annex X.6	Correction of the ASN.1 module of the TS 101 909-20-2 Technical Specification, used in Annex G1.4

Annex G.1 Choice of options and specification of additional technical requirements

Annex G.1.1 Choice of options and specification of additional technical requirements pertaining to ETSI TS 102 232-01

The following table describes the available options for defining the TS 102 232-01 ETSI specification and also specifying some additional requirements. Unless specified otherwise, the references in the table relate to the sections of the ETSI specification:

Section TS 102 232-01	Description of the option/problem area and provisions for national application	Additional requirement, background/additional information
5.2.1	**Version** As a result of the use of an OID in the ASN.1 description, a separate parameter is not necessary.	
5.2.2	**LIID** A unique value will be assigned by PSTS via HI-1 interface**.**	
5.2.3	**Authorisation country code** ‘CH’ shall be used in Switzerland.	
5.2.4	**Communication identifier** In Switzerland, 'CH' shall be used as the *delivery country code*. The operator identifier is issued by the OFCOM	The Operator Identifier consist of the ISO 3366-1 code in Numeric-3 format. For Switzerland (756) followed be the 10 Digit "TISP Number" assigned by OFCOM.
5.2.5	**Sequence number** The sequence number must already be set up where the copy of the monitored telecommunication was first generated (interception point).	In some cases this requirement cannot be followed. In those cases the sequence number must be ensured so that this function will be set up before the delivery function or at its same point. In any case the sequence number must reproduce the precise counting method at the place of origin. If UDP is used on this route, additional measures must be taken to actively avoid possible packet losses and to safeguard the order.
5.2.7	**Payload Direction** Shall be implemented for CC if applicable.	fromTarget(0) or toTarget(1) or unknown
6.2.2	**Error Reporting** The transmission is based in principle on the external OAR Document.	
6.2.3	**Aggregation of payloads** The aggregated transmission of monitored IP packets is provided in order to avoid unnecessary overhead.	However, this must not exceed a few seconds and must be agreed with the PSTS.
6.2.5	**Padding Data** Can optionally be implemented by the obligated party.	The PSTS must consent to the use of padding in operations.
6.3.1	**General** TCP/IP is used.	

Section TS 102 232-01	Description of the option/problem area and provisions for national application	Additional requirement, background/additional information
6.3.2	**Opening and closing of connections** There are no circumstances specified (refers to NOTE) to close down the transport connection	
6.3.4	**Keep-alives** Can optionally be implemented by the obligated party.	PSTS must consent to the use of keep-alives in operations in which the TCP connection is maintained.
6.4.2	**TCP settings** Port number is defined over HI1 from PSTS side (destination port) for export.	The port number applies in connection with the use of the service specifications TS 102 232-02, TS 102 232-03, TS 102 232-04, TS 101 909-20-2, TS 102 232-05 and TS 102 232-06.
7.1	**Type of Networks** Exported over the public Internet or over a redundant fiber optic connection	
7.2	**Security requirements** The requirements in Annex A.2 to the present document shall apply.	TLS must not be used nor must signatures and hash codes.
7.3.2	**Timeliness** The possible use of separate managed networks shall be agreed between the obligated party and the PSTS.	

Annex G.1.2 Choice of options and specification of additional technical requirements pertaining to ETSI TS 102 232-03

The following table describes the available options for the TS 102 232-03 ETSI Specifications and also specifies additional requirements. Unless specified otherwise, the references in the table relate to the sections of the ETSI specification:

Section TS 102 232-03	Description of the option/problem area and provisions for national application	Additional requirement, background/additional information
4.3.1	**Target Identity** The external OAR guideline shall apply for target identity. Chapter 6.2.2.	For instance, when a Cable Modem Identifier is used for monitoring an Internet Cable Acces, the Modem change or move must be considered.
6.1	**Events** The events and HI2 attributes from version 1.4.1 of the ETSI specification onwards shall be used.	In version 1.4.1 the event 'startOfInterceptionWithSessionActive' was added.

Annex G.1.3 Choice of options and specification of additional technical requirements pertaining to ETSI TS 102 232-04

The following table describes the available options with regards to the TS 102 232-04 ETSI Specification and also specifies additional requirements. Unless specified otherwise, the references in the table relate to the sections of the ETSI specification:

Section TS 102 232-04	**Description of the option/problem area and provisions for national application**	**Additional requirement, background/additional information**
4.2.1	**Target Identity** The external OAR guideline shall apply for target identity. Chapter 6.2.2.	For instance, when a Cable Modem Identifier is used for monitoring an Internet Cable Acces, the Modem change or move must be considered.
6.1	**Events** The events and HI2 attributes in version 1.3.1 of the ETSI specification shall be used.	Please note that in version 1.3.1 the event 'End of Interception Session_Active was deleted.

Annex G.1.4 Choice of options and specification of additional technical requirements pertaining to ETSI TS 101 909-20-2

The following table describes the available option for the TS 101 909-20-2 ETSI Specification and also specifies additional requirements. Unless specified otherwise, the references in the table relate to the sections of the ETSI specification:

Section TS 101 909-20-2	**Description of the option/problem area and provisions for national application**	**Additional requirement, background/additional information**
4.2	**Architecture** Implementation based on EuroDOCSIS is assumed.	Depending on the configuration of the TCE-O, in particular the scope of service, the PSTS may specify a particular version of the standard.
5	**LI architecture for IP multimedia Time Critical Services** The specification essentially refers to the remarks in ES/TS 101 671. Please refer to this specification.	The precise configuration of the monitoring equipment, in particular the events and associated parameters must be agreed with the PSTS.
Annex A	**ASN.1 modules** The TS101909202 module used contains syntax errors. A corrected version is contained in the Annex X.6.	
Supplement 1	**Target Identity** The external OAR guideline shall apply for target identity. Chapter 6.2.2.	For instance, when a Cable Modem Identifier is used for monitoring an Internet Cable Acces, the Modem change or move must be considered.

Annex G.2 Explanations regarding the ASN.1 descriptions

Extranet

The PSTS Extranet provides information, in accordance to the general purpose described on Article 15 of the Swiss Federal Law on the Monitoring of Postal and Telecommunications Traffic (BÜPF), on the applicable ETSI and 3GPP standards and specification, including their ASN.1 modules.

ASN.1 specification troubles

The use of various versions of the national ASN.1 module is also regulated. Annex X.4 contains further explanations.

The ASN.1 descriptions of the different modules for implementations in accordance with this Annex G shall be taken from the various versions of ETSI Specifications TS 102 232-01, TS 102 232-03, TS 102 232-04 and TS 101 909-20-2, whereby errors in the ASN.1 modules contained therein (e.g. wrong domain ID) must be corrected.

The following versions of the ASN.1 modules may be used once the above information has been updated on the PSTS Extranet.

Parameters

All the parameters contained in the ETSI Specification designated as ‘conditional’ and ‘optional’ should be adopted, if available and if no other specific description is contained in Annex G.1.

ASN.1 “OCTET STRING”

For the **ASN.1 “OCTET STRING”** format the following rules shall be followed:

- Where the standard defines a format for the individual parameters (e.g. ASCII or cross reference to a signalling standard), this must be used.
- If the format is not specified, both hexadecimal values must be entered in the individual bytes so that the higher value half-byte fills bit positions 5 – 8 and the lower value half-byte fills bit positions 1 – 4. (Example1: 4F H is entered as 4F H = 0100 1111 and not as F4 H. Example 2: DDMMYYhhmm = 23.07.2002 10:35 h is entered as '2307021035' H and not '3270200153'H)

Administrative and additional event

Administrative event (e.g. activation/deactivation/modification of an operation as well as fault reports) and additional event (e.g. with regard to manufacturer-specific services) are always transmitted in accordance with the external OAR document.

Annex X, Information and Updates

Preliminary remarks

Annex X contains the supplementary information regarding annex G.

Annex X.4 Table of applicable ETSI standards and specifications as well as the ASN.1 modules

PSTS provides all related ETSI Documents. The files are constantly uploaded on PSTS Extranet.

Please note that the table below is showing the minimal applicable version of each related Specification. Any superior version should be adopted from the TSP, for better performances.

Any existing syntax errors in the ASN.1 modules should be corrected. Please use the correct object identifier (OID) and the correct version number.

Applicable ASN.1 Module	**Version requirement**	**Requirement or instruction for application**
ETSI TS 102 232-01 (Annexes G)		
LI-PS-PDU, version 4	Version 1.4.1 or higher	
ETSI TS 102 232-03 (Annex G)		
IPAccessPDU, version 4	Version 1.6.1 or higher	
ETSI TS 102 232-04 (Annex G)		
L2AccessPDU, version 3	Version 1.3.1 or higher	
ETSI TS 101 909-20-2 (Annex G)		
PCESP, version-4(4)	Version 1.1.2 or higher	The original modules contain syntax errors; Annex X.6 contains corrected versions of these modules
TS101909202, interceptVersion (0)		

Annex X.6 ASN.1 modules in accordance with ETSI specification TS 101 909-20-2

The TS101909202 module of TS 101 909-20-2 ETSI specification, used in accordance with Annex G.1.4, contains syntax errors. These errors have been corrected in the following ASN.1 modules.

TS 101 909-20-2
ASN.1 module 'TS101909202'

```
TS101909202 {itu-t (0) identified-organization (4) etsi (0) ts101909 (1909) part20 (20) subpart2(2) interceptVersion (0)}

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN
```

```
TARGETACTIVITYMONITOR ::= SEQUENCE
{
     version          INTEGER DEFAULT 1,   -- header, version -
  lIInstanceid        LIIDdType,         -- header, who -
  timestamp          UTCTime,          -- header, when -
  targetLocation       LocationType,       -- header, where -
  direction          DirectionType,
  iRITransaction       IRITransactionType DEFAULT iRIreport,
  iRITransactionNumber    INTEGER,
  userSignal          UserSignalType,      -- Either copy or interpreted signalling
  cryptoCheckSum        BIT STRING         OPTIONAL
}
```

```
TTRAFFIC ::= SEQUENCE
{
      version         INTEGER DEFAULT 1,   -- header, version -
   lIInstanceid      LIIDdType,
   iRITransactionNumber   INTEGER,
   trafficPacket      BIT STRING,
   cryptoChecksum      BIT STRING  OPTIONAL
}
```

```
CTTRAFFIC ::= SEQUENCE
{
      version         INTEGER DEFAULT 1,   -- header, version -
   lIInstanceid      LIIDdType,
   correspondentCount    INTEGER,
   iRITransactionNumber   INTEGER,
   trafficPacket      BIT STRING,
   cryptoChecksum      BIT STRING  OPTIONAL
}
```

```
DirectionType ::= ENUMERATED
{
  toTarget,
  fromTarget,
  unknown
}
```

```
UserSignalType ::= CHOICE
{
  copySignal    BIT STRING,
  copyCharSignal  PrintableString,
  interpretedSignal INTEGER  -- Place holder
}
```

```
IRITransactionType ::= ENUMERATED
{
   iRIbegin,
   iRIcontinue,
   iRIend,
   iRIreport
}
```

```
LocationType ::= CHOICE
{
   geodeticData    BIT STRING,
   nameAddress     PrintableString (SIZE (1..100))
}
```

```
LIIDType ::= INTEGER (0..65535) -- 16 bit integer to identify interception
```

```
END
```