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

Delivery Network Concept

Concept paper on delivery networks between CSPs and the ISS for telecommunication surveillance of packet-switched and circuit-switched services

Date: 30 January 2012

Version: 1.0

Next review: 1 February 2013 (yearly review)

Address and contact:

Federal Department of Justice and Police FDJP
IT Service Centre ISC-FDJP
Post and Telecommunications Surveillance Service
Fellerstrasse 15
3003 Bern

https://www.li.admin.ch

Contents

List of figures

1 Purpose of this document

Given the evolution of the technology of telecommunications networks, there is a need to create new delivery networks in IP technology and possibly to replace the existing delivery networks.

This document describes solutions for the delivery of PS and CS interception data to the LEMF ISS by way of appropriate delivery networks. It also covers the attachment requirements per handover point for CSPs.

The document “Technical Requirements for Telecommunication Surveillance” (TR TS) [4] specifies the attachment requirements for delivery networks, the interfaces, the data formats (LI formats) and the mechanisms based on the relevant ETSI or 3GPP standards. It also contains the dimensioning parameters for the number of concurrent interceptions to be delivered.

Furthermore, based on this Delivery Network Concept, the PTSS will draw up bilateral non-disclosure agreements with each CSP (connection agreements) containing details that are not in the public domain, such as the physical handover points, network addresses, access points, responsibilities, contacts, service levels and detailed diagrams of the DNs as well access arrangements (24/7) to the ISS premises 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. TR TS [4] and the Delivery Network Concept are in the public domain. Confidential information must therefore be drafted separately in documents accessible only to the relevant parties.

2 Abbreviations

3GPP	3rd Generation Partnership Project
ASCII	American National Standard Code for Information Interchange
AS	Autonomous System
BIT	German acronym for FOITT
BRA	Basic Rate Access (ISDN)
BÜPF	Federal Act on Post and Telecommunications Surveillance
CA	Certification Authority
CC	Content of Communication
CS	Circuit-switched
CSP	Communications Service Provider (term covering both ISPs and TSPs)
DN	Delivery Network
DN-HP	Delivery Network - Handover Point
ETSI	European Telecommunications Standards Institute
FOITT	Federal Office of Information Technology, Systems and Telecommunication
HI	Handover interface
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INI	Internal Network Interface
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISS	Interception System Schweiz (new LEMF of the PTSS)
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility (LIS or the new ISS, run centrally by the PTSS)
LI	Lawful Interception
LI-HP	Handover Point at the level of LI formats
LIS	Lawful Interception System (current LEMF system of the PTSS)
LITS	Lawful Interception Test System (current LEMF test system of the PTSS)
MAC	Media Access Control (sub-layer of Layer 2 in the OSI Model)
MD	Mediation Device
NE	Network Equipment
OAR	Organisational and Administrative Requirements
PRA	Primary Rate Access (ISDN)
PS	Packet-switched
PTSS	Post and Telecommunications Surveillance Service
REL	Release Message
RFC	Request for Comments (repository of technical and organisational documents of the IETF)
SLA	Service Level Agreement
TR TS	Technical Requirements for Telecommunication Surveillance
TSP	Telecommunications Service Provider
VPN	Virtual Private Network
VÜPF	Ordinance on Post and Telecommunications Surveillance
WDM	Wavelength-Division Multiplexing

3 Definitions

Content of Communication (CC) [5] section 3.1
ETSI definition: Information exchanged between two or more users of a telecommunication service, excluding Interception Related Information. NOTE: This includes information which may, as part of some telecommunication service, be stored by one user for subsequent retrieval by another.

Handover interface (HI)
Interface between a provider and the LEMF
HI1: for administrative processes (delivery of interception order)
HI2: for delivery of Intercept Related Information (IRI)
HI3: for delivery of Content of Communication (CC).

Intercept Related Information (IRI) [5] section 3.1
ETSI definition: 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.

4 References

[1]	SR 780.1	Federal Act of 6 October 2000 on Post and Telecommunication Surveillance (BÜPF)
[2]	SR 780.11	Ordinance of 31 October 2001 on Post and Telecommunication Surveillance (VÜPF)
[3]	OAR	Guidelines for Lawful Interception of Telecommunication Traffic, Organisational and Administrative Requirements, Version 2.13, 23 November 2011
[4]	TR TS	Technical Requirements for Telecommunication Surveillance, Version 3.0, 23 November 2011
[5]	ETSI TS 101 671	Telecommunication security; Lawful interception (LI); Handover interface for the lawful interception of telecommunication traffic

5 The ISS platform

The ISS production system is designed to be fully redundant, with a primary system and a secondary system at two separate sites. ISS services remain available even if there is a breakdown at one of the sites. It is not visible to the CSPs which system is currently the primary system. The ISS can be accessed by virtual IP addresses distributed at both sites. Therefore, a CSP does not need to implement any manual processes for ISS failover.

In addition to the production system, there is a corresponding integration system, i.e. which also has a primary and secondary system at both sites. There is also a test system and a training system, each of which exists once only.

The details for connecting CSP systems to the ISS systems are set out in bilateral connection agreements, which also contain a connection matrix.

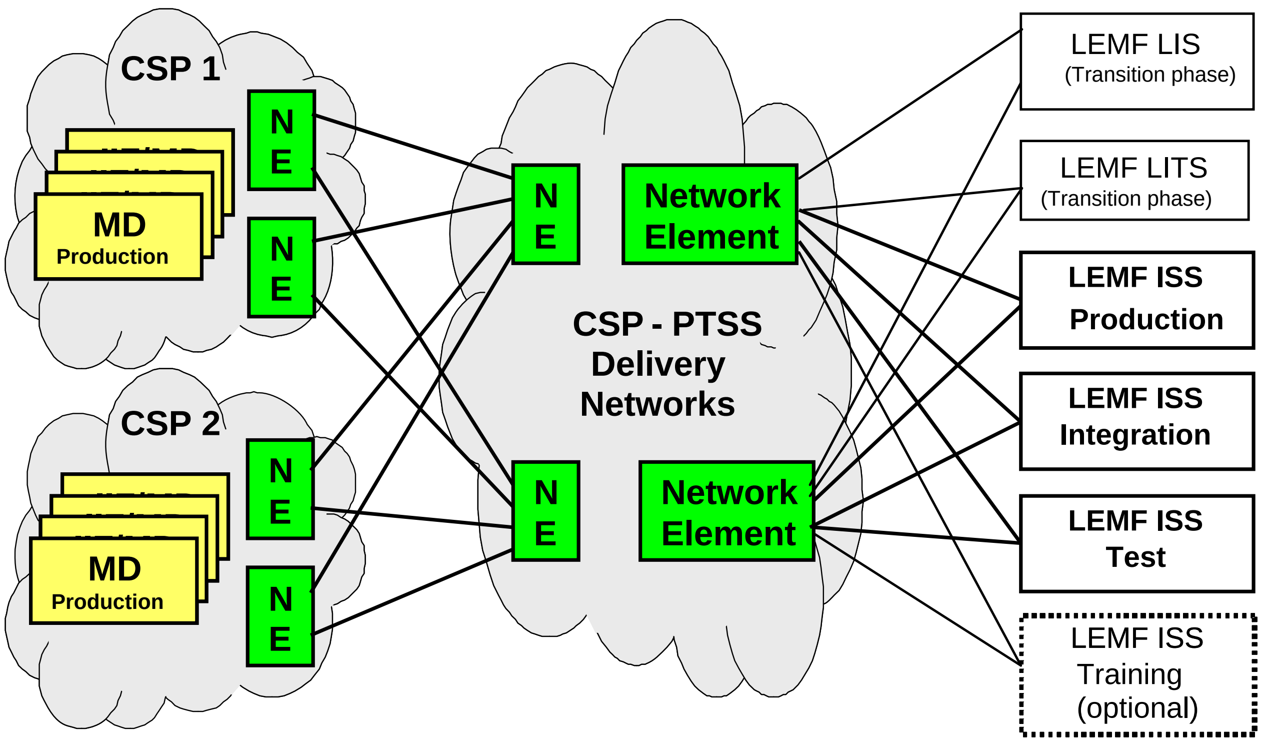


Figure 1 Overview of the LEMF systems ISS and LIS/LITS

6 General requirements of 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 TR TS [4], to ensure the availability of sufficient transmission capacity.
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, if possible, to increase the DN’s reliability (two disjoint paths to both of the ISS sites).
7. Cost-effective installation and operation shall be sought.
8. Low administrative expenses are to 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 TSP, number of intercepts, network architecture of the CSP, data volume per intercept), keeping expenses within an appropriate range.
10. The cost implications for all parties involved shall be taken into consideration.
11. The ISC-FDJP, PTSS and FOITT must adhere to the federal rules on information protection and data security.
12. The DN’s scalability must be ensured (fast and simple expansion of available capacity or bandwidth).
13. The hardware and software must be vendor-neutral.
14. No PTSS equipment shall be on the CSP’s premises (except in the case of intercepts implemented by the PTSS with the CSP’s consent).
15. Responsibilities must 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 DNs must be able to guarantee investment protection.

7 Overview of the delivery networks

7.1 Functional architecture

This document covers the delivery network (no. 4 in Figure 2) between the CSP and the LEMF (ISS) in accordance with the Swiss reference model. The access network (no. 6 in Figure 2) between the LEMF and the LEA is not dealt with here.

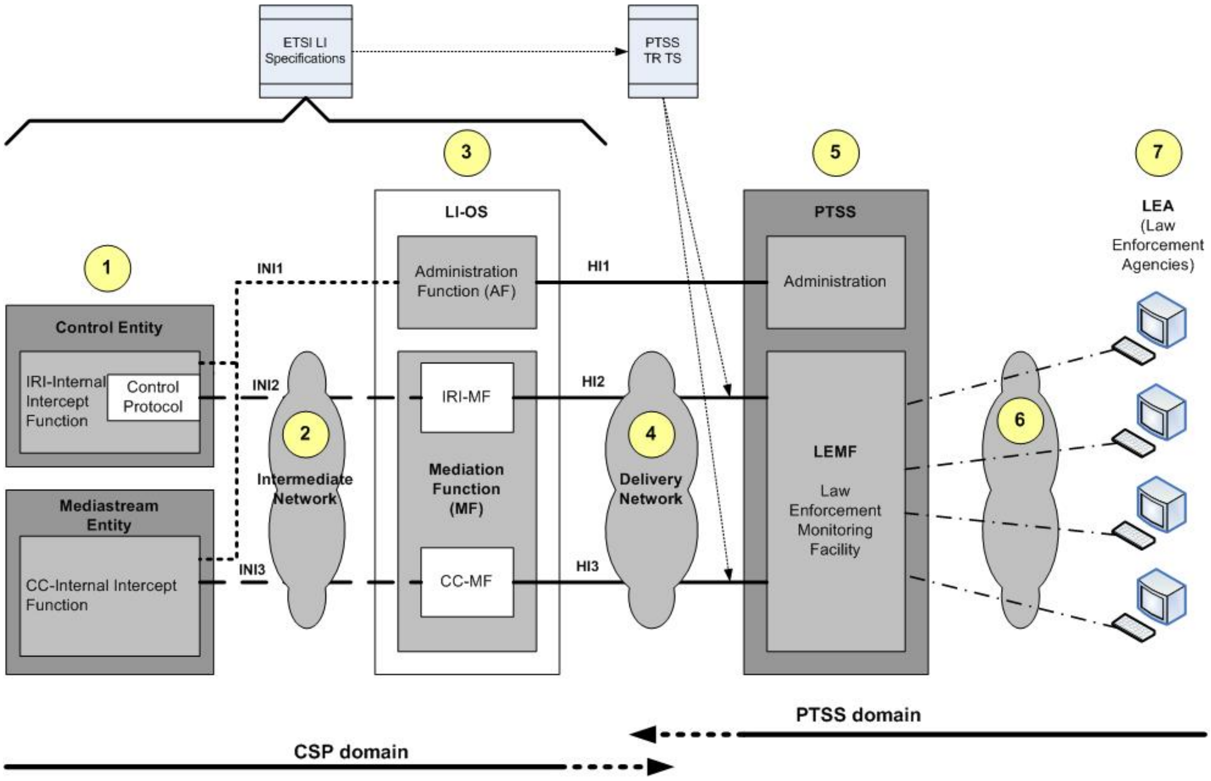


Figure 2 Swiss reference model

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

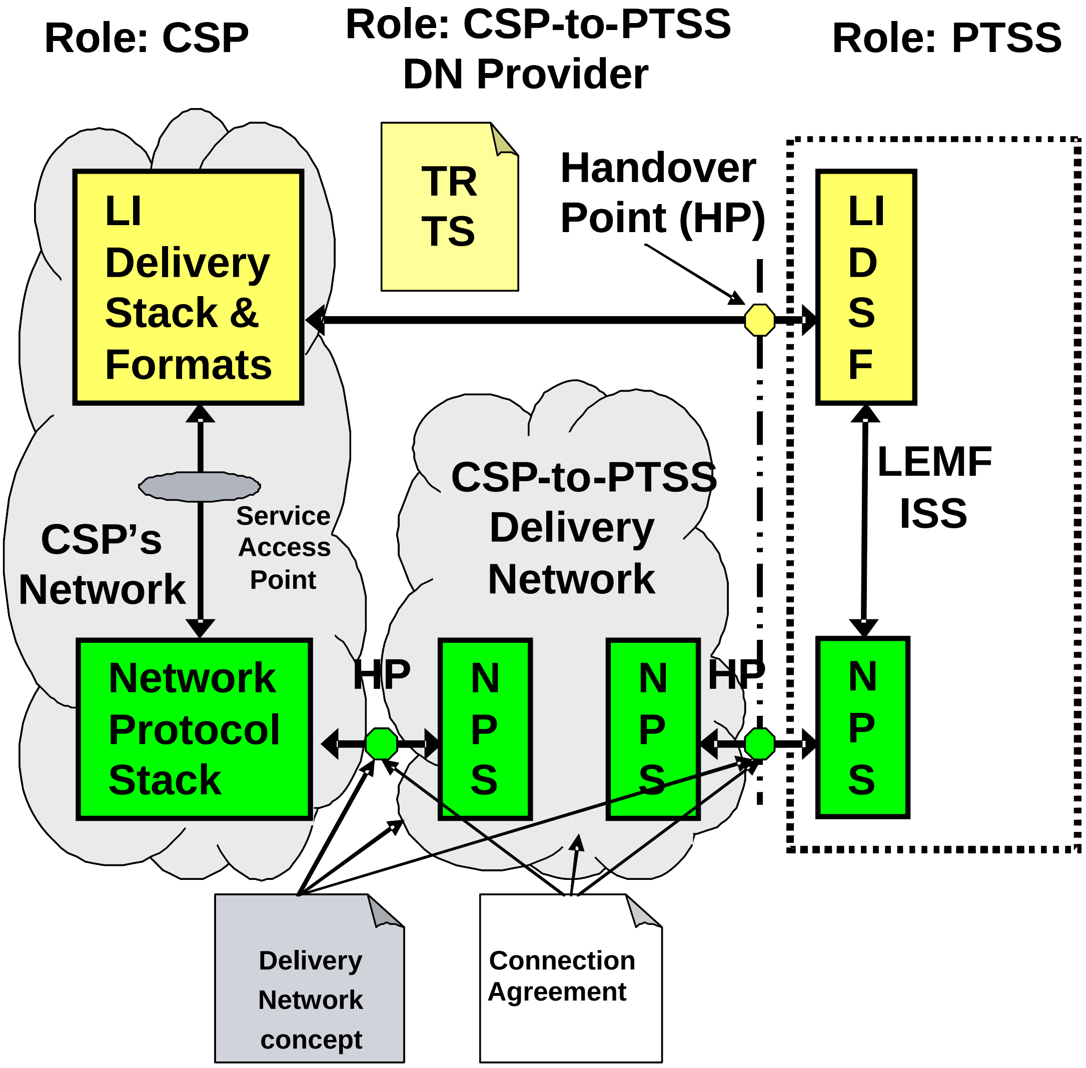


Figure 3 Roles, protocol stacks and handover points between the CSP and the PTSS

Figure 3 shows the *delivery networks* and *lawful interception formats* layers. *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 from the CSP to the PTSS in accordance with the Swiss reference model. For the purposes of this 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, Calling/Called Subaddress field when setting up CC links, 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).

Moreover, individual **connection agreements** are drawn up as bilateral documents between each CSP and the PTSS. Each connection agreement defines the detailed technical interface requirements a CSP must meet in order to be able to connect to the DN, contains 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 specifies 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 individual connection agreement 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 TR TS [4]. These aspects are not described in concepts for delivery networks.

7.2 Overview of roles in the DNs

1. Role of the CSP
2. Role of the ISS (LEMF)
3. Role of the delivery network provider

7.3 Overview of the ISS network interfaces with CSPs

1. ISDN interface for CC of CS interceptions
2. Alternatively: IP interface for CC of CS interceptions (with circuit emulation)
3. IP interface for IRI of CS interceptions
4. IP interface for CC and IRI of PS interceptions
5. Future TCP/IP interfaces for ETSI retained data (HI-A (administrative) and HI-B (results))
6. Swiss proprietary email interface for CC and IRI of email interception in real time and historical data as well as Internet access information in accordance with TR TS [4] – is not part of this concept paper
7. Swiss proprietary email interface for historical data (HD) for CS in accordance with TR TS [4] – is not part of this concept paper
8. Interface for HI1 (Order Management and Administration) – is not part of this concept paper

7.4 Overview of the delivery networks between CSPs and the ISS

1. IP DN: Delivery network for interfaces no. 2, 3, 4, 5 in accordance with the overview under section 7.3
2. ISDN DN: Delivery network for interface no. 1 in accordance with the overview under section 7.3
3. Email service for interfaces no. 6, 7 and 8 in accordance with the overview under section 7.3 – is not part of this concept paper

7.5 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 in 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 one of the buildings.

Note on Figure 4, Figure 5 and Figure 6: These figures give no guidelines for the connection between the ISS primary system and secondary system. From the CSP's point of view, there is only one ISS system. Aspects regarding failover (minimising the impact if the primary system breaks down) and the forwarding of information to the ISS secondary system 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 ISS are in one hand. The ISS 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 the 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).

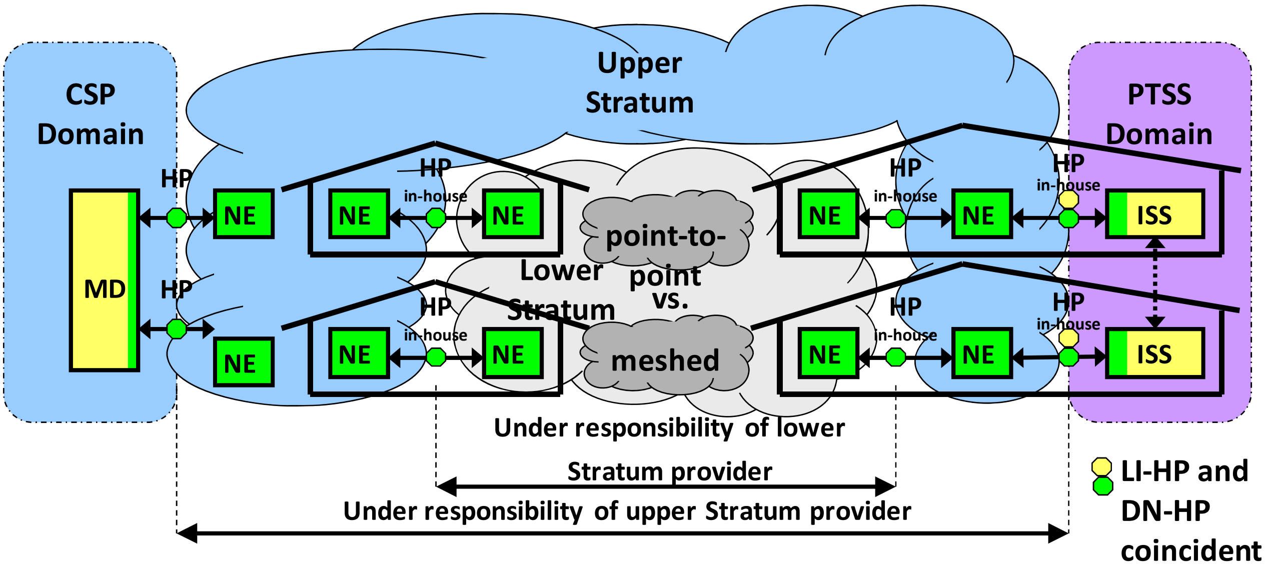


Figure 4 Stratified delivery network

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.

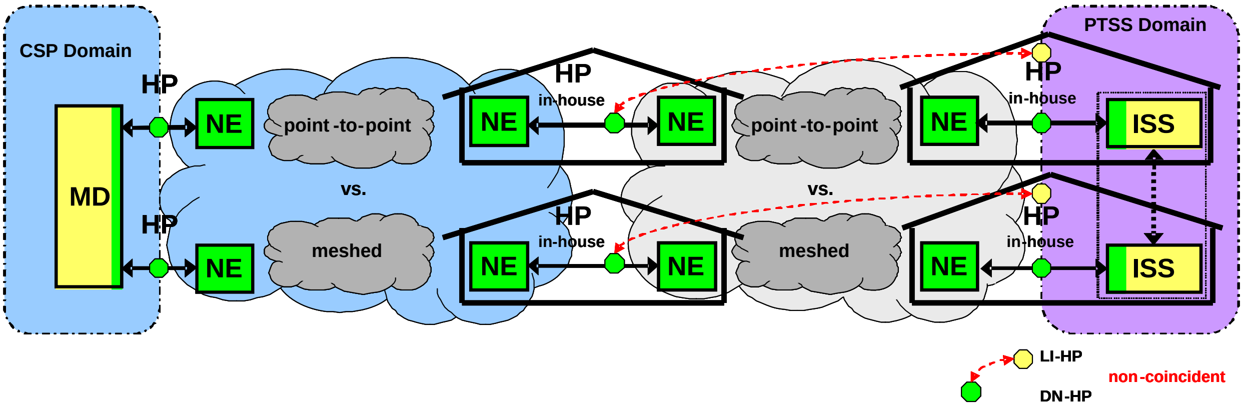


Figure 5 Concatenated delivery network with in-house handover point

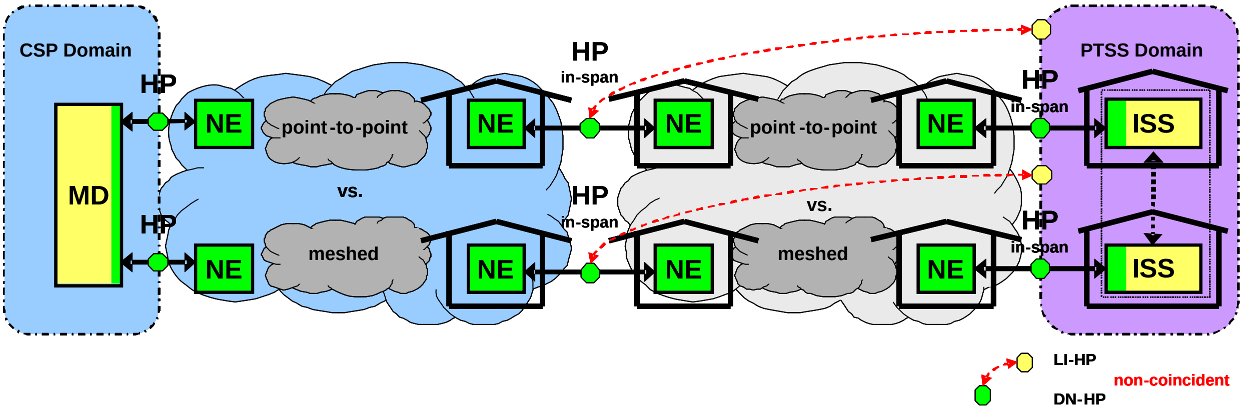


Figure 6 Concatenated delivery network with in-span handover point

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/DN Section Provider, DN Section Provider and the PTSS). If the ISS finds LI information is missing at the LI-HP, it must be determined whether the fault lies with the CSP/DN Section Provider (blue) or the DN Section Provider (grey) (one possible implementation of such a DN is delivery variant A “OpenVPN”).

8 CS delivery networks

For the delivery of CS interception data, two different interfaces are used in accordance with TR TS [4].

1. HI2 handover interface for Intercept-Related Information (IRI). This delivery is via IP DN.
2. HI3 handover interface for Content of Communication (CC) via the CS DN.

8.1 Delivery of CS IRI data (HI2)

The delivery of the CS IRI to the ISS is only possible via one of the IP DNs described in section 9.2. The data volume of the CS IRI is negligible compared with the IP delivery data.

8.2 Delivery of CS content data (CC, HI3) via CS DN

The CS delivery network between the CSP and the ISS comprises only the HI3 interface (CS CC) and is shown in Figure 7. Such a delivery network has been in use since 2003. What is new is the geographical redundancy of the LEMF (ISS). However, the E.164 delivery address is the same for both of the ISS redundant systems. The CSP cannot see which end of the ISS is currently active.

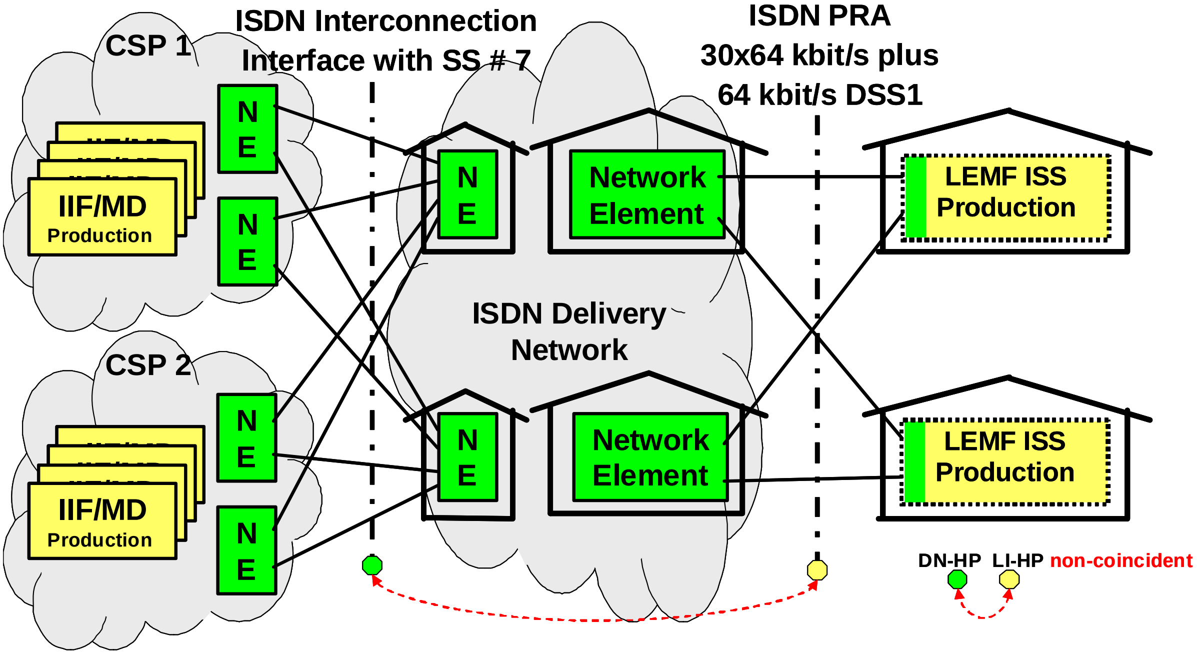


Figure 7 Delivery network for Content of Communication (CC) of circuit-switched services

The content (CC) of CS interceptions is transferred by the CSPs via the usual interconnect interfaces to the universal service licensee. The interconnection documents are on the universal service licensee’s website.

The redundant connection of the ISS to the telephone network of the universal service licensee concerns the PTSS and is set out in an internal document of the PTSS. It is not envisaged that CSPs will build direct PRA terminations to the ISS (with the exception of the universal service licensee).

The PRAs at both ISS sites and systems (production and integration) are connected to two geographically separate exchanges. Together with other redundancy measures, these guarantee a very high level of availability.

The delivery network itself does not take any recovery action in the event of a faulty set-up of CC links or if released by the delivery network or LEMF. Such action is initiated by the MF with the CSP.

If a CSP does not have an interconnect interface to the universal service licensee, this case must be handled separately.

Figure 8 shows the handover points and areas of responsibility in the ISDN delivery network for delivery of Content of Communication from circuit-switched services (CS-CC). This delivery network corresponds to the basic topology of a “concatenated delivery network” as per Figure 5 and Figure 6.

The handover point between the CSP and the PTSS for LI formats, i.e. the content of the calling und called party subaddress in setting up CC links (LI-HP) and the CSP's handover point for transportation (DN-HP) are not coincident. A triangular relationship thus exists between the LI-HP and two DN-HPs (between the CSP and the ISDN-DN Provider and between the ISDN-DN Provider and the PTSS).

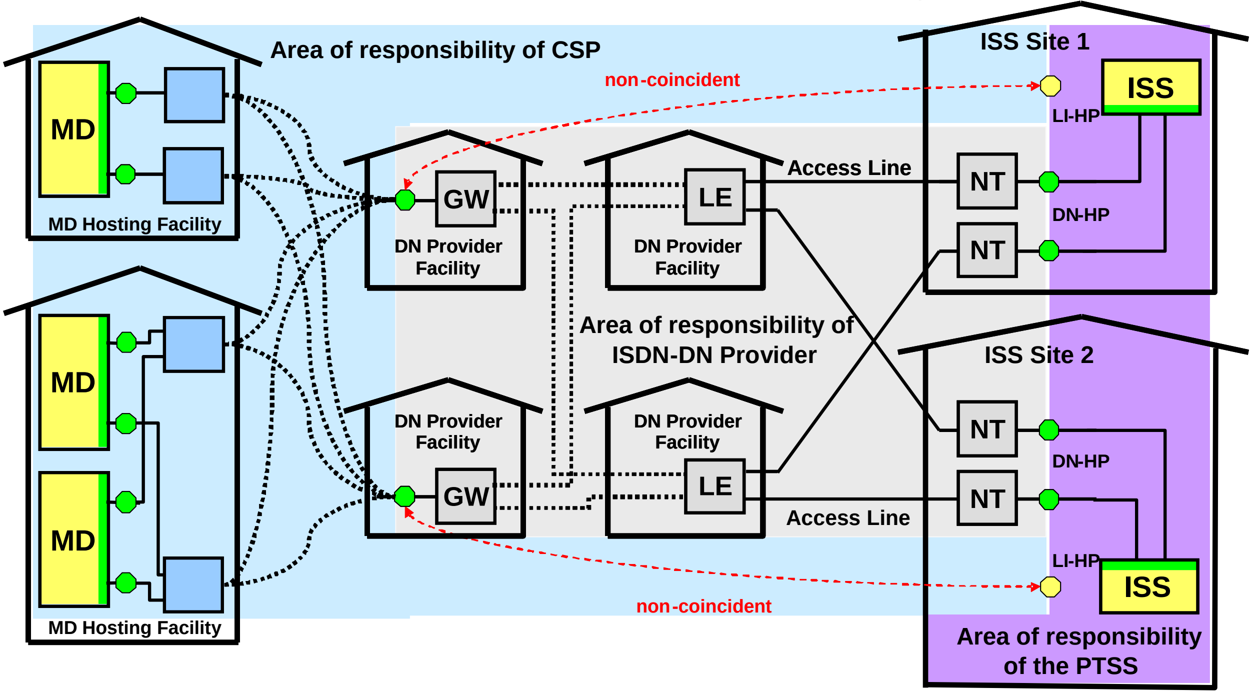


Figure 8 Handover points and areas of responsibility in the ISDN delivery network

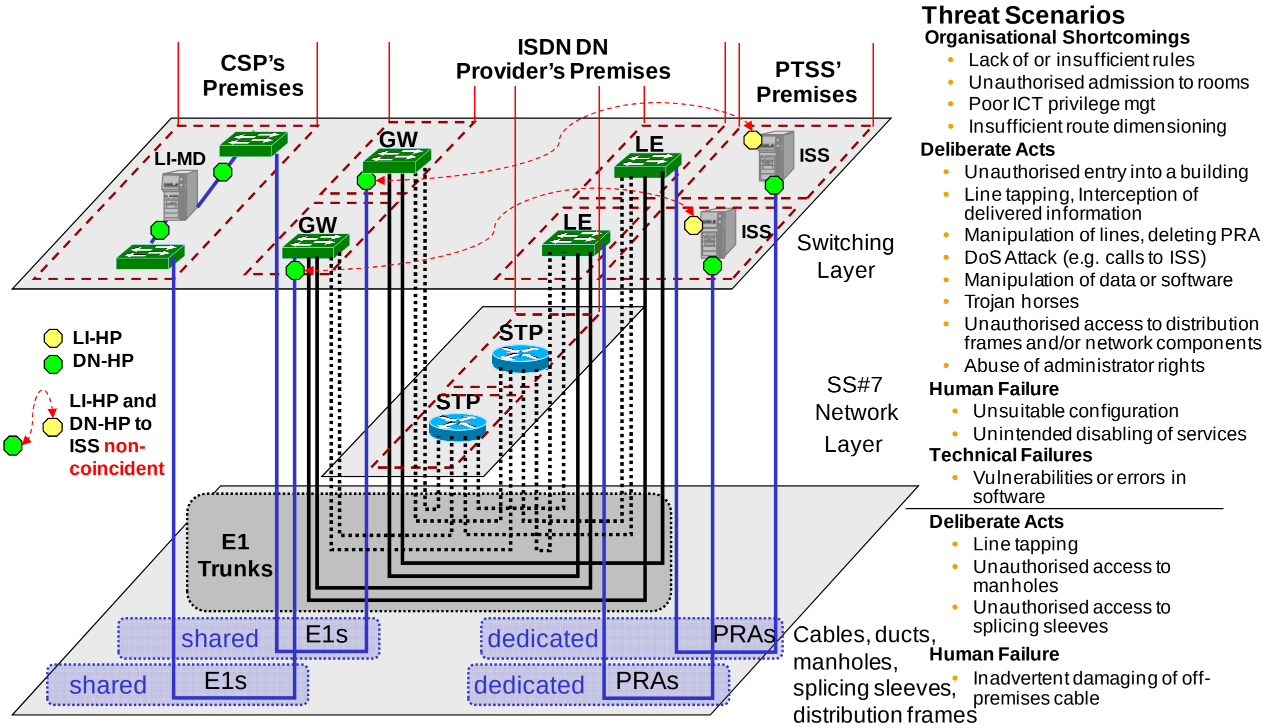
Note: Figure 8 contains no guidelines on the internal connections in the area of responsibility of the PTSS, e.g. concerning overflow traffic between the two ISS sites.

8.2.1 Security aspects of the CS DN

Based on this threat analysis of the CS DN, the individual connection agreements define specific protective measures for the following points:

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

Figure 9 shows the three functional layers "Cable channels/cabling", "SS7 Network" and "Network layer". At the interface between the CSP and the ISDN Delivery Network Provider (generally several E1), the "Circuit Switched Content of Communication" (CS-CC) traffic delivered is mixed with other interconnect traffic. In the network of the ISDN Delivery Network Provider, the payload traffic and signalling traffic are separated and the CS-CC traffic delivered is also mixed with other traffic. In the Primary Rate Accesses (PRA) to the ISS, only the CS-CC traffic delivered is conveyed. CS-CC does not contain any identifiers allowing for identification of the target using a telephone directory; only in the Calling Party Subaddress when setting up a CC link is there the parameter "Lawful Interception Identifier" (LIID) which has a concealed link to the target as its "order number". This relationship is treated as confidential between the CSP and the PTSS. Identification of the target would thus only be possible by way of voice recognition of the CS-CC delivered.



Threat Scenarios

Organisational Shortcomings

- Lack of or insufficient rules
- Unauthorised admission to rooms
- Poor ICT privilege mgt
- Insufficient route dimensioning

Deliberate Acts

- Unauthorised entry into a building
- Line tapping, Interception of delivered information
- Manipulation of lines, deleting PRA
- DoS Attack (e.g. calls to ISS)
- Manipulation of data or software
- Trojan horses
- Unauthorised access to distribution frames and/or network components
- Abuse of administrator rights

Human Failure

- Unsuitable configuration
- Unintended disabling of services

Technical Failures

- Vulnerabilities or errors in software

Deliberate Acts

- Line tapping
- Unauthorised access to manholes
- Unauthorised access to splicing sleeves

Human Failure

- Inadvertent damaging of off-premises cable

Figure 9 Threats in the CS delivery network

8.2.2 Capacity requirements for the CS DN

Three parameters influence the capacity of the CS DN:

i) Number of real-time CS interceptions
ii) Number of CC links required per target session
iii) Activity of the target

The formula for calculating the value of i) is defined in TR TS [4], section 9.1. The value of ii) is generally two CC links in the case of CS (forward and reverse channel of the target). The value of iii) is an indication of activity, based on the CSP's measurements or statistics. The CSPs themselves ensure that there is sufficient delivery capacity available at their DN-HP to the CS DN.

The PTSS is responsible for ensuring that there is sufficient delivery capacity available at the DN-HP from the CS DN to the LEMF (ISS) for all CSP deliveries. As the CS DN is a "virtual" network within the universal service licensee's ISDN and the LI traffic, including interconnect traffic, is a small part of the overall volume, the bottleneck lies at the DN-HP end from the CS DN to the LEMF, i.e. the number of ISDN-PRAs to the ISS. It is up to the PTSS to determine this number of ISDN-PRAs, as the PTSS is the only organisational unit with an overview of the values of each CSP, taking account of the trunking gain (common ISDN-PRAs vs. dedicated ISDN-PRAs per CSP). Scalability is ensured by adapting the number of ISDN-PRAs to the ISS.

9 IP delivery networks

9.1 Capacity (bandwidth) of the IP DN

TR TS [4] forms the basis for the dimensioning of DNs. The bandwidth of a DN must be large enough to deliver the interception data including overheads on time and without any information loss resulting from traffic overload in the DN.

9.2 Variants of IP delivery networks

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

There are currently two variants of the IP DN:

A) OpenVPN
B) Direct connection of a CSP to the ISC-FDJP

Depending on future requirements, further IP DN variants may be planned and implemented in agreement between the CSP and the PTSS.

9.2.1 IP DN Variant A: OpenVPN

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

The CSP sets up one or more individual VPN tunnels with the ISS. The PTSS is the single point of contact (SPOC) for the CSP. Chapter 13 of this document defines the individual responsibilities for error handling.

The CSP acquires its VPN clients at its own discretion in accordance with the TR TS [4].

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 (SLA) with its peering partner or upstream provider.

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

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 must provide as much redundancy as possible.

The CSP is responsible for its Internet accesses and for correct operation of the VPN client. The VPN tunnel is the joint responsibility of the CSP and the PTSS. The PTSS is responsible for correct operation of the VPN server. Problems are dealt with in accordance with the error handling process.

9.2.1.1 VPN tunnel CSP - ISS

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

9.2.1.2 Overview

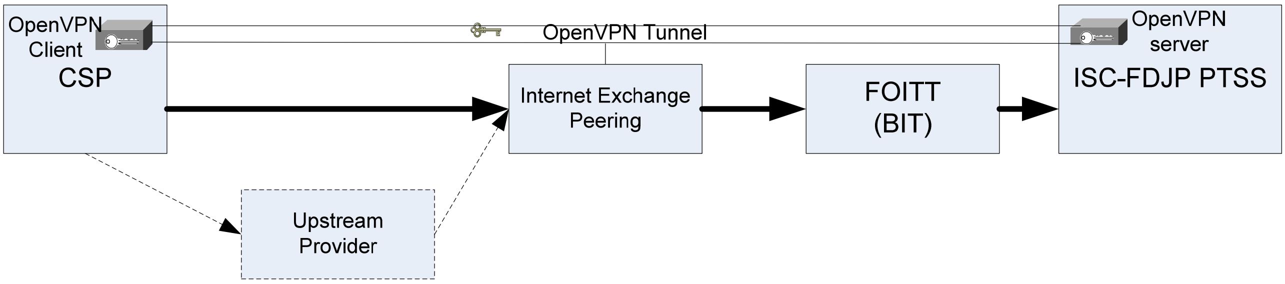
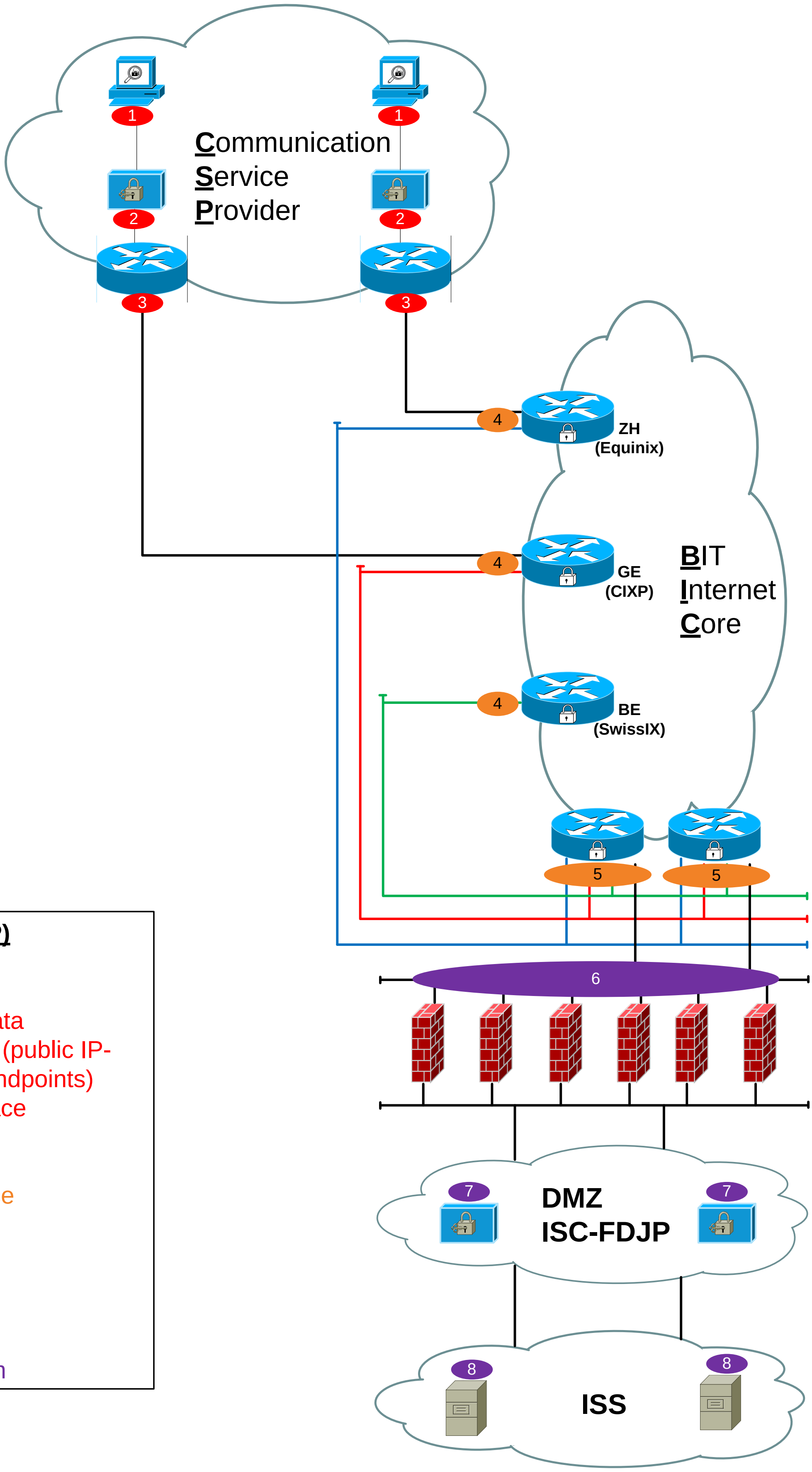


Figure 10 Schematic layout of IP DN Variant A: OpenVPN



Handover Points (HP)

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

BIT (FOITT):
4) BIT peering interface
5) BIT-ISC interface

ISC-FDJP / PTSS:
6) ISC-BIT interface
7) ISC VPN endpoint
8) ISC ISS end system

Figure 11 Handover points of IP DN Variant A: OpenVPN

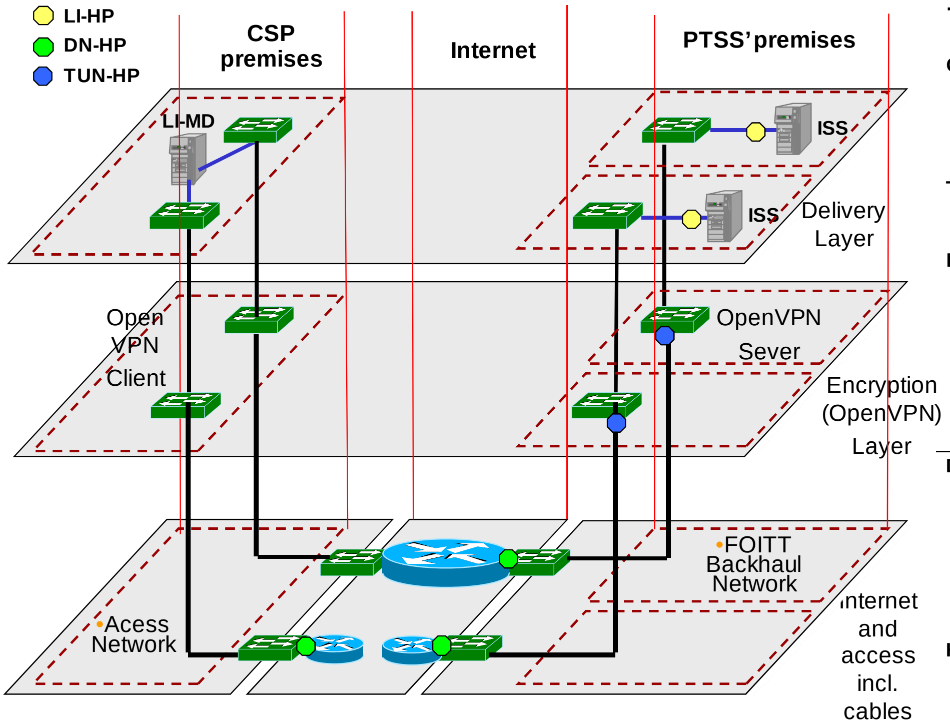
Regarding the physical handover points 3 and 4 in Figure 11, there are basically two configurations from the CSP’s point of view:

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)

9.2.1.3 Threat analysis for IP DN Variant A: OpenVPN

Based on this threat analysis of the OpenVPN DN, the individual connection agreements define specific protective measures for the following points:

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



Threat Scenarios

Organisational Shortcomings
- Lack of or insufficient rules
- Unauthorised admission to rooms
- Poor ICT privilege management

Technical Failures
- Vulnerabilities or errors in software

Deliberate Acts
- Unauthorised entry into a building
- Line tapping in-house
- Attack in-house
- Manipulation of data or software
- Trojan horses
- Unauthorised access to distribution frames

Deliberate Acts
- DoS Attack
- IP address spoofing
- Line tapping cable network
- Unauthorised access to manholes
- Unauthorised access to splicing sleeves

Human Failure (cable)
- Inadvertent damaging of off-premises cable

Figure 12 Threat analysis for OpenVPN

9.2.1.4 Scalability of IP DN Variant A: OpenVPN

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

As at January 2012, the following scalability is possible: The FOITT peering interface can be expanded up to a maximum of 300 Mbps. The maximum bandwidths for the FOITT transport network (backhauling) and the FOITT-FDJP interface can be increased to 1 Gbps. However, on account of the redundancy, only a maximum of 300 Mbps is available per CSP.

The throughput within an OpenVPN tunnel is also limited and, according to tests by the PTSS, is at least 100 Mbps. This capacity can be increased by using more powerful processors (vertical scaling). Also, additional OpenVPN tunnels may be added (horizontal scaling).

9.2.2 IP DN Variant B: Direct connection of a CSP to the ISC-FDJP

The CSP's handover point (DN-HP) resides on the premises of the ISS, near the ISS system. The ISC-FDJP 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 data delivery up to the handover points (DN-HP) on the premises of the ISC-FDJP.

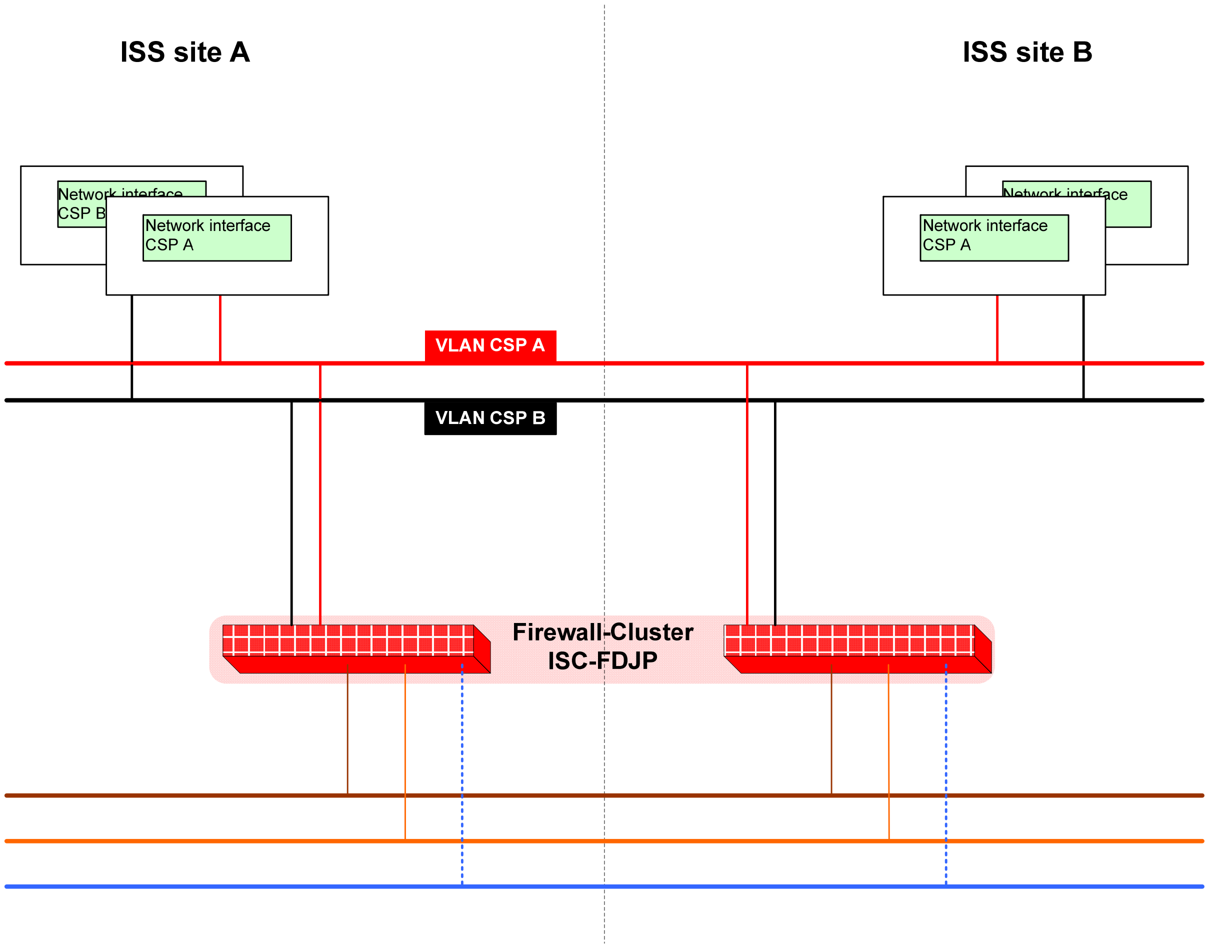


Figure 13 Schematic layout of IP DN Variant B: Direct connection of a CSP to the ISC-FDJP

The DN-HP between the CSP and the ISS 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 ISS sites:

- 1000BASE-SX or 1000BASE-T
- Connector: Electrical RJ-45 or optical LC
- No Spanning Tree Protocol (STP)
- Untagged

The interfaces at both ISS sites are connected at Ethernet level. Special attention must be given to avoiding loops at the CSP end.

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

ASR:	Aggregation Service Router
CO:	Central Office
CSP:	Communication Service Provider
DF:	Distribution Function
ISS:	Interception System Schweiz
LEMF:	Law Enforcement Monitoring Function
ODF:	Optical Distribution Frame
OF:	Optical Fibre
ONT-SR:	Optical Network Terminal – Service Router
MF:	Mediation Function
WAN:	Wide Area Network

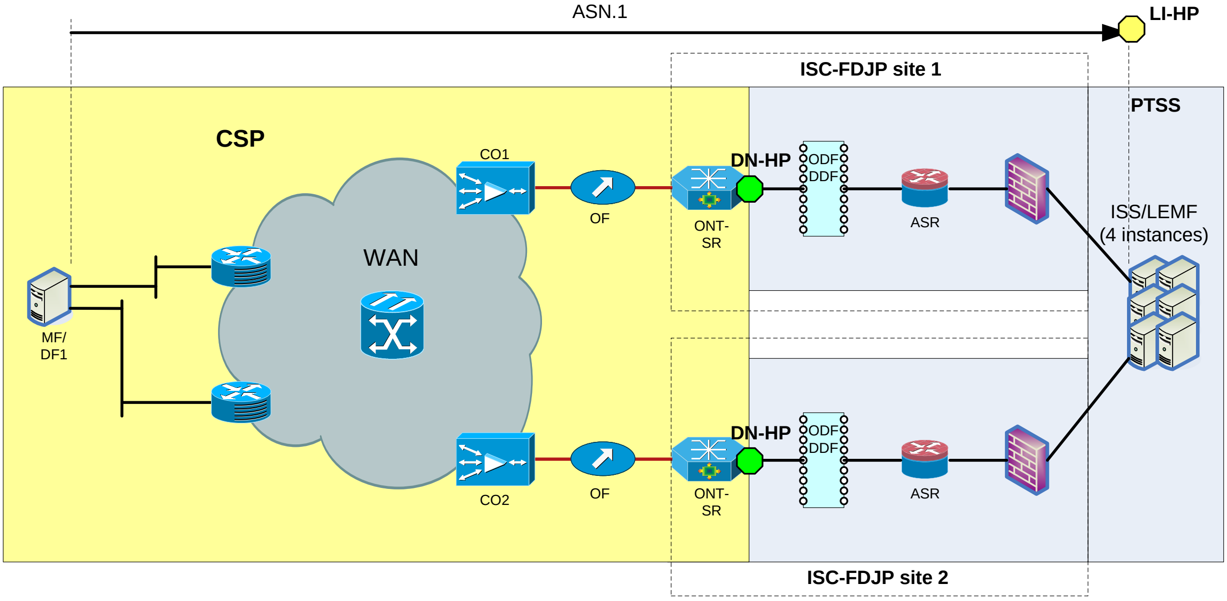


Figure 14 IP DN Variant B: Direct connection of a CSP to the ISC-FDJP

9.2.2.1 Threat analysis of IP DN Variant B: Direct connection of a CSP to the ISC-FDJP

Based on this threat analysis of the IP DN, the individual connection agreements define specific protective measures for the following points:

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

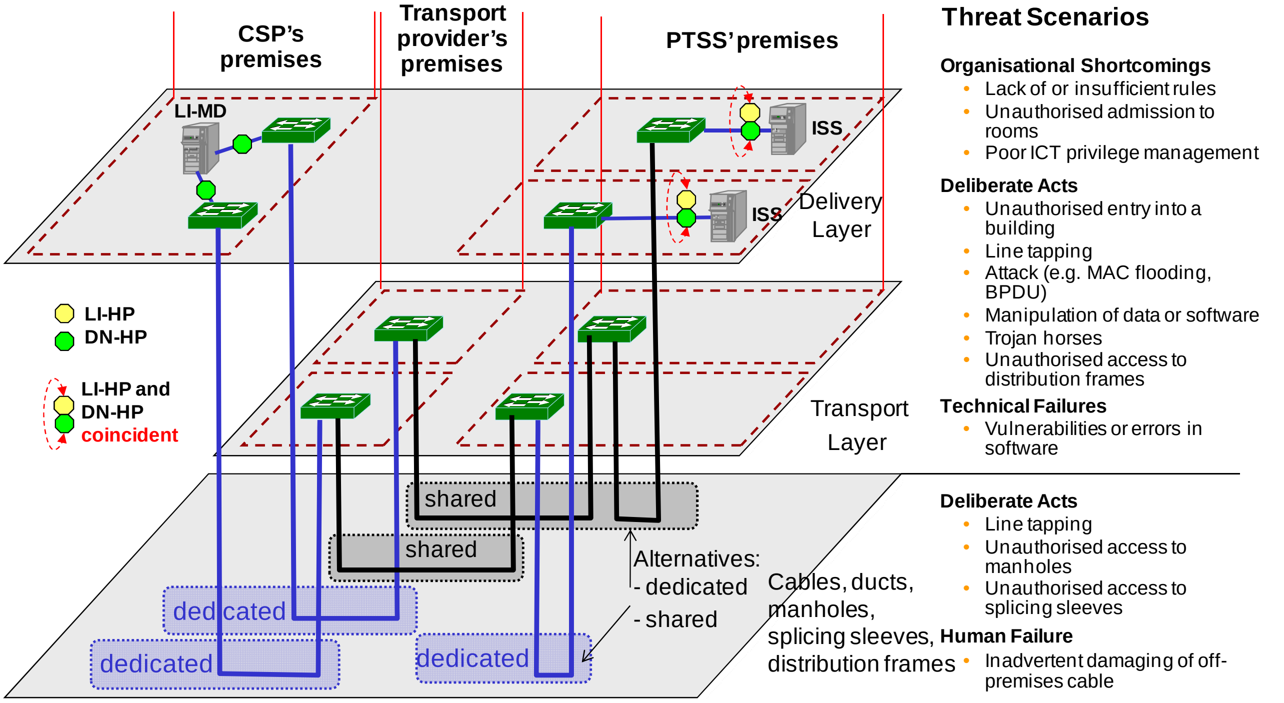

CSP's premises
Transport provider's premises
PTSS' premises
Threat Scenarios
Organisational Shortcomings
Lack of or insufficient rules
Unauthorised admission to rooms
Poor ICT privilege management
Deliberate Acts
Unauthorised entry into a building
Line tapping
Attack (e.g. MAC flooding, BPDU)
Manipulation of data or software
Trojan horses
Unauthorised access to distribution frames
Technical Failures
Vulnerabilities or errors in software
Deliberate Acts
Line tapping
Unauthorised access to manholes
Unauthorised access to splicing sleeves
Human Failure
Inadvertent damaging of off-premises cable
LI-MD
ISS
ISS
Delivery Layer
Transport Layer
LI-HP
DN-HP
LI-HP and DN-HP coincident
shared
shared
dedicated
dedicated
dedicated
Alternatives:
- dedicated
- shared
Cables, ducts, manholes, splicing sleeves, distribution frames

Figure 15 Threat scenarios for IP DN Variant B (direct connection)

9.2.2.2 Scalability of IP DN Variant B: Direct connection of a CSP to the ISC-FDJP

The scalability of delivery in this variant is restricted by the technology and interfaces used. Currently (as at January 2012), the interfaces to the ISC-FDJP are designed for 1 Gbps.

9.2.3 Sub-variant B1: Shared fibre infrastructure

The provider of the shared fibre infrastructure offers other CSPs the possibility of sharing the available fibre optics between two co-locations of the provider and both co-locations of the ISC-FDJP in the form of a Platinum Carrier Optical Service or Platinum Lambda Carrier Optical Service. With the second product, a CSP can lease one or more wavelengths. The DN-HPs are described in Figure 16.

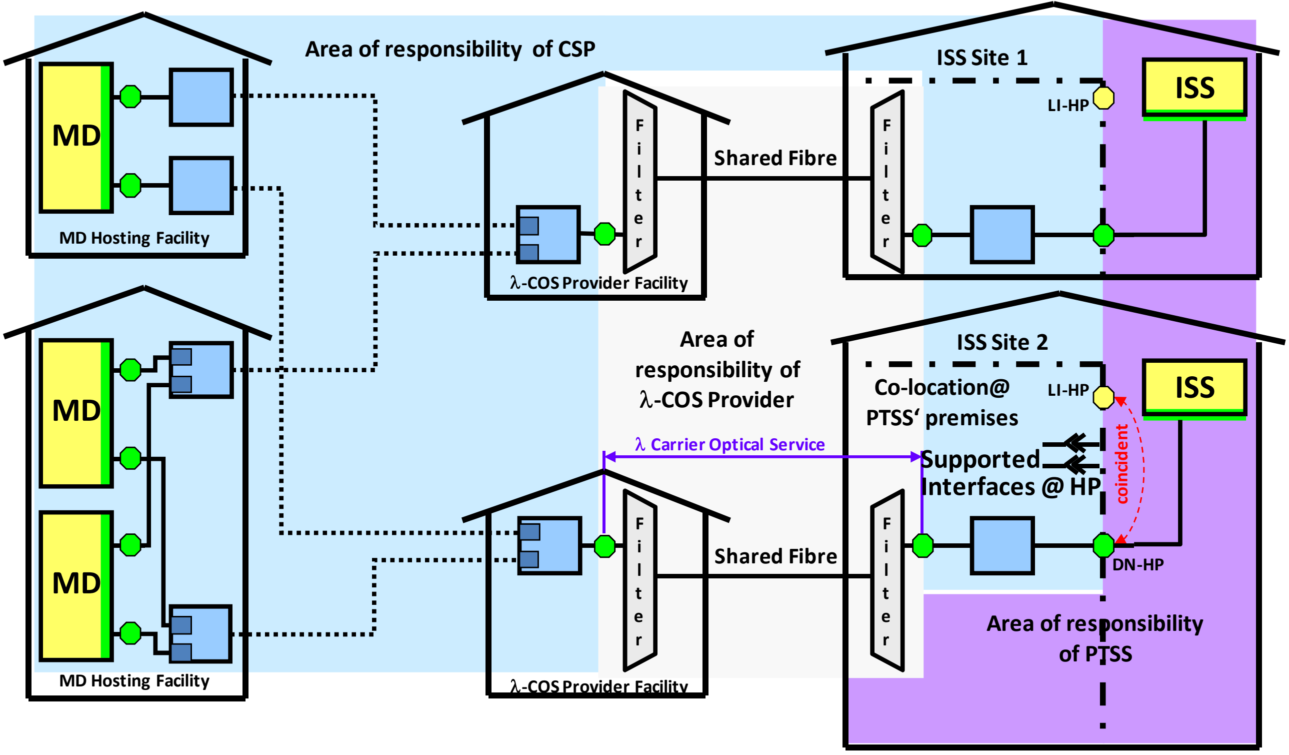


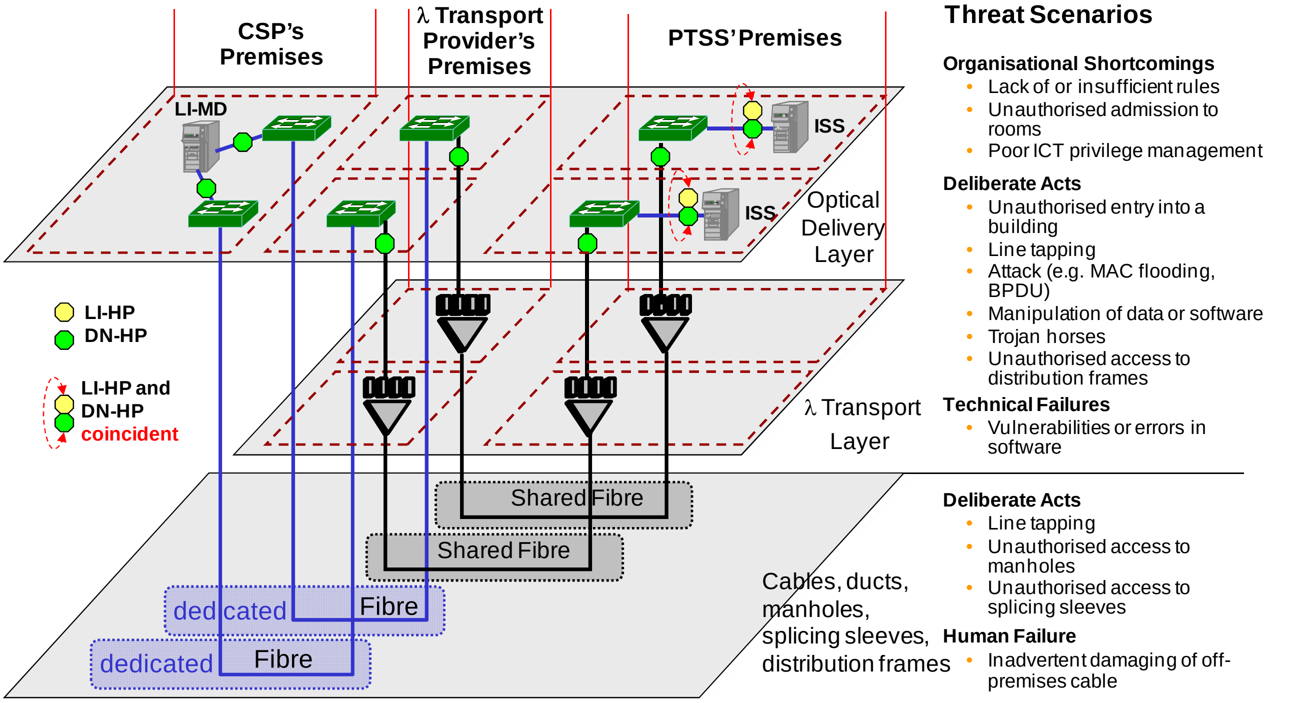
Figure 16 Lambda-COS

9.2.3.1 Threat analysis of IP DN sub-variant B1: Shared fibre infrastructure

Based on this threat analysis of the IP DN, the individual connection agreements define specific protective measures for the following points:

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

Figure 17 shows the three functional layers “Cable channels/cabling”, “Passive λ transport” and “Optical signal”. The basic concept assumes that no service higher than level 1 is implemented between the CSP network and the λ transport provider network. If this is not the case, the functional layers in the bilateral delivery agreement should be amended as appropriate. Higher protocol layers are separated in the upper stratum under the control of a single CSP.



Threat Scenarios

Organisational Shortcomings
- Lack of or insufficient rules
- Unauthorised admission to rooms
- Poor ICT privilege management

Deliberate Acts
- Unauthorised entry into a building
- Line tapping
- Attack (e.g. MAC flooding, BPDU)
- Manipulation of data or software
- Trojan horses
- Unauthorised access to distribution frames

Technical Failures
- Vulnerabilities or errors in software

Deliberate Acts
- Line tapping
- Unauthorised access to manholes
- Unauthorised access to splicing sleeves

Human Failure
- Inadvertent damaging of off-premises cable

Figure 17 Threats in the delivery network shared fibre infrastructure

9.2.3.2 Scalability of IP DN sub-variant B1: Shared fibre infrastructure

The filters are designed for connecting up to 8 wavelengths. This permits implementation of an IP delivery network for up to 8 CSPs with separate deliveries (1 wavelength per CSP). If a CSP uses more than one wavelength, this lowers accordingly the total number of CSPs possible. Up to 10 Gbps can be transmitted per wavelength. The bitrate can be selected per CSP and is determined by the optical equipment installed by each CSP and their interfaces. Currently (as at January 2012), the interfaces to the ISC-FDJP are designed for 1 Gbps.

10 Security

10.1 Scope

This Delivery Network Concept paper defines the technical parameters for delivery of the data within the context of the TR TS [4]. The security requirements and aspects of the transmitting (CSP systems) and receiving applications and systems (ISS) are not dealt with here.

The BÜPF [1] and the VÜPF [2] form the legislative framework and authorisation for the processing of personal data of a sensitive nature. As this is precisely the sort of data transmitted here, this transmission must be secured. In particular, the existence of the lawful interception order and all information related to it are subject to post and telecommunications secrecy with regard to third parties (Art. 12 (3) BÜPF [1]).

Specific security-related aspects of the individual delivery variants are dealt with in the relevant paragraph of chapter 8 or section 9.2, whereby the following protection objectives must be met:

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

Note: Protection from the effects of fire, water, natural hazards and other such disasters does not fall under the protection objectives outlined here.

10.2 Reliability and availability

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

10.3 Monitoring

Monitoring is briefly described below.

Monitoring has two areas of use:

1) Monitoring to support the error handling processes: With reference to one handover point, input data is generated for the error handling process for the purpose of triage in the case of an error.
2) Monitoring for the purpose of lawful interception of a section with a threshold value for an error rate (e.g. CRC check)

The monitoring considered in this concept is used throughout, beyond the handover points. Monitoring that is restricted to internal areas is not dealt with here.

Different monitoring procedures are used, depending on the delivery variant. These procedures are described in a separate monitoring concept paper. The specific details for monitoring are set out in the CSPs’ individual connection agreements. The CSPs ensure availability of delivery up to the DN-HP (direct connection) or up to point 3 in Figure 11 (for OpenVPN) in accordance with section 10.2 and monitor this accordingly.

The monitoring concept paper describes, among other things, monitoring that refers to the handover points between the CSP and the ISDN Delivery Network (interconnect interface), or between the ISDN delivery network and the ISS (PRA with DSS1), i.e. monitoring with reference to a handover point for triage in the case of an error. These can then be used to perform a triage by analysing signalling sequences (see Delivery Network Concept Annex A, Tables with cause values). Implementation is not defined in the monitoring concept paper. It is assumed that both ends of a handover point must recognise the monitoring specifications and, in particular, its judgements.

The following obligation applies for the PTSS/ISC-FDJP and for the CSP:

- In the event of an error, the available and relevant logfiles or traces must be mutually disclosed and test results backed up with facts.
- As the quality of error messages influences the repair time, all relevant information must be shared with the other party.

Monitoring must provide the necessary inputs for the error handling processes. There is a certain degree of flexibility in implementing the monitoring specifications, in that it can be highly automated or implemented manually by personnel with measuring devices.

Note: Monitoring should not be restricted to the delivery network area but should also be available for LI applications.

10.4 Redundancy

PTSS end

The ISS is geographically distributed over two sites. Failover of the ISS is not visible to the CSP. If a connection breaks down, the PTSS is responsible for switching from one end to the other. The failover mechanism and internal routing are controlled by the ISS.

Note: For the CS CC, an interruption to the CC link and the associated data loss are unavoidable for the duration of the failover.

CSP end

A CSP must ensure there 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.

11 Quality of service with OpenVPN

Resource reservation control mechanisms do not apply when using the Internet. This means that delivery of data via the Internet is on a “best effort” basis only and is not guaranteed, i.e. with effects on the latency and IP packet loss.

Data loss as a result of capacity bottlenecks is avoided by the CSPs by providing sufficient bandwidths at the Internet accesses.

12 Restrictions for the direct connection variant

The direct connection of a CSP to the ISC-FDJP is subject to certain restrictions in terms of available space and power supply in the ISC-FDJP co-location. With the eight wavelengths currently available, a maximum of eight CSPs can use the shared fibre infrastructure variant (one wavelength per CSP). Two rack units and 0.5 kVA in power is available in the co-location as standard for each CSP. If a CSP has greater requirements, this must be arranged on a case-by-case basis.

13 Error handling process for the OpenVPN variant

The actions in the following process (Figure 18) should be carried by the CSP, unless otherwise stated. The handover points numbered in Figure 18 (as Handoverpoint or HP) refer to Figure 11 “Handover points of IP DN Variant A: OpenVPN”.

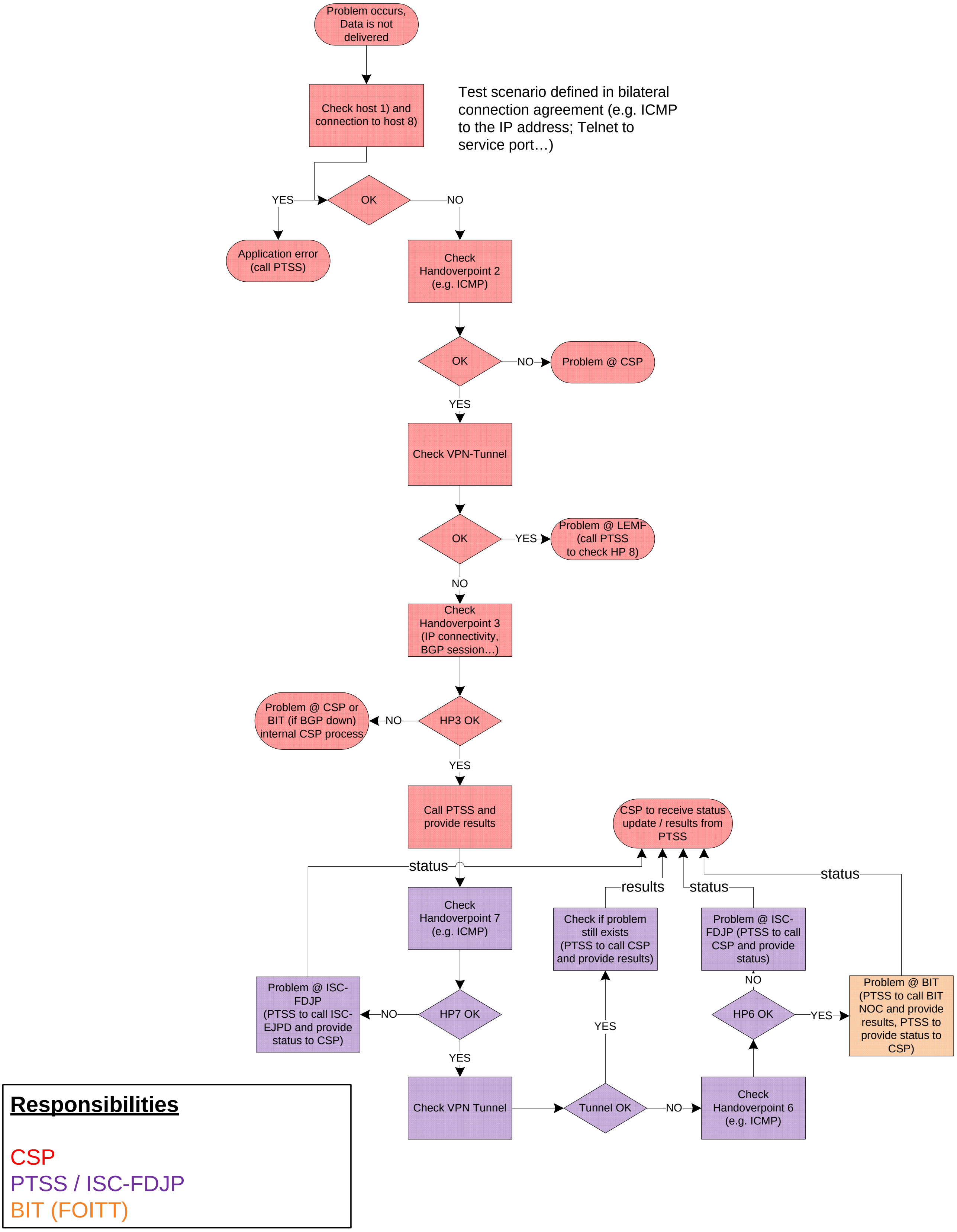
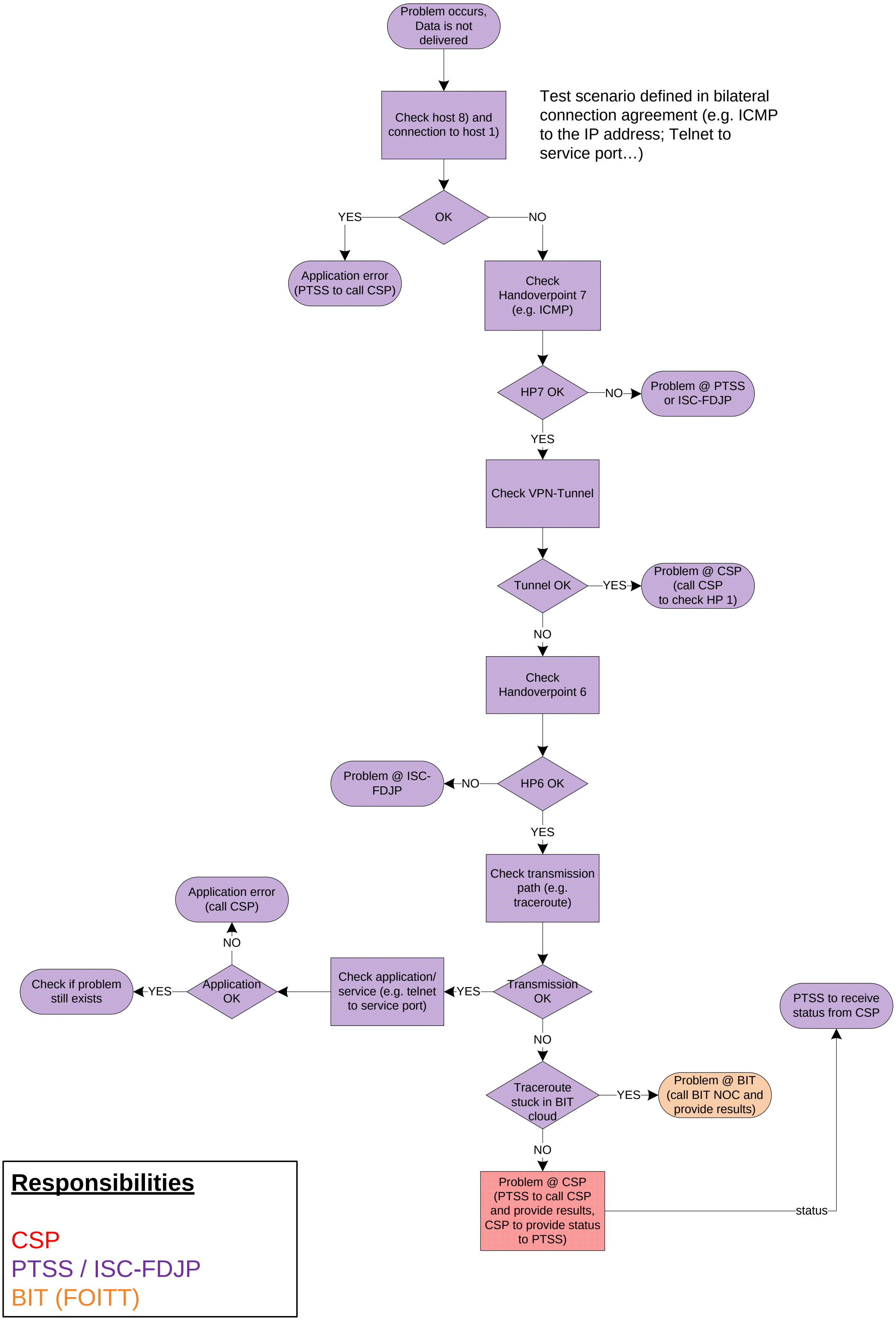

Problem occurs, Data is not delivered
Check host 1) and connection to host 8)
Test scenario defined in bilateral connection agreement (e.g. ICMP to the IP address; Telnet to service port…)
OK
YES
NO
Application error (call PTSS)
Check Handoverpoint 2 (e.g. ICMP)
OK
NO
Problem @ CSP
YES
Check VPN-Tunnel
OK
YES
Problem @ LEMF (call PTSS to check HP 8)
NO
Check Handoverpoint 3 (IP connectivity, BGP session…)
Problem @ CSP or BIT (if BGP down) internal CSP process
NO
HP3 OK
YES
Call PTSS and provide results
CSP to receive status update / results from PTSS
status
results
status
status
Check Handoverpoint 7 (e.g. ICMP)
Check if problem still exists (PTSS to call CSP and provide results)
Problem @ ISC-FDJP (PTSS to call CSP and provide status)
NO
Problem @ BIT (PTSS to call BIT NOC and provide results, PTSS to provide status to CSP)
Problem @ ISC-FDJP (PTSS to call ISC-EJPD and provide status to CSP)
NO
HP7 OK
YES
HP6 OK
YES
YES
Check VPN Tunnel
Tunnel OK
NO
Check Handoverpoint 6 (e.g. ICMP)
Responsibilities
CSP
PTSS / ISC-FDJP
BIT (FOITT)

Figure 18 Error handling process “CSP detects error” for the OpenVPN variant


Problem occurs, Data is not delivered
Check host 8) and connection to host 1)
OK
YES
NO
Application error (PTSS to call CSP)
Check Handoverpoint 7 (e.g. ICMP)
HP7 OK
NO
Problem @ PTSS or ISC-FDJP
YES
Check VPN-Tunnel
Tunnel OK
YES
Problem @ CSP (call CSP to check HP 1)
NO
Check Handoverpoint 6
Problem @ ISC-FDJP
NO
HP6 OK
YES
Check transmission path (e.g. traceroute)
Application error (call CSP)
NO
Check if problem still exists
YES
Application OK
Check application/ service (e.g. telnet to service port)
YES
Transmission OK
PTSS to receive status from CSP
NO
Traceroute stuck in BIT cloud
YES
Problem @ BIT (call BIT NOC and provide results)
NO
Problem @ CSP (PTSS to call CSP and provide results, CSP to provide status to PTSS)
status
Responsibilities
CSP
PTSS / ISC-FDJP
BIT (FOITT)

Test scenario defined in bilateral connection agreement (e.g. ICMP to the IP address; Telnet to service port…)

Figure 19 Error handling process “PTSS detects error” for the OpenVPN variant

14 Error handling process for the direct connection variant

The process in the case of an error is run directly between the CSP and the PTSS.

Situation 1:

The **PTSS** detects a disturbance in the data flow (see Figure 20).

Procedure:

1. The PTSS checks whether there is an interruption at layer 1 (loss of signal).
2. If so, the PTSS informs the CSP's contact of this, mentioning the time, link name and error type = Layer 1 down
3. If not, the PTSS pings to check whether layer 3 is interrupted.
4. If the ping is not OK, the PTSS informs the CSP's contact of this, mentioning the time, link name and error type = Layer 3 down, as well as the IP addresses that cannot be accessed.
5. If the ping is OK, this is not a delivery network problem. The PTSS informs the CSP's contact of this, indicating which data is not transmitted and that it is not a problem with the delivery network.

Note: The order of testing "Layer 1 Interface" and "Layer 3 Check PING" is not specified. The signals sent from the master process to the CSP (either "Layer 1 down <Parameters>" or "Layer 3 down <Parameters>") are independent of the order.

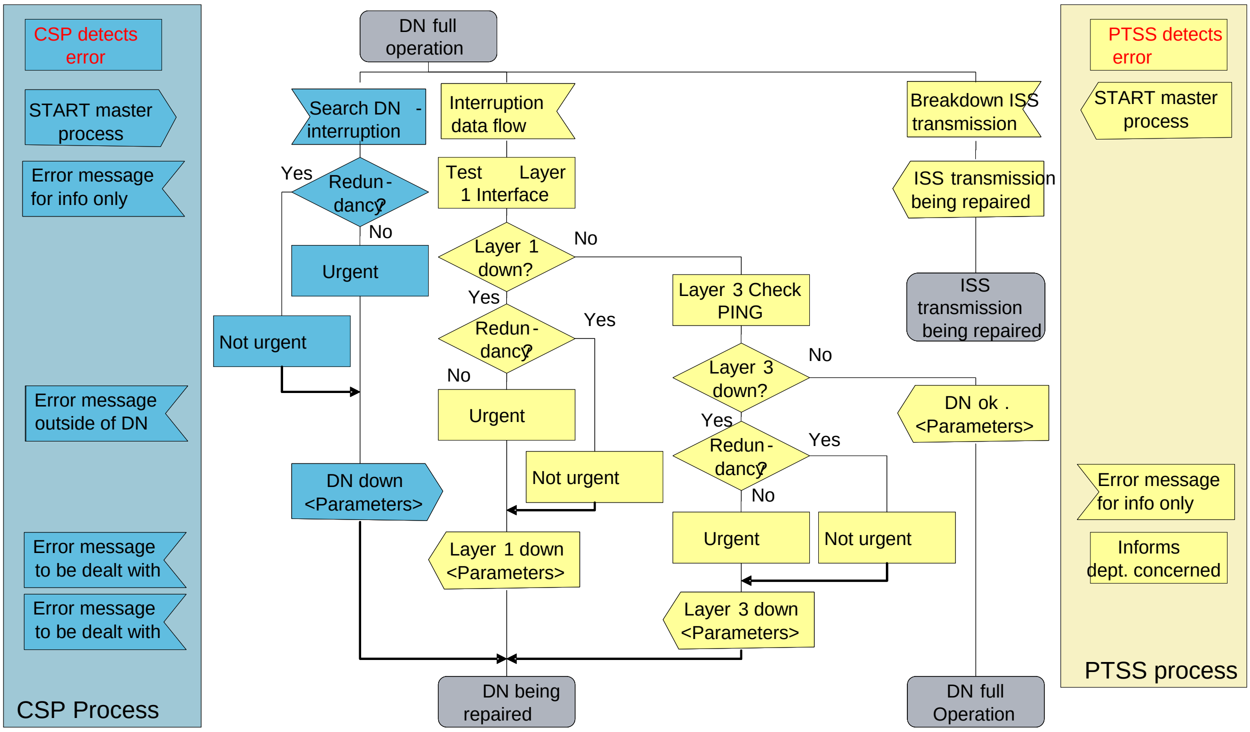


Figure 20 Master error handling process for the direct connection DN variant (1/2)

Explanations of Figure 20 and Figure 21:

The flowchart shows the triggers and subsequent process, e.g. "Start Master Process" and "Locate DN interruption".

<Parameters> means that certain parameters or information are to be entered.
Examples:
In the case of "DN down", such information is the link name, the duration of the interruption or at least how long it will take until the duration of the interruption is known.

In the case of "Layer 1 down", the additional parameters or details are, for example, the link name, error type (LOS, i.e. Layer 1 down, etc.), the time at which the error was determined and whether or not the redundant path is functioning.

In the case of “Layer 3 down”, the parameters are, for example, the route or which IP addresses of the PTSS can no longer be accessed, whether an interface may also be down on layer 2, the time at which the error was detected, and whether or not the redundant path is functioning.

For "DN ok”, it should be specified that the delivery network is not affected but that there is nonetheless an interruption to data delivery. The handling of this error scenario extends beyond the delivery network and is therefore not described in this document.

“Breakdown ISS Transmission” stands for a breakdown at the PTSS end, meaning that only one of the two links between the CSP and the PTSS can be used. In such a case, the CSP is not permitted to carry out any maintenance work on the other link. Accordingly, the link name and the expected duration of the interruption must be given.

“ISS transmission in repair” refers to the repair work in the PTSS area (ISS), while “DN in repair” refers to the section between the CSP and the PTSS.

The distinction between “urgent” or “not urgent” depends on whether there are redundancies at the DN level. The corresponding rules are specified in the OAR from Version 3.0 on. For problems classified as “not urgent”, support is available during office hours only.

The layer 3 check with a ping must at least reach the first equipment with layer 3 breakpoint. If firewalls are used, the owners must set and implement the roles such that pings can pass.

The CSPs can also send pings to the infrastructure of the PTSS. The PTSS shall take the necessary measures (e.g. firewall roles) to enable pings.

Situation 2:
The **CSP** detects an interruption in the delivery network (see Figure 21)

Procedure:

- The CSP informs the PTSS’s contact, specifying the interrupted link. It should also state the time by which the problem will have been resolved.

Process structure:
The master process described here refers to the DN handover point between the CSP and the PTSS.
Characteristics:

a) There is one PTSS process and one CSP process, both of which communicate with the master process.
b) The master process is started by the PTSS process or the CSP process by means of “START Master Process”.
c) The PTSS process or the CSP process have access to the master process.
d) The PTSS process or the CSP process receive data from the master process (<Parameters>).
e) The parameters have yet to be specified in detail (see examples below).
f) The specifications of the PTSS process and the CSP process concern the PTSS or the relevant CSP only and are not visible to the other party.

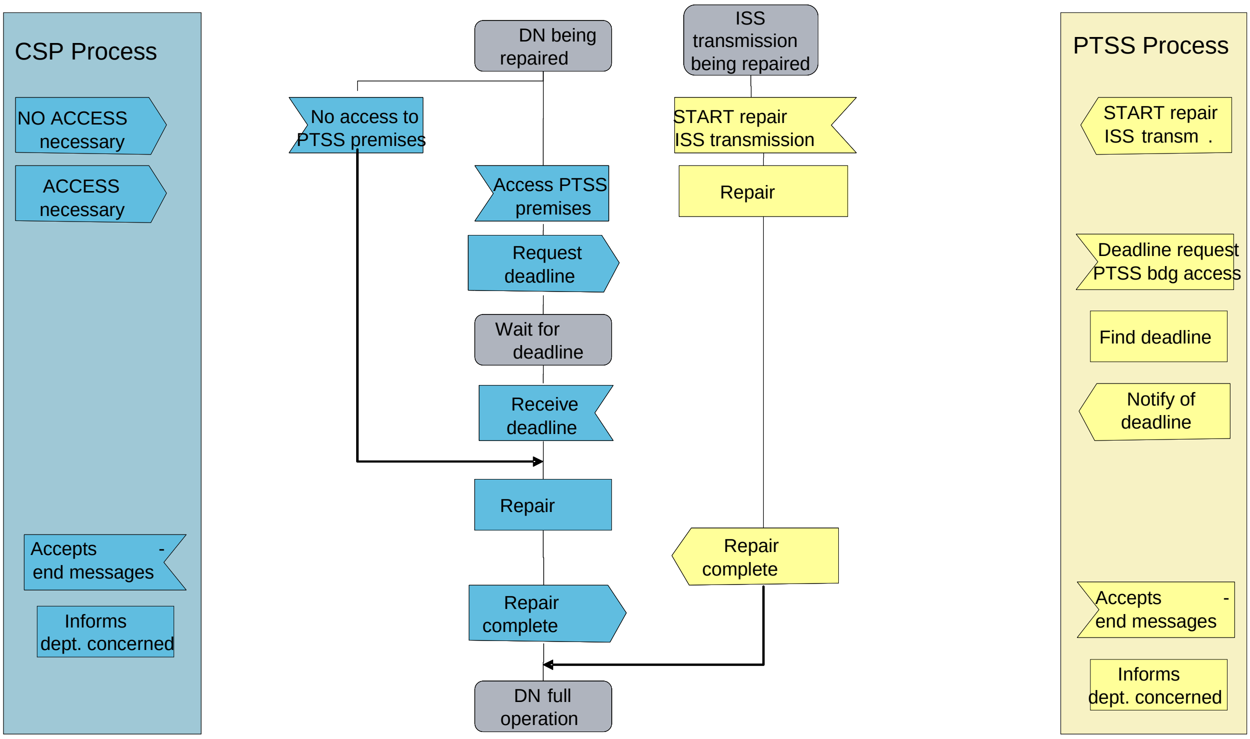


Figure 21 Master error handling process for the direct connection DN variant (2/2)

15 Annexes

Additional general requirements are specified in the following Annexes.

Annex A: Signalling sequences for the CS delivery network

The following diagrams show signalling sequences at both handover points from the CSP to the ISDN-DN provider (ISUP sequences) and from the ISDN-DN provider to the PTSS/ISS (DSS1 sequences).
Figure 22 shows a successful and complete delivery of CS-CC.

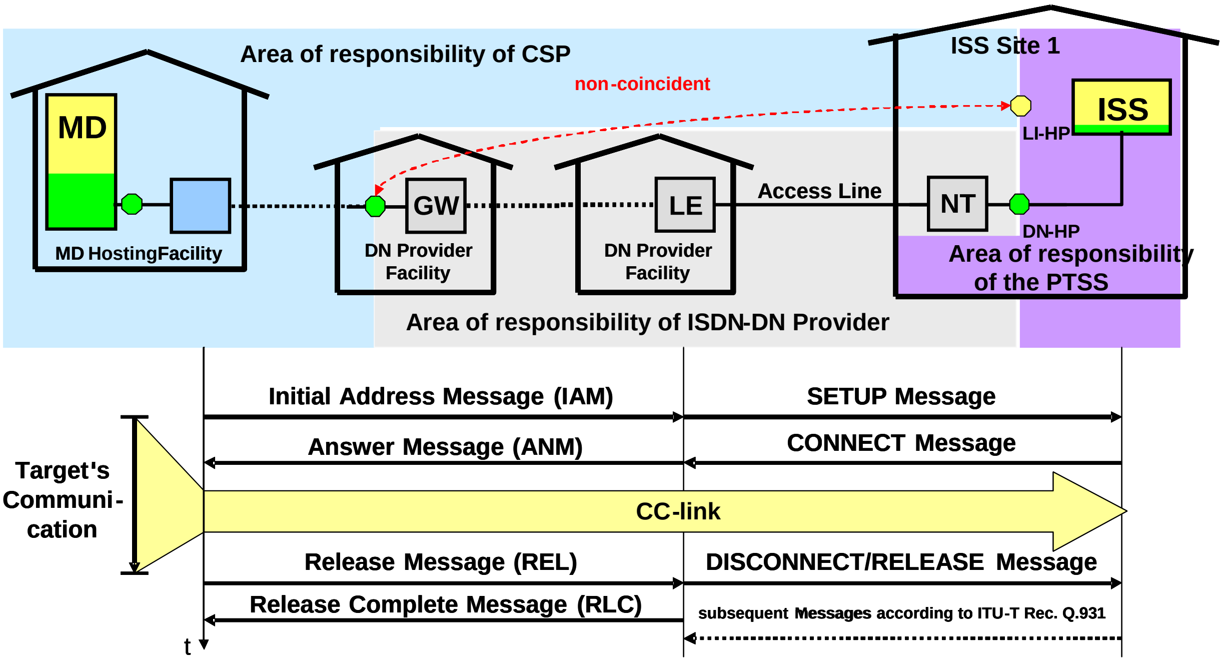

Area of responsibility of CSP
non-coincident
ISS Site 1
MD
ISS
LI-HP
GW
LE
Access Line
NT
DN-HP
MD HostingFacility
DN Provider Facility
DN Provider Facility
Area of responsibility of the PTSS
Area of responsibility of ISDN-DN Provider
Initial Address Message (IAM)
SETUP Message
Answer Message (ANM)
CONNECT Message
Target's Communi-cation
CC-link
Release Message (REL)
DISCONNECT/RELEASE Message
Release Complete Message (RLC)
subsequent Messages according to ITU-T Rec. Q.931
t

Figure 22 Signalling sequences for the required set-up and release of a CC link

The ANM is a form of acknowledgment for the CSP (received by the MD) that a CC link has been set up and the delivery of CC is starting. After the intercepted connection is released, the CC links are also released by the MD and the ISS receives a REL with cause value 16 and the location “user” (0000).
Figure 23, Figure 24 and Figure 25 show unsuccessful attempts to set up a CC link. The MD will repeat the connection set-up attempts a specific number of times (not shown in Figure 23, Figure 24 and Figure 25).

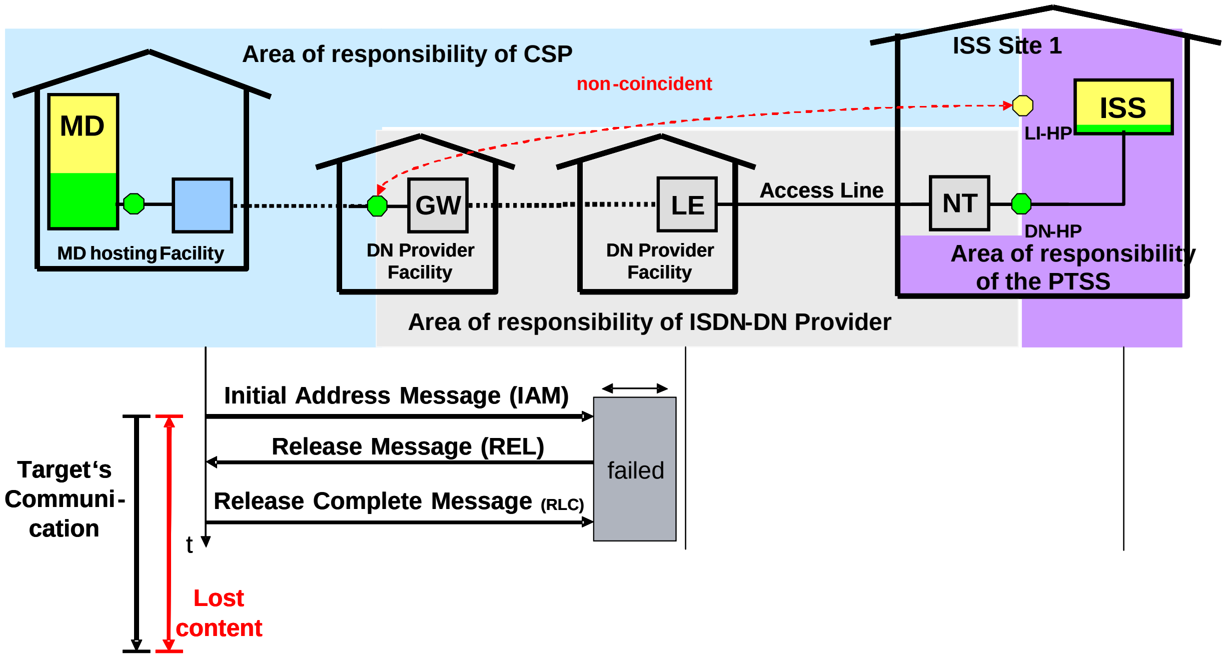


Figure 23 Signalling sequences in case of rejection of set-up of a CC link by the ISDN delivery network

The REL message at the handover point between the CSP and the ISDN-DN provider contains a cause value that indicates the location of the error.

Table 1 shows all cause values that can occur, as specified by the universal service licensee (based on the corresponding international standards). The CSP's incoming network receives information on which entity has caused an error. In principle, all the CSP needs to know is whether it has caused the error itself. In the case of an error with the ISDN-DN or the ISS, the CSP has to send a message to the ISDN-DN provider and/or the PTSS. The detailed determination of the reason falls under the responsibility of the ISDN-DN provider or the PTSS. In cases where the cause is not clear (e.g. “MD or ISDN-DN”) , further investigations must be carried out jointly.

Table 1: Cause values and location in case of rejection of set-up of a CC link by the ISDN delivery network

Cause value, see ITU-T Rec. Q.850	**Location**	**Failure caused by**	**Responsibility**
1	Other than user (0000)	MD	CSP
17	Other than user (0000)	ISS	PTSS
21	Other than user (0000)	MD	CSP
25	Other than user (0000)	ISDN-DN	ISDN-DN Provider
27	Other than user (0000)	ISS	PTSS
28	Other than user (0000)	MD	CSP
31	Other than user (0000)	MD or ISDN-DN	CSP
34	Other than user (0000)	ISDN-DN or ISS	PTSS
38	Other than user (0000)	ISDN-DN	ISDN-DN Provider
41	Other than user (0000)	ISDN-DN	ISDN-DN Provider
42	Other than user (0000)	ISDN-DN	ISDN-DN Provider
57	Other than user (0000)	MD	CSP
102	Other than user (0000)	ISDN-DN	ISDN-DN Provider
111	Other than user (0000)	MD or ISDN-DN	CSP

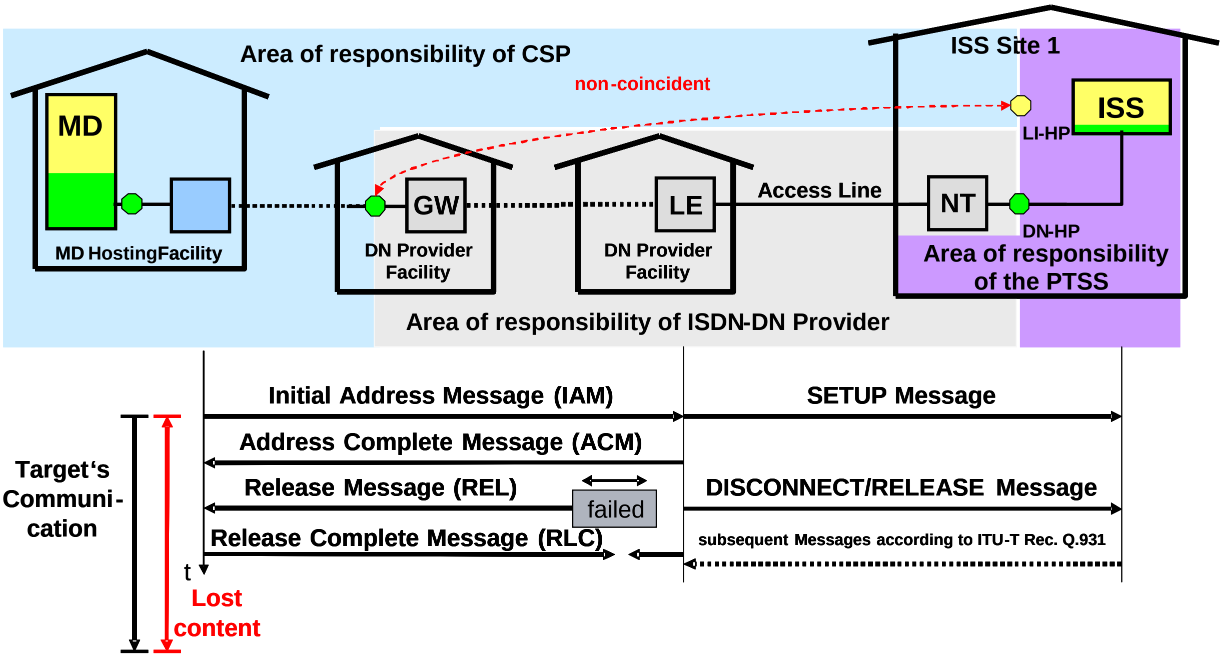

Area of responsibility of CSP
non-coincident
ISS Site 1
ISS
LI-HP
MD
MD HostingFacility
GW
DN Provider Facility
LE
DN Provider Facility
Access Line
NT
DN-HP
Area of responsibility of the PTSS
Area of responsibility of ISDN-DN Provider
Initial Address Message (IAM)
SETUP Message
Address Complete Message (ACM)
Release Message (REL)
failed
DISCONNECT/RELEASE Message
Release Complete Message (RLC)
subsequent Messages according to ITU-T Rec. Q.931
Target's Communi-cation
t
Lost content

Figure 24 Signalling sequences for release during set-up of a CC link by the ISDN delivery network

The REL message at the handover point between the CSP and the ISDN-DN provider contains a cause value that indicates the location of the error.
Table 1 shows all cause values that can occur, as specified by the universal service licensee (based on the corresponding international standards). The CSP's incoming network receives information on which entity has caused an error. In principle, all the CSP needs to know is whether it has caused the error itself. In the case of an error with the ISDN-DN or the ISS, the CSP has to send a message to the ISDN-DN provider and/or the PTSS. The detailed determination of the reason falls under the responsibility of the ISDN-DN provider or the PTSS. In cases where the cause is not clear (e.g. "ISDN-DN or MD") , further investigations must be carried out jointly.

Table 2: Cause values and location in case of release of set-up of a CC link by the ISDN delivery network

Cause value, see ITU-T Rec. Q.850	Location	Failure caused by	Responsibility
27	Other than user (0000)	ISDN-DN or ISS	PTSS
31	Other than user (0000)	MD or ISDN-DN or ISS	PTSS
38	Other than user (0000)	ISDN-DN or ISS	PTSS
41	Other than user (0000)	ISDN-DN	ISDN-DN Provider
102	Other than user (0000)	MD or ISDN-DN or ISS	PTSS
111	Other than user (0000)	MD or ISDN-DN or ISS	PTSS

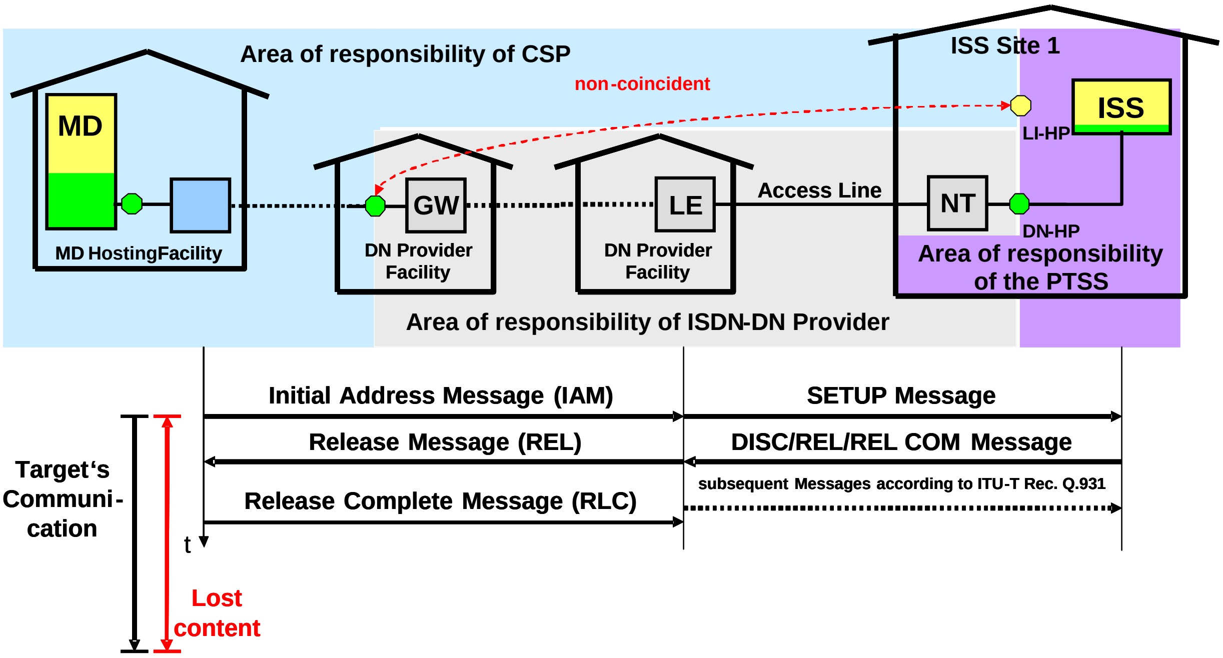

Area of responsibility of CSP
non-coincident
ISS Site 1
ISS
LI-HP
MD
GW
LE
Access Line
NT
DN-HP
MD HostingFacility
DN Provider Facility
DN Provider Facility
Area of responsibility of the PTSS
Area of responsibility of ISDN-DN Provider
Initial Address Message (IAM)
SETUP Message
Release Message (REL)
DISC/REL/REL COM Message
subsequent Messages according to ITU-T Rec. Q.931
Release Complete Message (RLC)
Target's Communi-cation
t
Lost content

Figure 25: Signalling sequences in case of rejection of set-up of a CC link by the LEMF (ISS)

Unless otherwise explicitly stated in Table 3, the REL messages at the handover point between the CSP and the ISDN-DN provider and at the handover point between the PTSS and the ISDN-DN provider contain the same cause value indicating the location of the error.

Table 3 does not require the ISS to support all cause values but merely specifies the interpretation by the receiving entity. In principle, all the CSP needs to know is whether the error lies in the ISS. The detailed determination of the reason falls under the responsibility of the PTSS. As the PTSS itself knows the status (all cause values are given by the ISS), it does not need a separate message from the CSP or the ISDN-DN provider.

Table 3: Cause values and location in case of rejection of set-up of a CC link by the LEMF (ISS)

Cause value, see ITU-T Rec. Q.850	Location	Failure caused by
1	user (0000)	ISS
17	user (0000)	ISS
18	user (0000)	ISS
19	user (0000)	ISS
20	user (0000)	ISS
21	user (0000)	ISS
22	user (0000)	ISS
27	user (0000)	ISS
31 may be different at PTSS side since the ISDN delivery network translates any cause value not appearing in this Table into 31	user (0000)	ISS
34	user (0000)	ISS
41	user (0000)	ISS
42	user (0000)	ISS
44 at PTSS side only, appears as 17 or 34 at MD side	user (0000)	ISS
47	user (0000)	ISS
65	user (0000)	ISS
88	user (0000)	ISS

Figure 26 and Figure 27 show abnormal releases of a CC link set-up. The MD repeats the connection set-up attempts a specific number of times in accordance with TR TS [4].

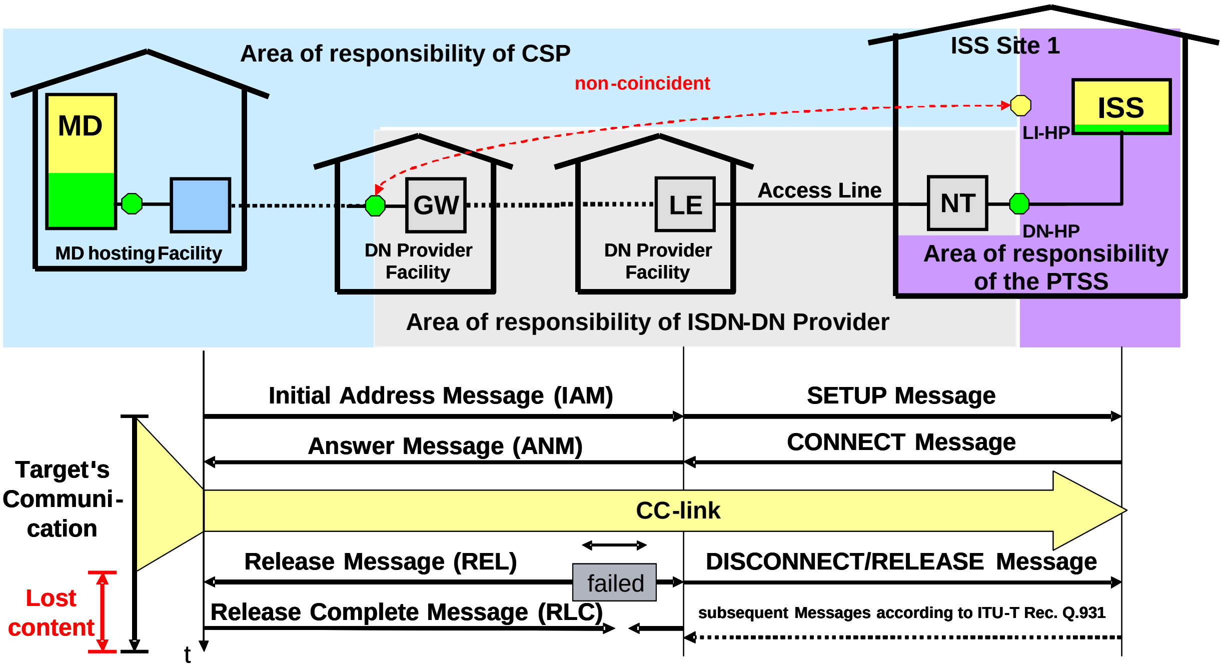

Area of responsibility of CSP
non-coincident
ISS Site 1
ISS
LI-HP
MD
MD hosting Facility
GW
DN Provider Facility
LE
DN Provider Facility
Access Line
NT
DN-HP
Area of responsibility of the PTSS
Area of responsibility of ISDN-DN Provider
Initial Address Message (IAM)
SETUP Message
Answer Message (ANM)
CONNECT Message
Target's Communi-cation
CC-link
Release Message (REL)
failed
DISCONNECT/RELEASE Message
Lost content
Release Complete Message (RLC)
subsequent Messages according to ITU-T Rec. Q.931
t

Figure 26: Signalling sequences for release of a CC link as a result of an error detected in the ISDN delivery network

NOTE: If an error is detected by the ISDN delivery network, the cause may also lie outside of this network (see table of cause values).

The REL messages at the handover point between the CSP and the ISDN-DN provider and at the handover point between the PTSS and the ISDN-DN provider contain the same cause value indicating the location of the error.

Table 4 shows all cause values that can occur, as specified by the universal service licensee (based on the corresponding international standards). The CSP's incoming network receives information on which entity has caused an error. In principle, all the CSP needs to know is whether it has caused the error itself. In the case of an error with the ISDN-DN or the ISS, the CSP has to send a message to the ISDN-DN provider and/or the PTSS, as the case may be. The detailed determination of the reason falls under the responsibility of the ISDN-DN provider or the PTSS. In cases where the cause is not clear (e.g. "ISDN-DN or MD"), further investigations must be carried out jointly.

Table 4: Cause values and location in case of release of a CC link as a result of an error detected in the ISDN delivery network

Cause value, see ITU-T Rec. Q.850	**Location**	**Failure caused by**
31	Other than user (0000)	MD or ISDN-DN or ISS
38	Other than user (0000)	ISDN-DN or ISS
41	Other than user (0000)	ISDN-DN
102	Other than user (0000)	MD or ISDN-DN or ISS
111	Other than user (0000)	MD or ISDN-DN or ISS

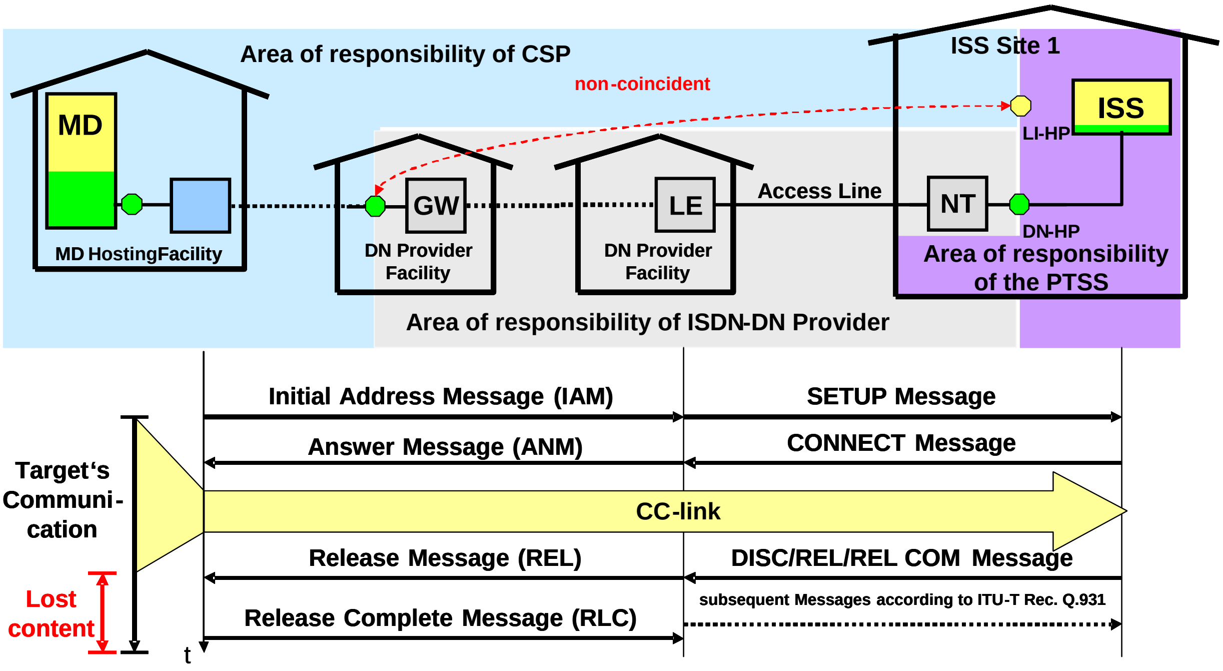


Figure 27 Signalling sequences for release of a CC link as a result of an error in the ISS

Unless otherwise explicitly stated in Table 5, the REL messages at the handover point between the CSP and the ISDN-DN provider and at the handover point between the PTSS and the ISDN-DN provider contain the same cause value indicating the location of the error.
Table 5 does not require the ISS to support all cause values but merely specifies the interpretation by the receiving entity. In principle, all the CSP needs to know is whether the error lies in the ISS. The detailed determination of the reason falls under the responsibility of the PTSS. As the PTSS itself knows the status (all cause values are given by the ISS), it does not need a separate message from the CSP or the ISDN-DN provider.

Table 5 Cause values and location in case of release of a CC link as a result of an error in the LEMF (ISS)

Cause value, see ITU-T Rec. Q.850	**Location**	**Failure caused by**
16	user (0000)	ISS (ISS must not release a CC link as a normal case)
27	user (0000)	ISS
31 may be different at PTSS side since the ISDN delivery network translates any cause value not appearing in this Table into 31	user (0000)	ISS
41	user (0000)	ISS
47	user (0000)	ISS

Annex B: 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 or 1000BASE-SX 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	10BASE-T according to IEEE 802.3 clause 14 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	100BASE-TX according to IEEE 802.3 clauses 24 and 25 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-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, 1000Base-LX, according to IEEE 802.3 clause 38 single mode Connector: LC with single 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	10BASE-T according to IEEE 802.3 clause 14 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	100BASE-TX according to IEEE 802.3 clauses 24 and 25 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-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, 1000Base-LX, according to IEEE 802.3 clause 38 single mode Connector: LC with single mode fibre

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

For connecting to the delivery network in relation to the IP-Header, the systems being attached 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.

INFORMATIVE NOTE:

In order to achieve compatibility between Precedence/TOS according to IETF RFC 791 and DiffServ according to IETF RFC 2474, code points selected from the set defined in the table below shall be used.

Bit position within 32-bit format according to IETF RFC 791 Figure 4	8	9	10	11	12	13	14	15
Function according to IETF RFC 791 (Type of Service (TOS))	Precedence			D	T	R	C	res
Function according to IETF RFC 2474 (DiffServ)	Differentiated Services Code Point (DSCP)						Currently Unused (CU)	
Codepoints	set of code points to be set to the value according to PTSS			pre-assigned (ensures compatibility and interoperability of IETF RFC 791 with IETF RFC 2474)				
Network Control	1	1	1	0	0	0	0	0
Internetwork Control	1	1	0	0	0	0	0	0
Critical Intelligence Communication/Emergency Command Precedence (CRITIC/ECP)	1	0	1	0	0	0	0	0
Flash Override	1	0	0	0	0	0	0	0
Flash	0	1	1	0	0	0	0	0
Immediate	0	1	0	0	0	0	0	0
Priority	0	0	1	0	0	0	0	0
Routine	0	0	0	0	0	0	0	0

Annex C: Equipment hosting

When in-house handover points (HP) are used, this means that equipment is housed in third-party premises (e.g. the equipment of a delivery network provider on the premises of ISC-FDJP or other federal authorities).

The following requirements must be met by the hoster's building infrastructure and the hosted equipment.

1 Power supply and earthing

With regard to the power supply, the systems must comply with the following European standards: ETSI ETS EN 300 132-3 "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 Power supply, rectified current source, alternating current source or direct current source."

ETSI, ETS EN 300 132-3 v1.2.1 (2003-08), 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 Power supply, rectified current source, alternating current source or direct current source, August 2003

With regard to earthing, the systems must comply with the following European standard: ETS EN 300 253 "Earthing and bonding of telecommunication equipment in telecommunication centres".

A server farm (consisting of locally installed equipment) is also classified as "telecommunication equipment".

ETSI ETS EN 300 253 v2.1.1 (2002-04), Equipment Engineering (EE); Earthing and bonding of telecommunication equipment in telecommunication centres, January 1995

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 ETSI Standard EN 300 019-1-3 "Environmental conditions and environmental tests for telecommunications equipment – Stationary use at weather-protected locations", Class 3.1.

For the broadband network equipment listed below, the requirements for "Class 3.2" must be met so as to address the recommendations set out in the European Commission's "Code of Conduct on Energy Consumption of Broadband Equipment".

The types of broadband network equipment covered under the Code of Conduct are as follows (see Table 1 of the Code of Conduct):

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)

ETSI EN 300 019-1-3 V2.23.2 (2009-11), Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-3: Classification of environmental conditions; Stationary use at weather protected locations; July 2004.

EUROPEAN COMMISSION, DIRECTORATE-GENERAL JRC; JOINT RESEARCH CENTRE; Institute for the Environment and Sustainability; Renewable Energies Unit; Code of Conduct on Energy Consumption of Broadband Equipment, Version 2, 17 July 2007

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.

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.

4 Electromagnetic compatibility (EMC)

The equipment must comply with the European standard ETS EN 300 386-1 “Telecommunication network equipment ElectroMagnetic Compatibility (EMC) requirements”, including the Corrigendum, with regard to the emission of electromagnetic interference and immunity to such interference.

ETSI ETS EN 300 386-1 v1.5.1 (2010-10), Equipment Engineering (EE); Public Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electro-Magnetic Compatibility (EMC) requirements Part 1: Product family overview, compliance criteria and test levels; December 1994

ETSI, Corrigendum modifying the European Telecommunication Standard ETS 300 386-1 (1994), April 1997

5 Electrostatic discharge (ESD)

The equipment must comply with the European standard ETS EN 300 386-1 “Telecommunication network equipment ElectroMagnetic Compatibility (EMC) requirements”, including the Corrigendum, with regard to electrostatic discharge to humans or objects.

ETSI ETS 300 386-1, Equipment Engineering (EE); Public telecommunication network equipment Electro-Magnetic Compatibility (EMC) requirements Part 1: Product family overview, compliance criteria and test levels; December 1994

ETSI, Corrigendum modifying the European Telecommunication Standard ETS 300 386-1 (1994), April 1997

6 Resistibility to overvoltages and overcurrents

The equipment must comply with the European standard ETS EN 300,386 3861 “Telecommunication network equipment ElectroMagnetic Compatibility (EMC) requirements”, including the Corrigendum, with regard to resistibility to overvoltages and overcurrents.

ETSI ETS 300 386-1, Equipment Engineering (EE); Public telecommunication network equipment Electro-Magnetic Compatibility (EMC) requirements Part 1: Product family overview, compliance criteria and test levels; December 1994

ETSI, Corrigendum modifying the European Telecommunication Standard ETS 300 386-1 (1994), April 1997

7 Uninterruptible power supply (UPS)

The UPS equipment must comply with the following ETSI guidelines: ETSI TR 102 446 Environmental Engineering (EE); General Requirements for UPS for use in Telecommunication Environment. Both ISS sites have a UPS and an emergency power supply by means of diesel generators.

8 Safety

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

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.