Annex 2 to the Ordinance of the Federal Department of Justice and Police (FDJP) of
15 November 2017 on the conduct of the Surveillance of Post and Telecommunications
(VD-ÜPF; SR 780.117)

Technical requirements for the delivery networks for the conduct of the Surveillance of Telecommunications

Version 2.0

Entry into force: 01.01.2024

1 Scope of application

The present document is the Annex 2 to the ordinance of the FDJP of 15 November 2017 on the conduct of the surveillance of post and telecommunications (VD-ÜPF).

It defines the technical requirements for the delivery networks between the Communications Service Providers (CSP) and the Processing System (*Verarbeitungssystem*) of the Post and Telecommunications Surveillance Service (PTSS) for information requests and responses, interception instructions, results of real-time and retroactive interceptions (historical data) as well as results of emergency searches and tracing. It also covers the attachment requirements per handover point for CSPs.

Based on the VD-ÜPF and its annexes and after hearing the concerned CSP, PTSS bilaterally specifies in writing the details of the connection between the CSP and the Processing System. These details include the physical handover points, the network addresses, the access points, the responsibilities, the contact details, the service levels and the detailed diagrams of the delivery networks as well as the access arrangements (24/7) to the premises of PTSS for CSPs using co-location for direct connection.

The reason for separating such information into several documents lies in their different life cycles and the confidential nature of certain information as well as the specific features of the interfaces. The VD-ÜPF and its annexes are in the public domain. Confidential information must therefore be drafted separately in documents accessible only to the concerned parties.

Contents

2 Abbreviations

3GPP	Third Generation Partnership Project
AS	Autonomous System
BÜPF	“Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1)” - Federal Act of 18 March 2016 on Post and Telecommunications Surveillance
CA	Certification Authority
CC	Content of Communication
CS	Circuit-switched
CSP	Communications Service Provider
DN	Delivery Network
DN-HP	Delivery Network - Handover Point
DSF	Delivery Stack & Formats
DSL	Digital subscriber line
DSS1	Digital Subscriber Signalling System No 1
E.164	International public telecommunication numbering plan defined by ITU-T
ETSI	European Telecommunications Standards Institute
FDJP	Federal Department of Justice and Police
FOITT	Federal Office of Information Technology, Systems and Telecommunication
HI	Handover Interface
HP	Handover Point
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIF	Internal Interception Function
IP	Internet Protocol
IRI	Interception Related Information
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunication Standardisation Sector
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LI-HP	Handover Point at the level of LI formats
LIID	Lawful Interception Identifier
MAC	Media Access Control (sub-layer of Layer 2 in the OSI Model)
MD	Mediation Device
NE	Network Equipment
NPS	Network Protocol Stack
PRA	Primary Rate Access
PS	Packet-switched
PSTN	Public Switched Telephone Network
PTSS	Post and Telecommunications Surveillance Service
REL	Release Message
SR	“Systematische Sammlung des Bundesrechts” – Classified Compilation of Federal Legislation
TCP	Transport Control Protocol
VD-ÜPF	Ordinance of the FDJP of 15 November 2017 on the conduct of Post and Telecommunications Surveillance (SR 780.117)
VPN	Virtual Private Network
VÜPF	„Verordnung vom 15. November 2017 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11)“ - Ordinance of 15 November 2017 on Post and Telecommunications Surveillance

VVS-ÜPF	„Verordnung vom 15. November 2017 über das Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.12)“ - Ordinance of 15 November 2017 on the Processing System for Telecommunications Surveillance.
WDM	Wavelength-Division Multiplexing

3 Definitions

See section 3 of the Annex 1 to the ordinance of the FDJP of 15 November 2017 on the conduct of the surveillance of post and telecommunications (VD-ÜPF)

4 The Processing System for Telecommunications Surveillance

The Processing System for Telecommunications Surveillance is composed of several specialised components operated by PTSS according to the ordinance VVS-ÜPF.

The Processing System for Telecommunications Surveillance production environment is designed to be redundant, with a primary instance and a secondary instance at two separate sites. If there is a major breakdown at the primary instance which cannot be fixed within a specific timeframe, a failover procedure can be initiated by PTSS to make the secondary instance active. Except from the service interruption during the failover procedure, it is transparent to the CSP which instance is currently active. The Processing System for Telecommunications Surveillance can be accessed by virtual IP addresses distributed at both sites. Therefore, a CSP does not need to implement any manual processes for Processing System for Telecommunications Surveillance instance failover.

In addition to the Processing System Production instance, there are Integration_1 and Integration_2 instances for testing and training purposes.

The details for connecting CSP systems to the Processing System for Telecommunications Surveillance environments, including a connection matrix, are set out bilaterally in writing.

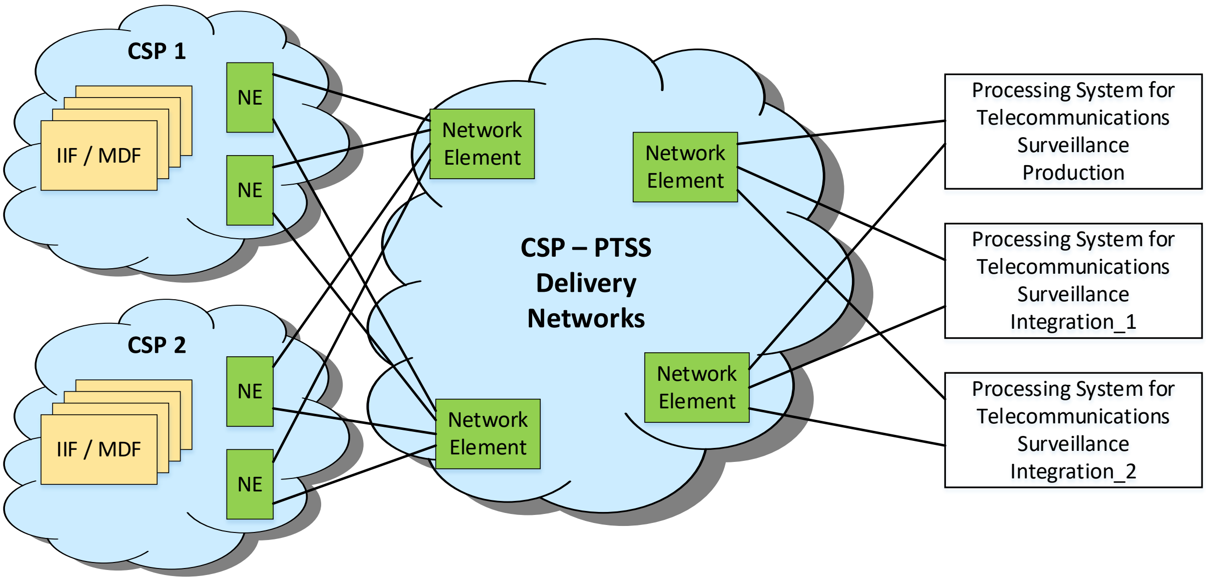

CSP 1
IIF / MDF
NE
NE
CSP 2
IIF / MDF
NE
NE
Network Element
Network Element
Network Element
Network Element
CSP – PTSS Delivery Networks
Processing System for Telecommunications Surveillance Production
Processing System for Telecommunications Surveillance Integration_1
Processing System for Telecommunications Surveillance Integration_2

Figure 1 Overview of the Processing System for Telecommunications Surveillance environments

5 General requirements for delivery networks

The following requirements apply to the delivery networks:

1. The DNs shall be built on existing products.
2. The DNs shall use functions already available, i.e. no new functions are to be specially developed for the DN.
3. The DNs are not “LI aware”, i.e. they are not developed specifically for lawful interception. Standard protocols and technologies shall be used.
4. The DN shall be designed in accordance with the Annex 1 to the VD-ÜPF, in order to ensure the timely delivery of the intercepted data.
5. Based on a threat analysis for the DN’s specific architecture, protective measures shall be defined for the DN in question.
6. Geographical redundancy shall be implemented to increase the DN’s reliability (two disjoint paths to each of the Processing System sites).
7. Cost-effective installation and operation should be sought.
8. Low administrative expenses should be incurred.
9. Appropriate DNs for CSPs of all sizes shall be defined, i.e. different solutions according to requirements (e.g. number of customers of the CSP, number of interceptions, network architecture of the CSP, data volume per interception).
10. The cost implications for all parties involved shall be taken into consideration.
11. PTSS and FOITT shall adhere to the federal rules on information protection and data security.
12. The DN’s scalability shall be ensured (fast and simple expansion of available capacity or bandwidth).
13. The hardware and software shall be vendor-neutral.
14. No PTSS equipment shall be on the CSP’s premises (except in the case of interceptions implemented by PTSS).
15. Responsibilities shall be clearly defined between all parties involved.
16. There shall be clear definition of the handover points (DN-HP) between all parties involved.
17. The DN implementation shall respect investment protection.
18. The DN shall be useable for data transmission in both directions (bi-directional), for example for requests and responses related to information requests, instruction management (tasking) and historical data.

6 Overview of the delivery networks

6.1 Functional architecture

The present document covers the delivery network (no. 4 in Figure 2) between the CSPs and the Processing System for Telecommunications Surveillance in accordance with the Swiss LI reference model. The access network (no. 6 in Figure 2) between the Processing System and the LEA is not addressed in the present document.

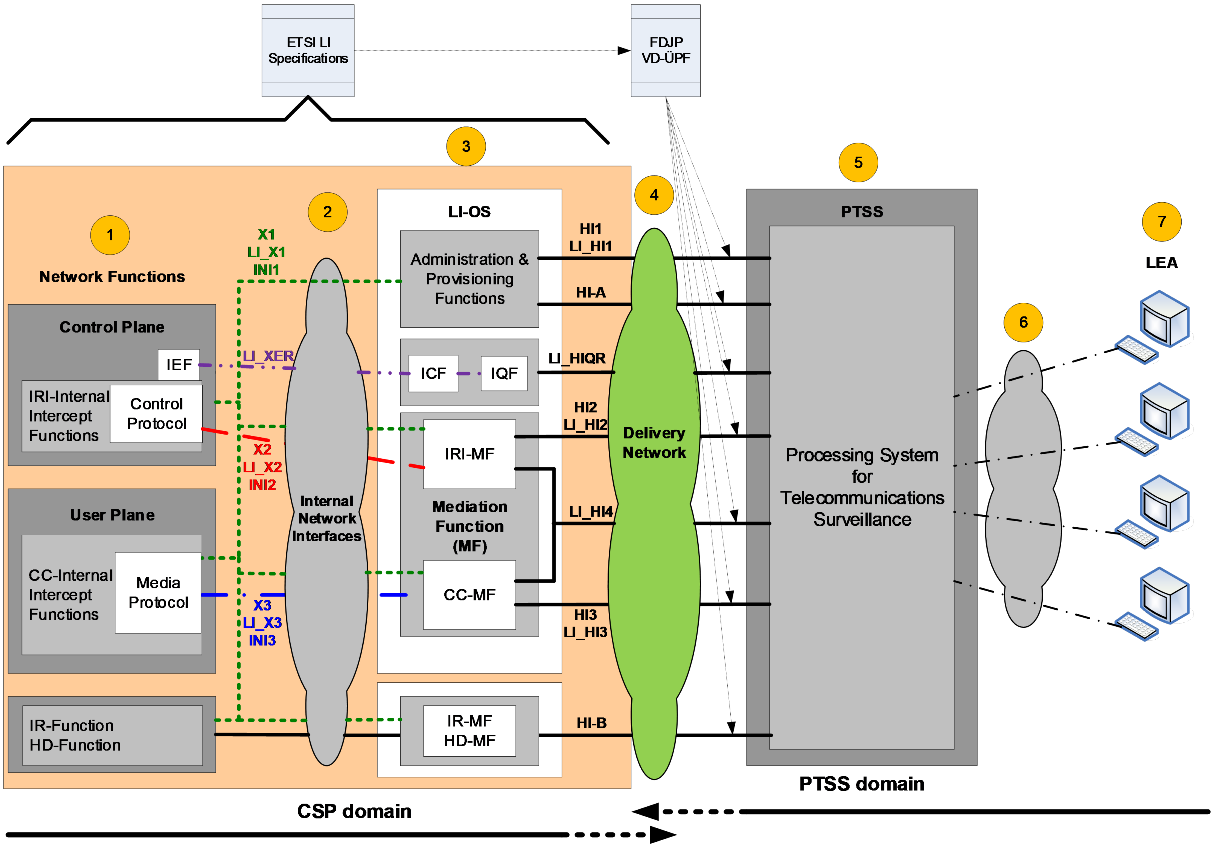


Figure 2 Swiss LI reference model

Figure 2 shows the functional LI architecture in Switzerland, based on the ETSI reference architectures.

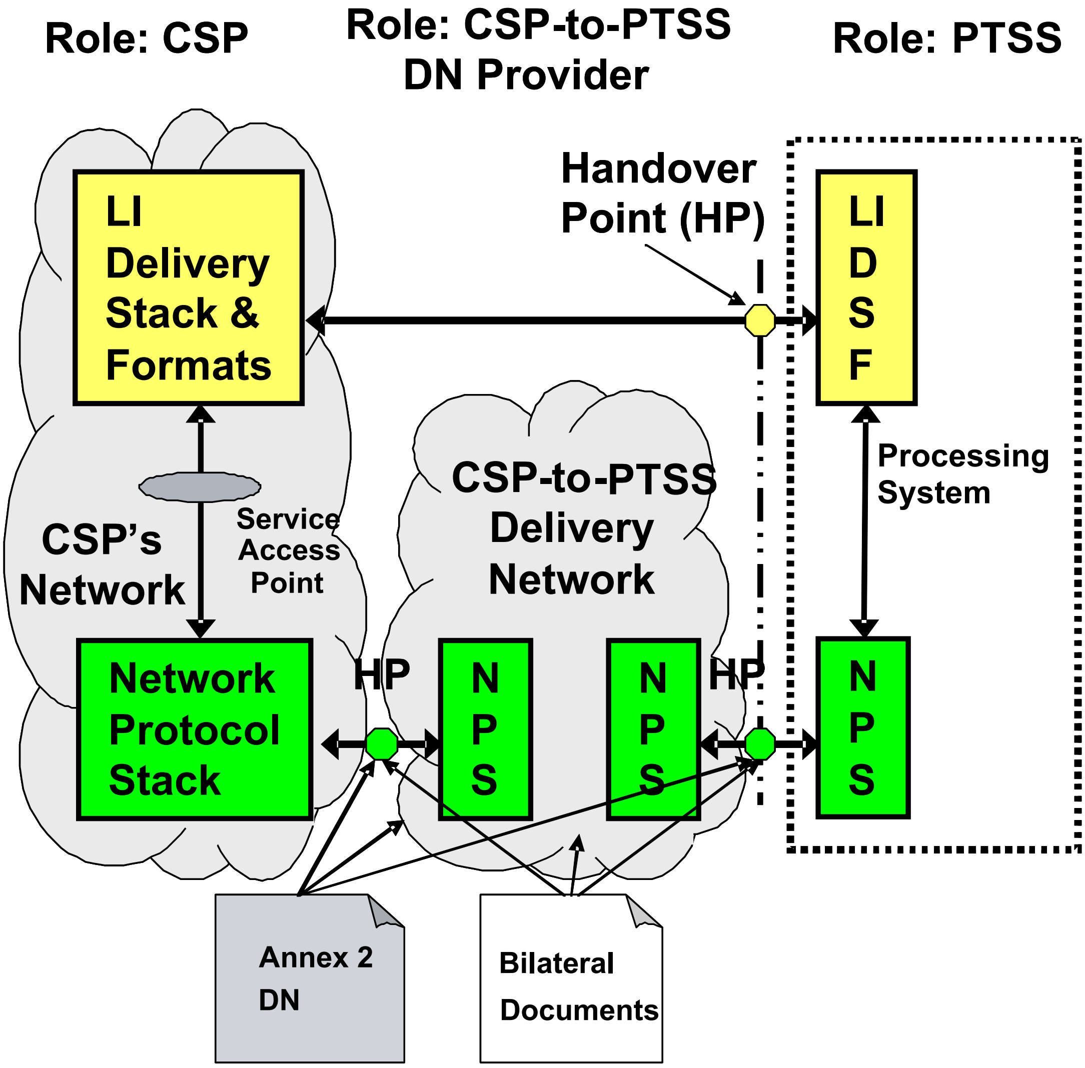


Figure 3 Roles, protocol stacks and handover points between the CSP and PTSS

Figure 3 shows the layers *delivery networks* and *lawful interception formats*. Delivery networks are transparent for lawful interception formats, i.e. they do not check or change the interception data delivered. Furthermore, Figure 3 shows the relationship between the CSP and PTSS in accordance with the Swiss LI reference model. For the purposes of the present document, only the CSP-to-PTSS delivery network and the corresponding handover points are of relevance.

CSP-to-PTSS delivery is ensured by various roles in different network sections. Handover points exist between the various roles.

A distinction is made between handover points at the level of:

a. Delivery networks (DN-HP), and

b. Lawful interception formats (LI-HP), i.e. LI-specific information (CC, IRI formats).

The DN-HP and the LI-HP may be coincident. This is the case at the CSP end in Figure 3. Elsewhere (e.g. in the CSP's network), the DN-HPs are associated with a Service Access Point (SAP) between a delivery network layer (Network Service Provider) and a lawful interception layer (Network Service User).

As mentioned in section 1, bilateral documents are drawn up between PTSS and each CSP connected to the DN. The bilateral documents define the detailed technical interface requirements a CSP must meet in order to be able to connect to the DN, contain confidential information concerning the interfaces, addresses and delivery networks (e.g. telephone numbers, IP addresses, network diagrams), services (e.g. contacts, availability, failure notifications) and specify the service level required of the corresponding delivery network, as well as the mechanisms and parameters required by a user entity (e.g. user system, system administrator) for configuration purposes.

The specifications set out in the present document and in the bilateral documents contain all the information needed for implementation and operation of user systems of the corresponding delivery networks.

The document governing the level of lawful interception formats is the Annex 1 to the VD-ÜPF. These aspects are not described in the present document.

6.2 Overview of roles in the DN

1. Role of the CSP
2. Role of the Processing System
3. Role of the delivery network provider

6.3 Overview of the Processing System network interfaces with CSPs

1. IP-based interface HI3 for delivering CC of CS real-time interceptions;
2. IP-based interface HI3 or LI_HI3 for delivering CC of real-time PS interceptions;
3. IP-based interface HI2 for delivering IRI of real-time CS interceptions;
4. IP-based interface HI2 or LI_HI2 for delivering IRI of real-time PS interceptions;
5. IP-based interface LI_HI4 for delivering notifications;
6. XML over HTTPS administrative interface HI1 for instructing real-time interceptions (eWarrant and ad-hoc);
7. XML over HTTPS administrative interface HI-A for instructing retroactive interceptions (HD request);
8. XML over HTTPS interface HI-A for making Information Requests (IR request);
9. XML over HTTPS interface HI-B for delivering results of retroactive interceptions (HD response);
10. XML over HTTPS interface HI-B for delivering results of Information Requests (IR response);
11. XML over HTTPS interface LI_HIQR for sending and delivering temporary to permanent identity associations.
12. Secure Email as a fallback or, as the case may be, alternative solution for interfaces no. 6 – 10.

6.4 Overview of the delivery networks between the Processing System and CSPs

1. IP DN: Delivery network for interfaces no. 1 – 11;

Note: Interface numbers are according to section 6.3.

6.5 Basic topologies of delivery networks

Delivery networks can be divided into two basic topologies:

1. Stratified delivery networks, see Figure 4;
2. Concatenated delivery networks, see Figure 5 and Figure 6.

There are also combinations of these basic topologies.

The diagrams refer to the area between the CSP and the handover point to the PTSS domain.

Another distinction can be made by the implementation of the handover point, which may be either:

1. in-house (see Figure 4 and Figure 6), or
2. in-span (see Figure 5).

In-house handover points require the hosting of third-party equipment by the owner of the premises (co-location). An advantage is that the connecting link can be kept short, which makes troubleshooting easier in the case of breakdowns and allows for physical protection against unauthorised access (e.g. cage).

In-span handover points generally require longer connecting links, possibly with cable ducts, splices, etc. Troubleshooting takes longer in the case of a breakdown, and physical protection against unauthorised access is generally only possible if the handover point is in the same building.

Note on Figure 4, Figure 5 and Figure 6: These figures give no guidelines for the connection between the Processing System primary instance and secondary instance. From the CSP's point of view, there is only one Processing System production environment. Aspects regarding failover (minimising the impact if the primary instance breaks down) and the forwarding of information to the Processing System secondary instance are not described here. Likewise, no guidelines are given on how to implement at the CSP end the transition from the MD to the NE, which serves as a gateway to the delivery network.

Figure 4 shows an approach for a delivery network based on an upper and a lower stratum. The upper stratum has the lower stratum under its control, as higher protocol layers between the MD and the Processing System are in one hand. The Processing System "sees" only the upper stratum, which falls under the responsibility of the CSP supposed to deliver the interception results.

The LI-HP and DN-HP of a CSP are coincident, which, in the event of an error, requires a triage in a two-part relationship (CSP/Upper Stratum Provider and PTSS). If the lower stratum is provided by a third party, here too there is a two-part relationship (CSP/Upper Stratum Provider and Lower Stratum Provider).

A typical example of such an approach is a fibre optics network, separated by WDM filters (lower stratum) and an upper stratum per CSP consisting of a network using an allocated wavelength (one possible implementation for such a DN is sub-variant B1 “Shared fibre infrastructure” of IP DN delivery variant B).

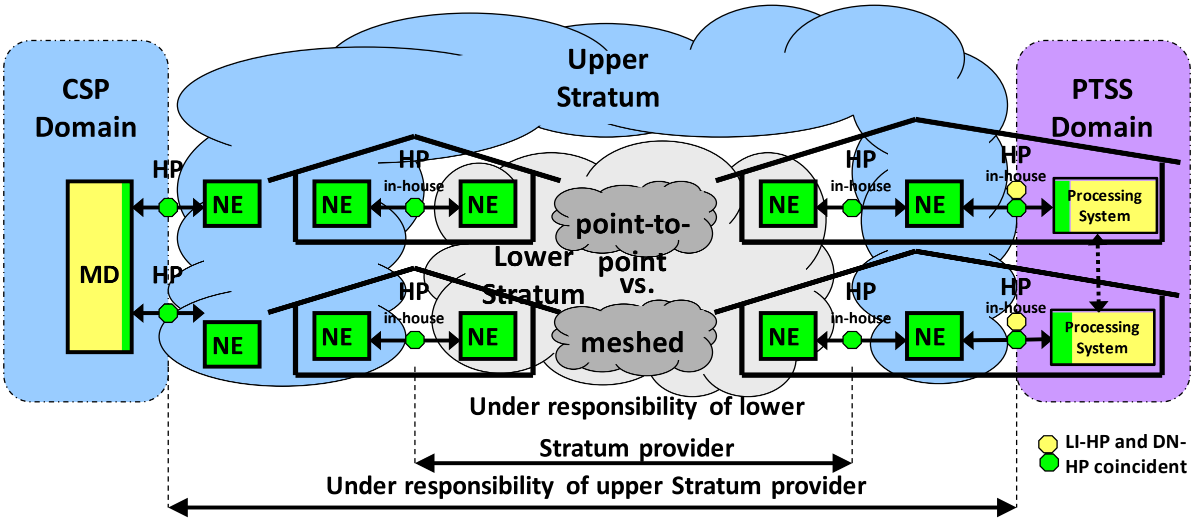


Figure 4 Stratified delivery network

Figure 5 and Figure 6 show an approach for a delivery network based on concatenated sub-networks. These sub-networks can have a different top protocol layer.

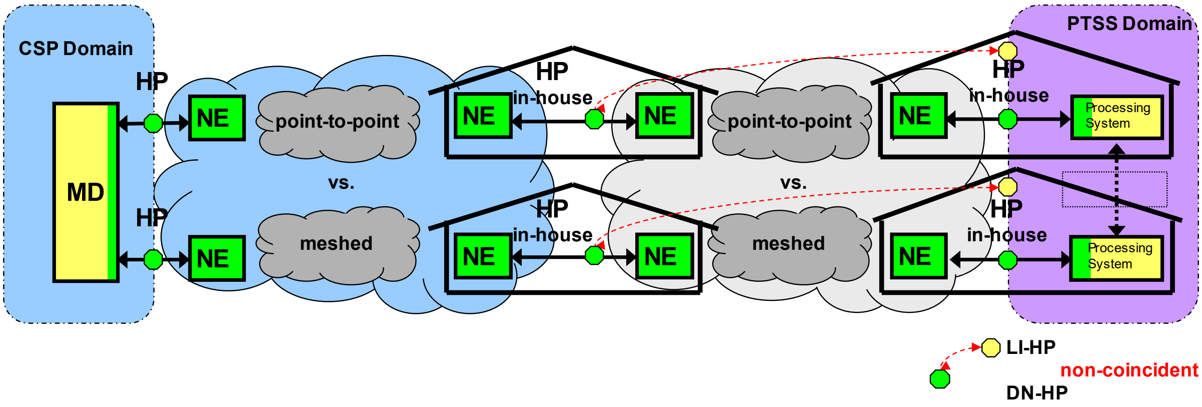


Figure 5 Concatenated delivery network with in-house handover point

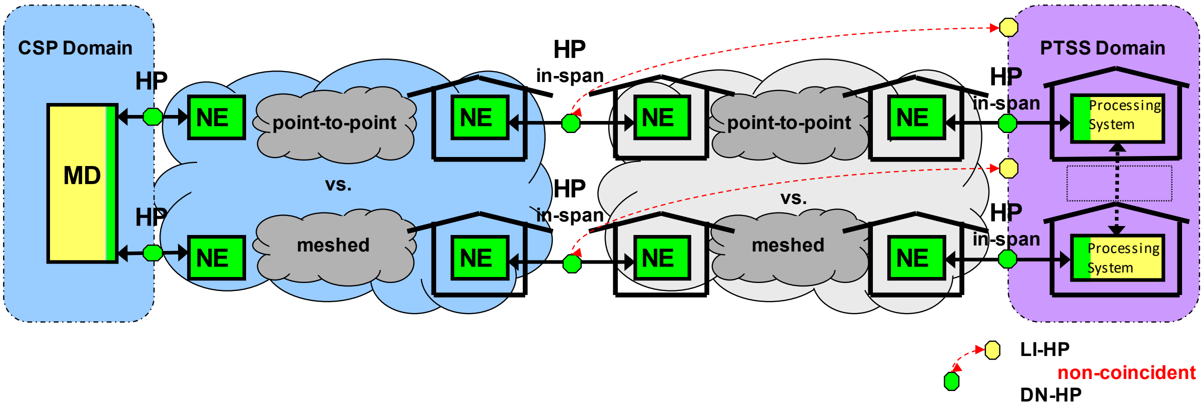


Figure 6 Concatenated delivery network with in-span handover point

The LI-HP and DN-HP of a CSP are not coincident, which, in the event of an error, requires a triage in a relationship between three parties (CSP (blue), DN provider (grey) and PTSS (purple)). If the Processing System detects that LI information is missing at the LI-HP, it shall be determined whether the fault lies with the CSP (blue), the DN Provider (grey) or PTSS (purple). One possible implementation of such a Concatenated DN is variant A “OpenVPN”.

7 CS delivery networks

CS delivery network is not supported by PTSS and shall not be used. Any real-time interception performed on circuit-switched services, such as ISDN networks, shall be converted and delivered on the IP delivery network by the means of standardized IP packet based protocols.

For the delivery of CS interception data, two different interfaces are used in accordance with the Annex 1 to the VD-ÜPF.

1. HI2 handover interface for Interception Related Information (IRI) via the IP DN;
2. HI3 handover interface for Content of Communication (CC) via the IP DN.

8 IP delivery networks

8.1 Capacity (bandwidth) of the IP DN

The dimensioning of the DNs shall be agreed bilaterally between PTSS and the CSP. The bandwidth of a DN must be large enough to deliver the interception data including overhead on time and without any information loss resulting from traffic overload in the DN.

8.2 Variants of IP delivery networks

The variant ultimately chosen by a CSP must be agreed upon with PTSS.

There are currently two variants of the IP DN:

A) OpenVPN;

B) Direct connection of a CSP to PTSS.

In order to accommodate new requirements such as bi-directional transmission of instruction management (tasking) data or historical data, the IP DN variants shall be adapted accordingly.

8.2.1 IP DN Variant A: OpenVPN

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

The CSP shall set up one or more individual VPN tunnels to the Processing System. PTSS is the single point of contact (SPOC) for the CSP.

The CSP shall acquire its VPN clients at its own discretion.

The FOITT is the provider of IP DN Variant A. The CSP manages the connections with the FOITT and arranges for the required service level through Service Level Agreements with its peering partner or upstream provider.

PTSS acquires the VPN servers. PTSS is responsible for the connection between the delivery network provider (FOITT) and the Processing System. The VPN keys and certificates are managed and assigned by PTSS as the Certificate Authority (CA).

PTSS defines the IP addressing plan which is mandatory. PTSS publishes an informative guideline called *OpenVPN Handbook* which provides details to the CSPs on how to implement the VPN access.

The CSPs can use Internet upstream, private or public peering with the FOITT. In order to reduce the risk of interruption, the delivery from the CSP shall provide as much redundancy as possible.

The CSP is responsible for its Internet accesses and for the correct operations of the VPN client. The VPN tunnel is the joint responsibility of the CSP and PTSS. PTSS is responsible for the correct operations of the VPN server. Problems shall be dealt with in accordance with the error handling process (see Section 12).

8.2.1.1 VPN tunnel CSP - Processing System

One or more VPN tunnels are configured between the CSP and the Processing System.

8.2.1.2 Overview

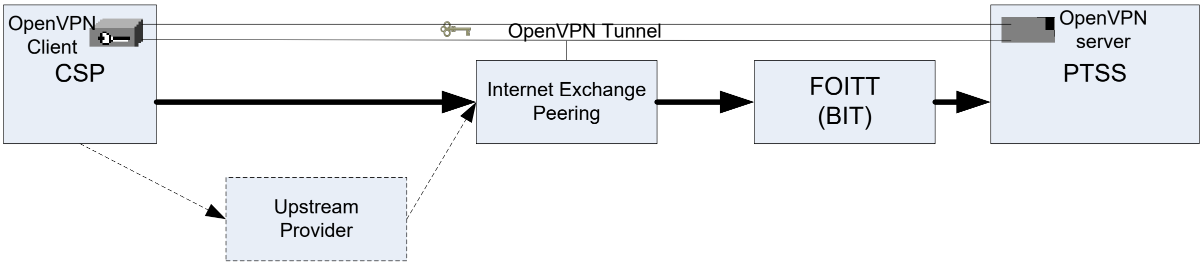
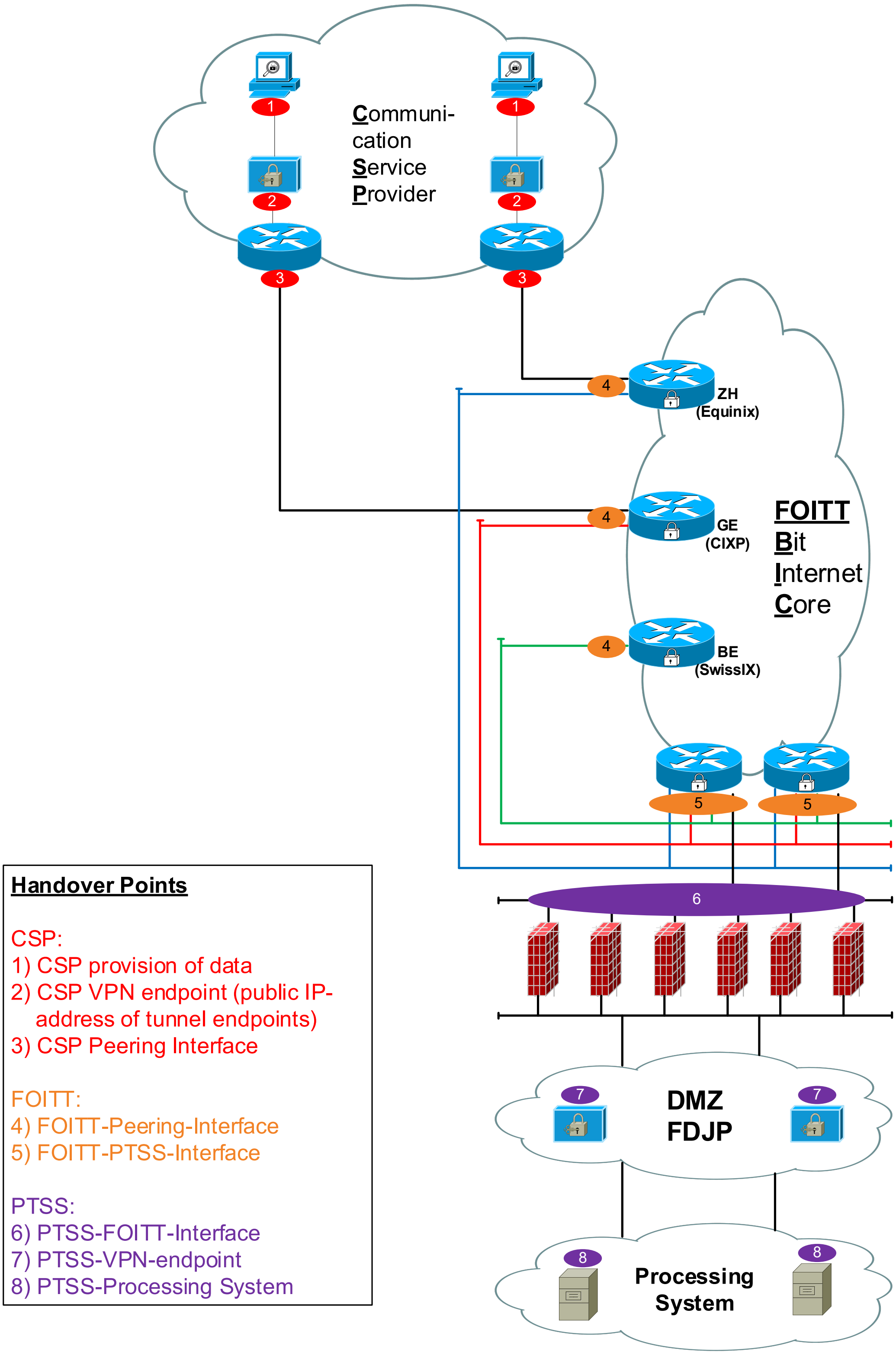


Figure 7 Schematic layout of IP DN Variant A: OpenVPN



Handover Points

CSP:
1) CSP provision of data
2) CSP VPN endpoint (public IP-address of tunnel endpoints)
3) CSP Peering Interface

FOITT:
4) FOITT-Peering-Interface
5) FOITT-PTSS-Interface

PTSS:
6) PTSS-FOITT-Interface
7) PTSS-VPN-endpoint
8) PTSS-Processing System

Figure 8 Handover points of IP DN Variant A: OpenVPN

Regarding the physical handover points 3 and 4 in Figure 11, there are basically two configurations from the CSP’s point of view:

1. No direct peering with the FOITT (connection via upstream provider to the FOITT);
2. Direct peering with the FOITT (direct peering agreement between the CSP’s AS and the FOITT’s AS).

8.2.1.3 Threat analysis of the IP DN Variant A: OpenVPN

The bilateral documents shall define specific protective measures for the following points:

- Confidentiality (including data protection);
- Authentication;
- Authorised access availability (i.e. no refusal of authorised access to network elements, saved information, information flows, services and applications but not in terms of general availability);
- Data integrity;
- Non-repudiation (incontestability of receipt of the data, similar to a registered letter with acknowledgment of receipt).

8.2.1.4 Scalability of the IP DN Variant A: OpenVPN

The scalability of the DN is restricted by the overall capacity of the FOITT transport network (backhauling) to the Processing System and by the capacity of the CSP’s peering partner or Internet access. The OpenVPN variant thus offers a limited available bandwidth.

The FOITT peering interface can be expanded up to a certain maximum bandwidth. There is also a maximum bandwidth for the FOITT transport network (backhauling) and the FOITT-PTSS interface. However, on account of the redundancy, the maximum individual bandwidth available per CSP is lower than the overall bandwidth.

The throughput within an OpenVPN tunnel is also limited. This capacity can be increased by using more powerful processors (vertical scaling). Also, additional OpenVPN tunnels may be added (horizontal scaling). The details are addressed in the bilateral documents between PTSS and the CSPs.

8.2.2 IP DN Variant B: Direct connection of a CSP to PTSS

The CSP’s handover point (DN-HP) resides on the premises of PTSS, near the Processing System. PTSS provides on its premises a shared co-location for a limited number of CSPs. Each CSP is responsible for the installation, operation and maintenance of its network termination equipment within the co-location. The interception data is handed over at the DN-HP non-encrypted. The CSP is responsible for the data delivery up to the handover points (DN-HP) on the premises of PTSS.

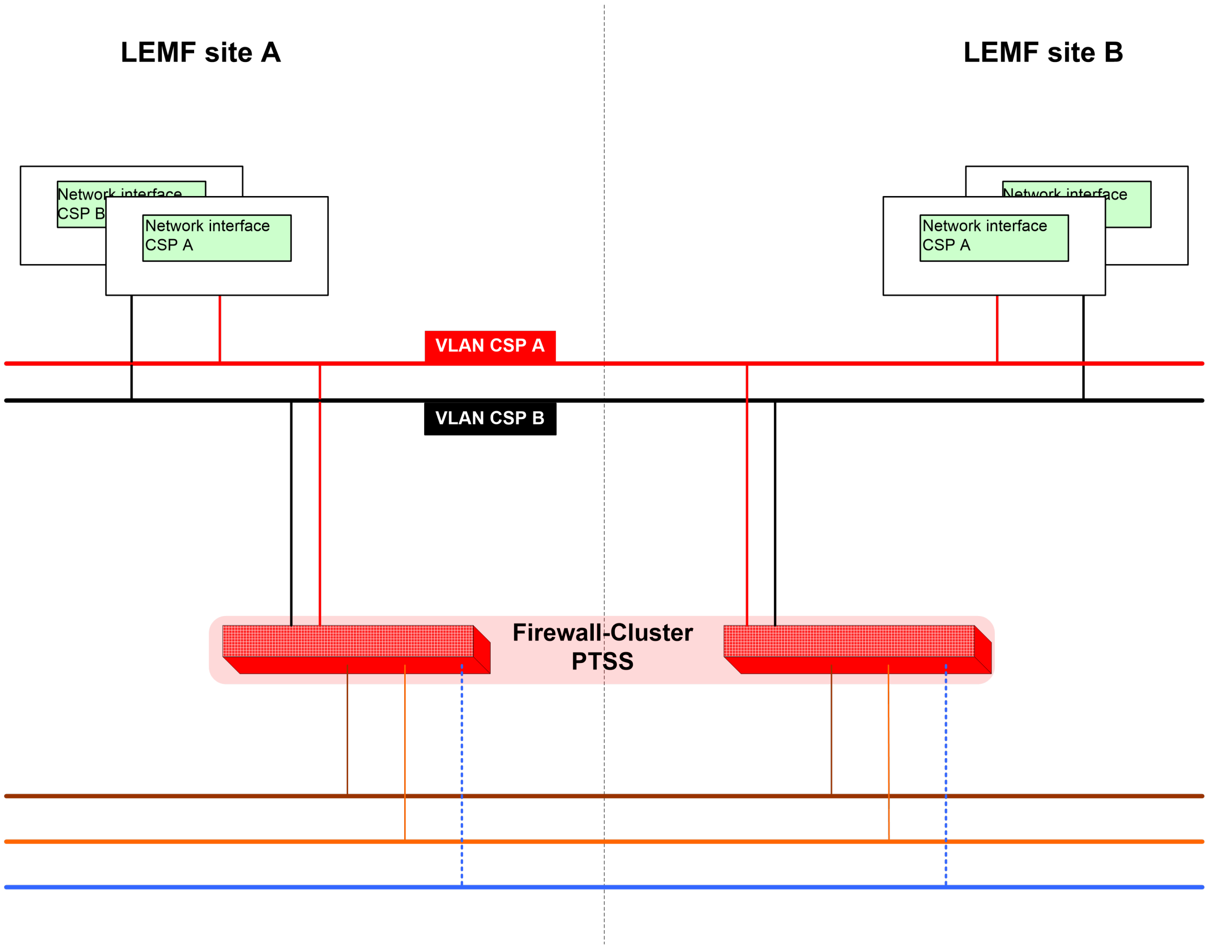


Figure 9 Schematic layout of IP DN Variant B: Direct connection of a CSP to PTSS

The DN-HP between the CSP and the Processing System is the Ethernet port of the CSP's network termination equipment. A handover interface with the following specifications is available per CSP at each of the two Processing System sites:

- 1000BASE-SX, 1000BASE-T, 1000BASE-LX, 10GBASE-SR or 10GBASE-LR;
- Connector: Electrical RJ-45 or optical LC;
- No Spanning Tree Protocol (STP);
- Untagged.

The interfaces at both Processing System sites are connected on Ethernet level. Special attention shall be given to avoid loops at the CSP end.

There are solutions with or without the CSP's router on the premises of PTSS. A CSP is free to decide whether it wishes to set up its router in PTSS' co-location facility or elsewhere.

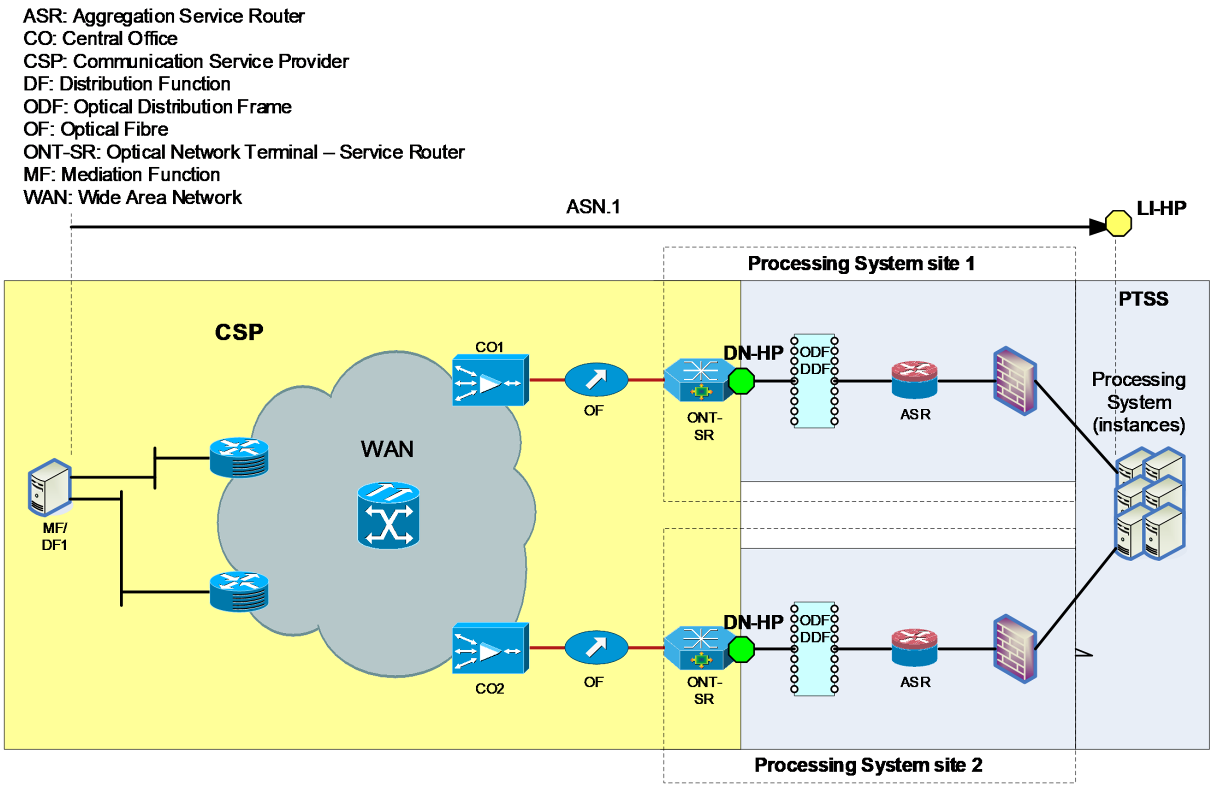


Figure 10 IP DN Variant B: Direct connection of a CSP to PTSS

8.2.2.1 Threat analysis of the IP DN Variant B: Direct connection of a CSP to PTSS

The bilateral documents shall define specific protective measures for the following points:

- Confidentiality (including data protection);
- Authentication;
- Authorised access availability (i.e. no refusal of authorised access to network elements, saved information, information flows, services and applications but not in terms of general availability);
- Data integrity;
- Non-repudiation (incontestability of receipt of the data, similar to a registered letter with acknowledgment of receipt).

8.2.2.2 Scalability of the IP DN Variant B: Direct connection of a CSP to PTSS

The scalability of the DN in this variant is restricted by the technology and interfaces used. The details are addressed in the bilateral documents between PTSS and the CSPs.

8.2.3 IP DN sub-variant B1: Shared access infrastructure

The providers of a shared access infrastructure may offer other CSPs the possibility of sharing the available access media between two co-locations of a shared access provider and both co-locations of PTSS. The DN-HPs are described in Figure 16. This allows CSP to take advantage of their existing interconnection points with a provider of a shared access infrastructure (e.g. fibre access) and to get a direct connection to PTSS without having to build it physically.

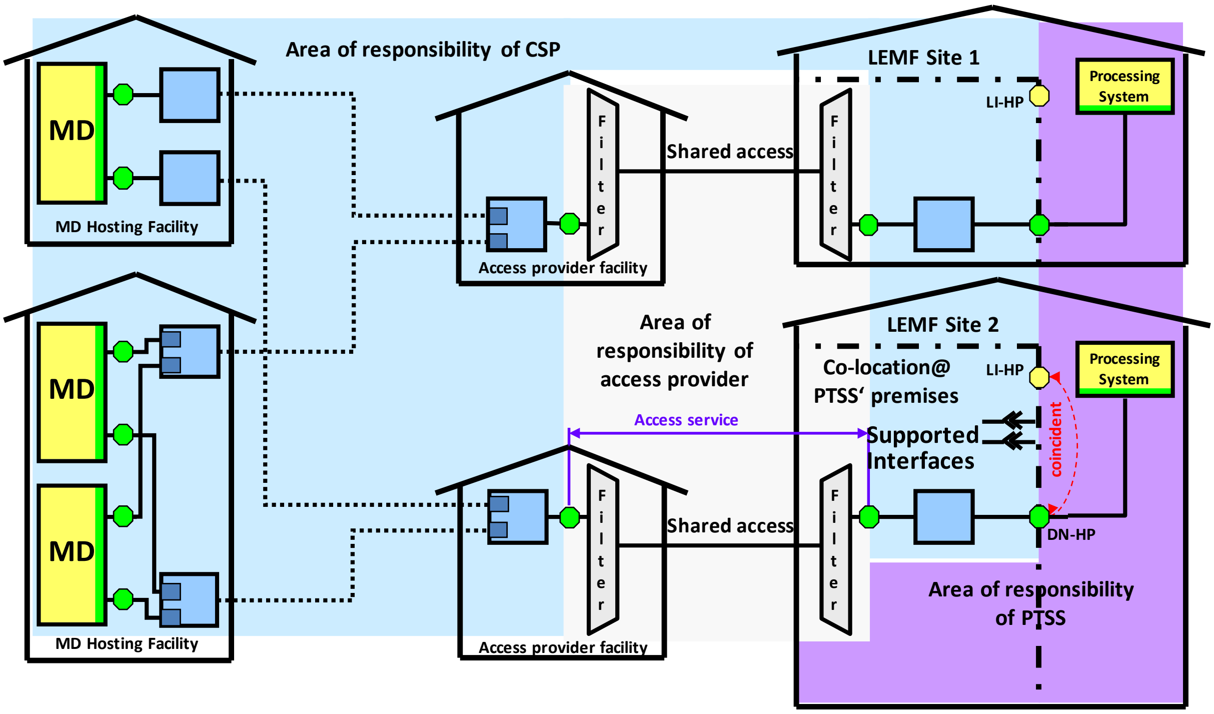


Figure 11 End-to-End view of shared access infrastructure

8.2.3.1 Threat analysis of the IP DN sub-variant B1: Shared access infrastructure

The bilateral documents shall define specific protective measures for the following points:

- Confidentiality (including data protection);
- Authentication;
- Authorised access availability (i.e. no refusal of authorised access to network elements, saved information, information flows, services and applications but not in terms of general availability);
- Data integrity;
- Non-repudiation (incontestability of receipt of the data, similar to a registered letter with acknowledgment of receipt).

In the basic concept it is assumed that no service higher than level 1 is implemented between the CSP network and the transport provider network. Otherwise, the functional layers in the bilateral documents shall be amended as appropriate. Higher protocol layers are separated in the upper stratum under the control of a single CSP.

8.2.3.2 Scalability of the IP DN sub-variant B1: Shared access infrastructure

The scalability of this IP DN sub-variant is limited by the technology and the interfaces used. For example, in the case of a shared fibre access infrastructure, different wavelengths can be used for the transmission. The details are addressed in the bilateral documents between PTSS and the CSPs.

8.3 XML over HTTPS interfaces

The administrative handover interface HI1 is used for instructing real-time interceptions whereas the administrative handover interface HI-A is used for instructing retroactive interceptions (see section 4.2 of the Annex 1 to the VD-ÜPF) as well as for making information requests (see section 8.5 of the Annex 1 to the VD-ÜPF).

The handover interface HI-B serves for the transmission of retroactive interception results (historical data, see section 7.5 of the Annex 1 to the VD-ÜPF) and the results of information requests (IR responses, see section 8.5 of the Annex 1 to the VD-ÜPF).

The handover interface LI_HIQR serves for the transmission of Identity Association Queries and Responses (see section 8.5.2 of the Annex 1 to the VD-ÜPF).

The keys and certificates are managed and assigned by PTSS as the Certificate Authority (CA). Alternatively, the CSP can generate the keys, send a Certificate Signing Request (CSR) to PTSS and have it signed by PTSS as the CA. If the request is successful, PTSS sends the certificate to the requesting CSP.

9 Security

9.1 Scope

The data transmission across the delivery networks must be secured. Such data consists of information requests and responses, interception instructions, as well as results of real-time and retroactive interceptions (historical data).

The following general objectives must be met:

- Protection from deliberate acts;
- Protection from inadvertent damage;
- Protection from organisational defects;
- Protection from technical failure;
- Protection from human error.

The specific security-related aspects of the individual DN variants are addressed in the "Threat analysis" sections in chapter 8.

Note: The internal security requirements within the CSP domain and the PTSS domain as well as the protection from the effects of fire, water, natural hazards and other disasters are not dealt with here.

9.2 Reliability and availability

The target value for the availability of the delivery networks per CSP to the DN-HP, in the case of a direct connection, or to point 3 in Figure 11, in the case of OpenVPN, is 99.8% (calculated over a calendar year). Although the OpenVPN connections via the Internet are on a “best effort” basis, they shall include redundancy.

A high degree of reliability of the DN (avoidance of complete failure of the DN) is achieved by avoiding Single Points of Failure.

The administrative interface using secure email may be used to support several administrative processes. In addition, the secure email can also be used to transport results of retroactive interceptions and information requests results.

The Processing System is geographically distributed over two sites. If one Processing System instance breaks down, PTSS is responsible for switching from one end to the other. The failover mechanism and internal routing are controlled by the Processing System and shall not impact the CSPs.

The CSPs shall implement a redundant delivery via disjoint paths or other suitable measures so that traffic can be routed via an alternative delivery path in the case of a breakdown.

10 Quality of service

The OpenVPN DN variant uses the Internet which does not provide resource reservation control mechanisms. This means that delivery of data via the Internet is on a “best effort” basis. There is no guarantee in terms of quality of service (e.g. latency, IP packet loss). However, the CSPs shall make all reasonable effort to avoid data loss, especially by using Internet accesses with sufficient bandwidth and by scaling up the OpenVPN tunnels.

If the bandwidth requirements of a CSP cannot be met with the OpenVPN DN variant then the CSP shall implement the direct connection variant according to prior agreement with PTSS.

11 Protocol stack for the IP delivery network

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, 1000BASE-SX, 1000BASE-LX, 10GBASE-SR or 10GBASE-LR Connector: Electrical RJ-45 or optical LC

For connecting to IP delivery networks, the systems being attached shall support at least one protocol stack for the lower layers capable of providing the bandwidth required to deliver the results of interception for a specific service with the specified number of concurrent interceptions.

Protocol stacks with Tagged MAC Frame Format are preferred.

MAC-Frame	Basic MAC Frame Format according to IEEE 802.3 clause 3.1.1, 3.2, 3.3 and 3.4
PHYSICAL	1000Base-T according to IEEE 802.3 clause 40 Connector: RJ45

MAC-Frame	Basic MAC Frame Format according to IEEE 802.3 clause 3.1.1, 3.2, 3.3 and 3.4
PHYSICAL	1000Base-SX or 1000Base-LX, according to IEEE 802.3 clause 38 single-mode or multi-mode Connector: LC with single-mode or multi-mode fibre

MAC-Frame	Basic MAC Frame Format according to IEEE 802.3 clause 3.1.1, 3.2, 3.3 and 3.4
PHYSICAL	10GBASE-SR or 10GBASE-LR, according to IEEE 802.3 clause 49 single-mode or multi-mode Connector: LC with single-mode or multi-mode fibre

MAC-Frame	Tagged MAC Frame Format according to IEEE 802.3 clause 3.2 (in particular 3.2.7 item b)), 3.3 and 3.4, and IEEE 802.1Q clause 9 and Annex C
PHYSICAL	1000Base-T according to IEEE 802.3 clause 40 Connector: RJ45

MAC-Frame	Tagged MAC Frame Format according to IEEE 802.3 clause 3.2 (in particular 3.2.7 item b)), 3.3 and 3.4, and IEEE 802.1Q clause 9 and Annex C
PHYSICAL	1000Base-SX or 1000Base-LX, according to IEEE 802.3 clause 38 single-mode or multi-mode Connector: LC with single-mode or multi-mode fibre

MAC-Frame	Tagged MAC Frame Format according to IEEE 802.3 clause 3.2 (in particular 3.2.7 item b)), 3.3 and 3.4, and IEEE 802.1Q clause 9 and Annex C
PHYSICAL	10GBASE-SR or 10GBASE-LR, according to IEEE 802.3 clause 49 single-mode or multi-mode Connector: LC with single-mode or multi-mode fibre

For connecting to the delivery network, the systems being attached shall support IP according to IETF RFC 791.

In relation to the IP-Header, the systems being attached to the delivery network shall meet the following requirements:

a) It shall be possible to enter into the equipment any source address and any destination address.

b) It shall be possible to enter into the equipment any sub-net mask.

c) It shall be possible to enter into the equipment any value for the field Precedence/TOS according to IETF RFC 791 and DiffServ according to IETF RFC 2474, respectively.

12 Equipment hosting

The use of in-house handover points in PTSS premises by a CSP requires equipment hosting. The following basic requirements shall be met by the hoster’s building infrastructure and the hosted equipment. The details of the equipment hosting shall be agreed between the CSP and PTSS in the bilateral documents.

12.1 Power supply and earthing

With regard to the power supply, the systems must comply with the European standard ETSI ETS EN 300 132-3 V2.2.1 (2021-07) “Environmental Engineering (EE); Power supply interface at the input to telecommunications equipment; Part 3: Operated by rectified current source, alternating current source or direct current source up to 400 V”.

With regard to earthing, the systems must comply with the European Standard ETSI EN 300 253 V2.2.1 (2015-06) "Environmental Engineering (EE); Earthing and bonding configuration inside telecommunications centres". A server farm (consisting of locally installed equipment) is also classified as “telecommunication equipment”.

12.2 Environmental conditions

Environmental conditions refer to the conditions to which the equipment is exposed in the course of transportation, installation and operation. This concept paper refers only to the conditions for installation and operation.

For indoor operation, the equipment must at least meet the requirements of the ETSI European Standard EN 300 019-1-3 V2.4.1 (2014-04) “Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-3: Classification of environmental conditions; Stationary use at weather protected locations".

For the broadband network equipment listed below, the requirements for “Class 3.2” must be met.

1. DSL port;
2. Combined ports (e.g. MSAN, analogue/DSL, ISDN/DSL);
3. Network termination for ISDN basic access;
4. WiMAX base station;
5. Optical line termination (OLT).

For equipment in operation according to Class 3.1, operators and manufacturers are required to declare any loss of performance caused by exceptional conditions. Losses of performance are not permitted unless declared in advance.

12.3 Maximum power dissipation of equipment

All equipment providers of a delivery network (this may be a CSP itself, or a third party that provides a delivery network) that is hosted by another third party must declare the maximum power dissipation (in W) of their equipment.

12.4 Electromagnetic compatibility (EMC)

The equipment must comply with the European Standard ETSI EN 300 386 v2.2.0 (2020-10) “Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electro Magnetic Compatibility (EMC) requirements”, with regard to the emission of electromagnetic interference and immunity to such interference.

12.5 Electrostatic discharge (ESD)

The equipment must comply with the European Standard ETSI EN 300 386 v2.2.0 (2020-10) “Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electro Magnetic Compatibility (EMC) requirements", with regard to electrostatic discharge to humans or objects.

12.6 Resistibility to overvoltage and overcurrent

The equipment must comply with the European Standard ETSI EN 300 386 v2.2.0 (2020-10) "Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electro Magnetic Compatibility (EMC) requirements", with regard to resistibility to overvoltage and overcurrent.

12.7 Uninterruptible power supply (UPS)

The UPS equipment must comply with the Technical Report ETSI TR 102 446 V1.1.1 (2005-11) "Environmental Engineering (EE); General Requirements for UPS for use in Telecommunication Environment". Both Processing System sites have a UPS and an emergency power supply.

12.8 Safety

The Electrosuisse (SEV) standards with regard to electrical safety must be met.

12.9 Space requirements

All providers of delivery network equipment (this may be a CSP itself, or a third party providing a delivery network) that is hosted by another third party, must declare the space requirements of their equipment.

13 List of Technical Specifications

This section provides a list of the ETSI European Telecommunication Standards (ETS), ETSI European Standards (EN), ETSI Technical Reports (TR), IEEE Standards and IETF Requests for Comments (RFC) used in the present document. It is meant to ease the reading.

ETSI EN 300 019-1-3 V2.4.1 (2014-04)	Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-3: Classification of environmental conditions; Stationary use at weather protected locations
ETSI ETS EN 300 132-3 V2.2.1 (2021-07)	Environmental Engineering (EE); Power supply interface at the input to telecommunications equipment; Part 3: Operated by rectified current source, alternating current source or direct current source up to 400 V
ETSI ETS EN 300 253 V2.2.1 (2015-06)	Environmental Engineering (EE); Earthing and bonding configuration inside telecommunications centres
ETSI EN 300 386 V2.2.1 (2020-10)	Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electro Magnetic Compatibility (EMC) requirements
ETSI TR 102 446 V1.1.1 (2005-11)	Environmental Engineering (EE); General Requirements for UPS for use in Telecommunication Environment
IEEE 802.3™-2015	IEEE Standard for Ethernet
IETF RFC 791	Internet Protocol
IETF RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

Table 13-1: List of technical specifications