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

IP-based Delivery Network via OpenVPN Provider Handbook

Date: 04 July 2012

Version 1.2

Address and contact:

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

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

Table of contents

1. Scope of the Document

The present handbook provides information about the setup and the correct operation of the IP-based Delivery Network via OpenVPN according to TR TS [1], section 16.6.2.4.

Its intended audience is any CSP implementing this delivery method.

2. Abbreviations

CSP	Communications Service Provider
FDJP	Federal Department of Justice and Police
IIF	Internal Interception Function
IRI	Interception Related Information
ISC-FDJP	IT Service Centre Federal Department of Justice and Police
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MF	Mediation Function
NAT	Network Address Translation
PTSS	Post and Telecommunications Surveillance Service
VPN	Virtual Private Network

3. Terminology

Internal Interception Function (IIF) of the CSP
Point within a network or network element at which the Content of Communication and the Interception Related Information are made available.

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

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

Mediation Function (MF)
Mechanism which passes information between a CSP and a Handover Interface, and information between the Internal Network Interface and the Handover Interface

VPN client
The VPN client is part of the CSP’s infrastructure and it connects to the VPN endpoint.

VPN endpoint
The VPN endpoint is part of the IP-based Delivery Network via OpenVPN and it acts as a server for the VPN connections of the CSPs. It is operated by the ISC-FDJP.

4. References

[1]	TR TS	Guidelines for Lawful Interception of Telecommunication Traffic, Technical Requirements for Telecommunication Surveillance, Version 3.0, 23 November 2011
[2]	RFC1918	Address Allocation for Private Internets, February 1996
[3]	Delivery Network Concept	Concept paper on delivery networks between CSPs and the ISS for telecommunication surveillance of packet-switched and circuit-switched services, Version 1.0, 30 January 2012

5. OpenVPN Overview

5.1. Concept

The concept is described in [3]. The VPN is implemented using the OpenVPN software. The CSP is free to select its own operating system. Currently, the software is available for various Windows versions, Unix derivatives and Mac OS X.

There are two alternatives:

- OpenVPN is installed as an additional service on the Mediation Function or the Internal Interception Function of the CSP. This alternative causes the least effort.
- OpenVPN is installed on a dedicated server. This alternative causes more effort because care must be taken to configure the correct routing.

5.2. Addressing

The IP address of the VPN endpoint at ISC-FDJP does not change for the CSP. In the event that the VPN connection fails the CSP shall periodically (approximately every 5 seconds) retry to re-establish the connection. The CSP can use redundant VPN clients under its own responsibility. ISC-FDJP does not screen the IP source address of the VPN tunnel.

The addresses used within the VPN are allocated according to RFC1918 [2]. Each VPN client receives such an address for its virtual network interface towards the VPN tunnel. The CSP can choose amongst 4 different VPN endpoints which use different RFC1918 [2] ranges.

All ISS systems (Production, Integration, Test, Schulung (training) and the predecessor system LIS / LITS can be reached via one unique tunnel. If required, additional tunnels can be added by the CSP in agreement with PTSS.

4 different IP ranges will be proposed. The purpose of the 4 different ranges is to prevent conflicts with the internal addressing of the CSP. Each CSP can decide which VPN endpoint to use. The ranges within the VPN will not change in the foreseeable future.

5.3. Current LEMF LIS / LITS

5.3.1. CS HI2 IRI and HI1 notifications

Another aspect of the addressing is the LEMF which is configured as the endpoint for the transmission of the results of interception. A public IP address range is reserved for this purpose.

FTP usernames and passwords will be provided by PTSS.

PTSS can modify or replace the public IP address range or it can add other ranges.

5.4. New LEMF ISS

5.4.1. CS HI2 IRI and HI1 notification

The CS IRI are delivered via the IP Delivery Network.

FTP usernames and passwords will be provided by PTSS.

5.4.2. Specification for PS Delivery (HI2/HI3)

The IP IRI (HI2) and content of communication (HI3) are delivered via the IP Delivery Network.

5.4.3. Specification for the ISS Warrant Management System WMS (HI1)

- Email addresses of the ISS WMS for sending warrants and receiving administrative acknowledgements will be provided by PTSS.

- New public PGP keys for each email addresses of the ISS WMS will be generated and delivered to the CSP

5.5. Allocation of Addresses within the VPN Tunnel

The CSP’s IP address within the VPN tunnel is allocated automatically during the handshake when establishing the connection. The VPN client uses the IP address assigned by the VPN endpoint (OpenVPN Server).

The allocation of an IP address to a CSP is defined statically on the VPN endpoint. But PTSS can adapt this allocation. When setting up the VPN connection, a CSP must therefore not assume to get the same IP address every time and take this into account in its configuration (see also 7.2).

5.6. Security Features

By using OpenVPN, it is ensured that the data transmitted over the Internet is encrypted. The encryption is done with the AES algorithm with at least 128 bit key length. Additionally, an integrity check of the transmitted data is performed in order to detect manipulations.

For authentication purposes, each CSP receives 2 keys or key pairs.

- One «TLS Auth Key» which is used for the authentication of the TLS handshake

- One certificate as well as the corresponding private key in order to authenticate the connection establishment to the VPN endpoint

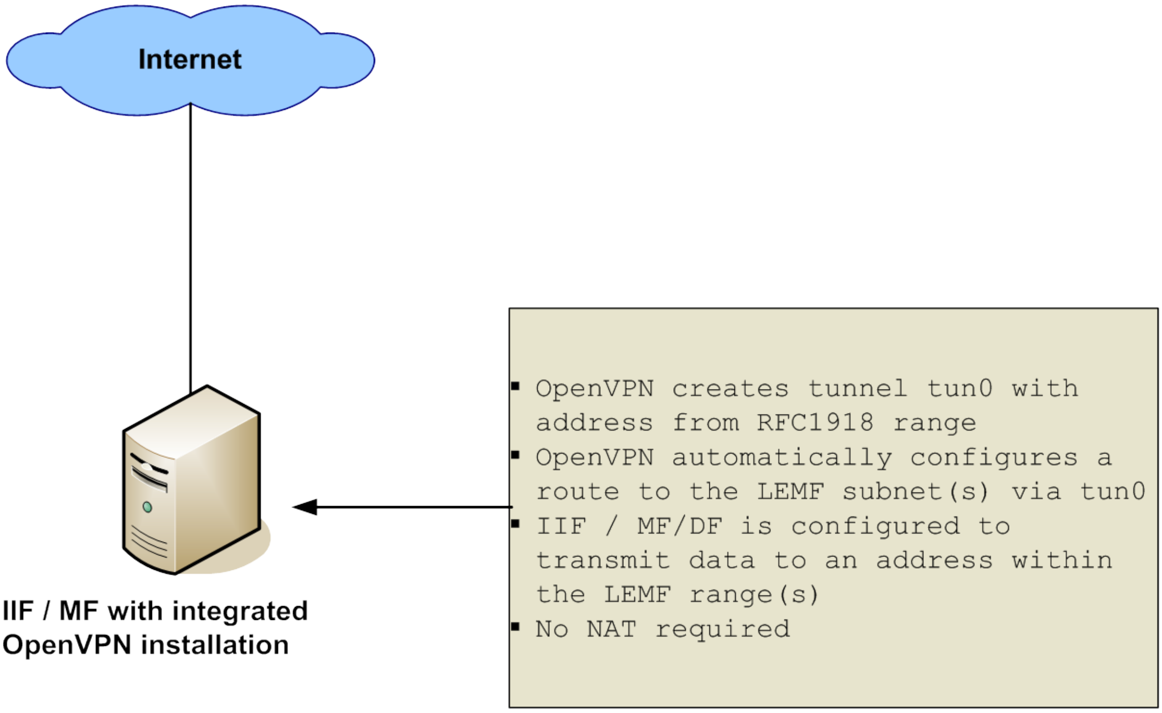
The CSP is obliged to appropriately protect the keys or key pairs from misuse and to make sure that they are not accessible to third parties.

After a VPN client has successfully authenticated itself to the VPN endpoint, they are periodically negotiating individual session keys for the encryption. The method for generating the session key complies with the Perfect Forward Secrecy principle.

6. Schematic View of the Installation

6.1. Alternative 1: OpenVPN client on IIF or MF

The installation of OpenVPN as an additional component on the IIF or the MF is simple. The diagram below shows the schematic view.



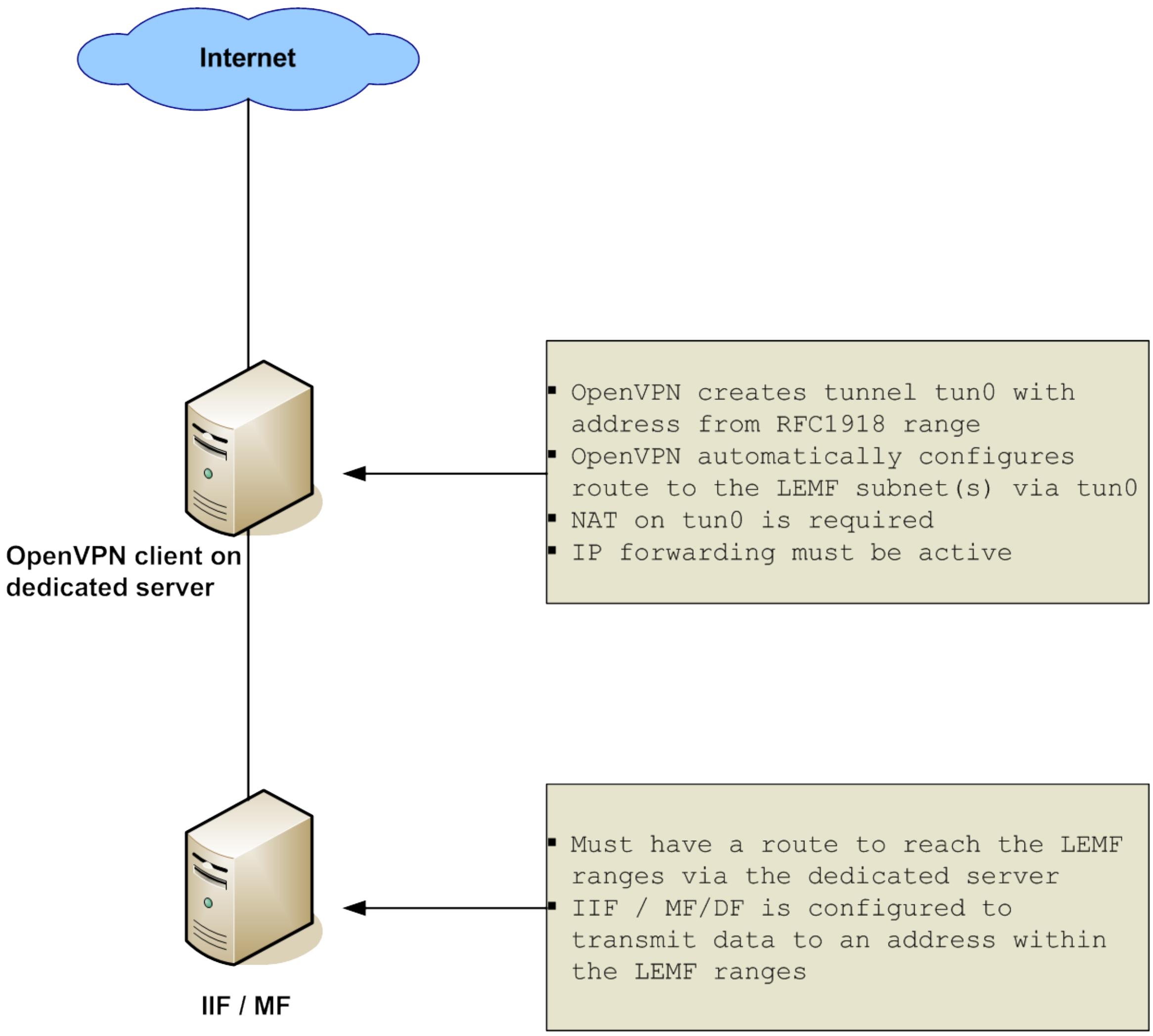
- OpenVPN creates tunnel tun0 with address from RFC1918 range
- OpenVPN automatically configures a route to the LEMF subnet(s) via tun0
- IIF / MF/DF is configured to transmit data to an address within the LEMF range(s)
- No NAT required

Figure 1 : IIF or MF with integrated OpenVPN client

6.2. Alternative 2: OpenVPN client on a dedicated server

The configuration is slightly more complex if the OpenVPN client is installed on a dedicated server. As shown in the figure below, certain points have to be respected, especially the NAT on the tunnel device. The provider chooses itself the IP range for the delivery network between its own components.

IP-based Delivery Network via OpenVPN



- OpenVPN creates tunnel tun0 with address from RFC1918 range
- OpenVPN automatically configures route to the LEMF subnet(s) via tun0
- NAT on tun0 is required
- IP forwarding must be active

- Must have a route to reach the LEMF ranges via the dedicated server
- IIF / MF/DF is configured to transmit data to an address within the LEMF ranges

Figure 2: OpenVPN on a dedicated server

7. OpenVPN Configuration

7.1. Configuration File for the OpenVPN Client

The configuration file for the OpenVPN is shown below. A CSP must adopt this configuration for its installation of the OpenVPN client.

```
# Define OpenVPN as a client, “tun” device as virtual tunnel interface and
# UDP as the transport protocol
client
dev tun
proto udp

# Configure the IP address and port of the VPN endpoint (remote)
# see VPN endpoints and IP ranges table
remote xxx.xxx.xxx.xxx pppp

# Do not bind to local address and port
nobind

# Define the username and group of the OpenVPN client
user someuser
group somegroup

# Re-use the key and the “tun” device each time the connection is
# re-established
persist-key
persist-tun

# Limit the size of the UDP packets to max. 1300 bytes (MTU) within the
# tunnel
fragment 1300

# Path to the CA certificate
ca /path/to/ca.crt

# Path to the client certificate
cert /path/to/client.crt

# Path to the Client-Private-Key
key /path/to/client.key

# Path to the TLS-Auth Key
tls-auth /path/to/tlsauth.pem

# Ensure that the client only connects to a host which is a designated
# server. This is an important security precaution to protect against a
# man-in-the-middle attack where an authorized client attempts to connect
# to another client by impersonating the server.
ns-cert-type server

# Use fast LZO compression - mandatory
comp-lzo

# Set log output verbosity level to 3. Level 3 is recommended if
# you want a good summary of what's happening without being swamped by
# output. (see OpenVPN manual for details)
verb 3
```

Table 1: Configuration file of a VPN client

7.2. Considerations about the Configuration of the Client

In general, it makes sense to run the VPN client under a dedicated user account. This way, the Least Privilege Principle is applied. It is wise not to grant administrator or other special rights to the VPN client.

All keys which the CSP receives from the PTSS must be stored as clear text on the system with the VPN client in order to establish the VPN connection. Care must be taken to prevent the theft of the keys. This can be achieved by granting limited access rights on the file system (for example exclusive read access for the dedicated user account of the OpenVPN client).

The CSP can implement the VPN client according to its own security policy. The two proposals above are recommendations. However, the PTSS definitely requires the CSP to adequately protect the VPN keys from theft. In the event that a key has been compromised, PTSS has to be informed immediately so that the certificate can be revoked.

Particular care must be taken when the IP address assigned to the VPN virtual interface changes. On some operating systems, re-configuring the VPN tunnel with another IP address causes a connection loss: The client could stop when it gets a new address from the server. Therefore, the CSP must prepare its VPN system for such events by implementing an appropriate monitoring and ensuring prompt automatic re-establishment of the VPN connection.