General Intelligence and
Security Service
*Ministry of the Interior and
Kingdom Relations*

Europaweg 4 2711 AH
Zoetermeer
P.O. Box 20010 2500 EA The
Hague The Netherlands
www.aivd.nl

Contact
T +31 (0)79 320 50 50
F +31 (0)70 320 07 33

Date
October 24, 2018

Our reference
8f495785-or1-1.4

Enclosures
0

Copy number

Deployment Advisory

OpenVPN-NL

For use at Security Level 2

Valid until: 1-1-2024

Table of Contents

1 Introduction

The open source VPN (virtual private network) implementation OpenVPN has been hardened and documented by Fox-IT under direction of the NLNCSA (Netherlands National Communications Security Agency, in Dutch “NBV”: Nationaal Bureau voor Verbindingsbeveiliging) and in preparation for an evaluation against security level 2 of the NLNCSA criteria in 2010/2011. Since then Fox-IT has maintained OpenVPN-NL under direction of the NLNCSA. This report describes the outcome of the original evaluation up to and including the most recent release (the OpenVPN-NL 2.4 branch). This report outlines the requirements and guidance for secure deployment of the hardened version of OpenVPN (from this point on identified as OpenVPN-NL or OpenVPN) where the original open source version will be denoted `vanilla OpenVPN'.
This advisory is intended for ICT decision makers, process owners, security officers and administrators of the product. Based on this advisory, the user organization is able to make a responsible assessment whether or not to use the product in its business process.

Please check on the OpenVPN-NL downloadsite, https://openvpn.fox-it.com (in section "Lifecycle") if you have the latest version of this Deployment Advisory.
As soon as an updated version is available, it will be published there.

2 Product description

A Virtual Private Network (VPN) is a connection between endpoints that transports network traffic. For data transported by the VPN, the connection between the VPN endpoints appears to be a direct link, when in fact the transported data may travel many steps over multiple external carrier networks. In other words, a VPN creates a new network topology on top of the underlying carrier network(s). Note that VPN tunnels typically connect two machines, but that either endpoint may be the endpoint in multiple connections. In particular, networks may have fully meshed or hub-spoke architectures as well as point to point.

2.1 OpenVPN software

OpenVPN is a software-only VPN implementation that runs as a normal userspace program, as opposed to e.g. IPsec that is typically integrated in the kernel of an operating system. Instead of sending network traffic to a physical network device, OpenVPN attaches to a virtual network device that relays packets to the OpenVPN process – both TAP devices (layer two) and TUN (layer three) devices can be configured. This process performs the set up of the VPN tunnel and takes care of encryption and decryption of outgoing and incoming packets respectively. Other programs and processes on the platform need not be changed. The setup of the virtual network interface and the adjustment of the operating systems routing tables must be performed with administrative privileges.

An advantage of the implementation as a user space process is the fact that multiple instances of OpenVPN can run simultaneously on the same host. Server and client instances can run side-by-side. Another advantage of a user space application is portability across multiple platforms. All the specific VPN functionality is portable, leaving only the generic low interfacing for each individual operating system.

OpenVPN builds a VPN on top of UDP or TCP. The use of standard higher-level protocols allows OpenVPN tunnels to be easily handled by traditional firewall and Network Address Translation (NAT) systems. The security model of OpenVPN can be divided into three parts:

1. mutual authentication of OpenVPN endpoints based on the TLS/SSL protocol;
2. a secure control channel to set up and manage VPN tunnels, that is multiplexed with:
3. a secure data channel to transport VPN tunnel payload using a dedicated protocol similar to IPsec's ESP.

2.1.1 Main differences between vanilla OpenVPN and OpenVPN-NL

The following are the most important differences between vanilla OpenVPN and OpenVPN-NL:

	vanilla OpenVPN	OpenVPN-NL
Maintainer	OpenVPN community	Fox-IT
Distribution channel	Various means	https://openvpn.fox-it.com, offline fingerprints

		available
Certification	None	NLNCSA criteria Level 2, "Dep. VERTROUWELIJK" (Dutch) if deployed in compliance with the Deployment Advisory
Functionality	Full	Many insecure and less secure options stripped, hardened, otherwise unchanged
Cryptographic library	OpenSSL	mbedTLS
Default encryption and message digest	BF-CBC + SHA1 (static) or AES-256-GCM (negotiated)	AES-256-CBC + SHA256 (static) or AES-256-GCM (negotiated) (no other options allowed)
Accepted moduli for RSA and DH	Various, including 1024 and 2048 bits	2048 bits (to be compliant with this advisory) ECDH recommended instead of DH
Accepted Elliptic curves	Various, including 112, 256 and 384 bit curves	secp256r1, secp384r1 (no other options allowed)

Apart from these differences, many things are the same. The functionality is for the most part identical. Vanilla OpenVPN and OpenVPN-NL are mutually compatible, in the sense that a client of the one can connect to a server of the other (given that a crypto suite is chosen which is available in both products). Configuration files can be freely exchanged (given that the options are available in both products). Both vanilla OpenVPN and OpenVPN-NL and underlying libraries are licensed under GPLv2.

OpenVPN-NL is fully compatible with the OpenVPN protocol, in particular no incompatibilities have been intentionally added.

2.2 System

The security of an OpenVPN-NL deployment depends on several factors:
- the security of the OpenVPN-NL software;
- the configuration of the OpenVPN-NL software;
- the security of the machines/OSes that run the OpenVPN-NL software;
- the security of the key management systems.

When one of these factors fails, the security of the whole deployment falls apart. Therefore this evaluation will take all these factors into consideration.

2.3 Components

OpenVPN-NL	a software product that is installed on a platform to provide a VPN service.
Configuration	settings for correct operation of OpenVPN and its platform, typically enumerated in a configuration file. Minimal

	configuration specifies whether an implementation acts as a client or a server.
mbedTLS	A software TLS implementation designed to have a small footprint. The mbedTLS library has been integrated into OpenVPN as part of the hardening, instead of using the much more complex OpenSSL implementation.
liblzo2	plugin software library that provides on-the-fly compression and decompression of packets before encryption and after decryption respectively. Though optional this is typically enabled for performance reasons. Use of compression is deprecated. This option will be removed in a later release.
pkcs11-helper	plugin software library that enables OpenVPN to use certificates from a smartcard (and performing cryptographic operations on the smartcard) rather than reading the certificates from a regular filesystem.

2.4 Infrastructure

Platform	host with an operating system (Linux and Windows are supported).
PKI	existing Public Key Infrastructure that provides the X.509 certificates needed to establish a connection between an OpenVPN client and server, OpenVPN can be run with an ad hoc PKI (this is not recommended when a suitable PKI at security level two according to the NLNCSA criteria is available).
Black IP network	the network that carries the VPN tunnels. This network is deemed "black" from the OpenVPN perspective.
Red IP network	protected network in situations where OpenVPN is used on a gateway to provide a secure connection to a remote network or host.

2.5 Classification

OpenVPN-NL is evaluated with the classification Restricted or "Dep. Vertrouwelijk" (DV) as reference, this corresponds with security level 2 as defined in the NLNCSA criteria. Parts of the system carry the following classifications:

Unclassified	OpenVPN sourcecode, IP network
Unclassified, but sensitive	Configuration, Platform without keys
Departementaal Vertrouwelijk	Platform with keys, red network

The source code for the vanilla OpenVPN is not classified and the patches for the hardened version will be donated to the OpenVPN project. Both should be regarded as known to potential attackers. Local configuration and hardening details should not be made public without an explicit need to do so.

2.6 Deployment scenario's

The evaluation investigates two primary scenario's: peer-to-peer configurations where a client and a server instance of OpenVPN form a single tunnel as peers, and hub spoke configurations where a concentrator acts as server for multiple clients. In the second scenario a red network behind the concentrator is implied. The peer-to-peer scenario includes cases where the peers are actually gateways between red networks, i.e. function as conventional IP crypto devices.

Alternate scenario's, that are not investigated in depth in this report, include deployment of OpenVPN as an add-on product on user machines to allow users to access restricted networks while simultaneously being openly connected to the black carrier network. This allows e.g. surfing the internet while simultaneously being connected to a restricted network. This mode of operation is called 'split tunneling'.

The use of split tunneling on a hostile network brings serious risks as attackers can easily target the host machine. Use of split tunneling on a trusted network (to build a tunnel between two endpoints in a trusted network) does not have these risks.

Split tunneling is not recommended unless it is used to create an exclusive channel over a trusted network.

The PKI infrastructure, that is used for authentication and session set up, is a vital part of the security offered by OpenVPN. Therefore private key material used in this phase needs to be protected. The OpenVPN software supports two modes: using smartcards to store the private key material and perform any operations with that key material – i.e. the private key material never leaves the smartcard – and using a software implementation that uses private key material stored on the filesystem.

Use of smartcards that store the private key material and perform all operations with this key material is recommended.

Use of private key material on the filesystem and/or operations on this key material in software are not recommended, unless the security mechanisms can be shown to offer equivalent security.

3 Level of protection

3.1 Criteria

NLNCSA has evaluated a hardened version of the OpenVPN code base according to the NLNCSA criteria for "Dep. Vertrouwelijk" (DV), in conjunction with attackers with a high attack potential. The choice for the high attack potential is based on the fact that OpenVPN is intended to provide communications security over public networks. An additional reason is the fact that the code base is known to attackers due to the fact that OpenVPN is open source and publicly available.

The criteria as used in this evaluation are: "NLNCSA Evaluation Criteria 2.0 for securing technology protecting NL classified information", 1 June 2013.

3.2 Evaluated security functions

The hardened version of OpenVPN has been evaluated as a component to provide communications security over public networks. This includes cases where OpenVPN is used as a drop in security measure.

As OpenVPN depends on the host platform for its own security and correct functioning, requirements for the platform have been investigated.

3.3 Absent or non-guaranteed security functions

Although the evaluation provides guidance and recommendations for deployment and requirements for the environment, e.g. regarding routing, firewall settings and assumptions about the PKI architecture, the quality of the implementation of these underlying mechanisms is not part of the evaluation proper. Though these aspects are not part of the evaluation, note that these functions are vital for the overall security of security solutions that incorporate OpenVPN-NL.

3.4 Disclaimer

The evaluation is not a complete code review. The hardening and documentation process carried out by Fox-IT is intended to minimize the need for such reviews.

The evaluation does not consider an actual deployment and therefore can only provide requirements and guidance on how to securely deploy OpenVPN-NL in generic terms. A user organization needs to perform its own assessment on systems that build on OpenVPN-NL or incorporate OpenVPN-NL. OpenVPN-NL is a building block, not a total security solution.

4 Conclusions

OpenVPN-NL is suitable as a building block for securing communication and access to systems up to the Dutch national classification level of "Dep. Vertrouwelijk", security level 2, given that the requirements detailed in this report are correctly implemented, notably that:

- the underlying platform is secure and configured such that OpenVPN is in charge of all incoming and outgoing traffic,
- a PKI conforming to security level two of the NLNCSA criteria is used for authentication.

Please note that while correct implementation of the requirements detailed in this report provides sufficient assurance, NLNCSA cannot guarantee the platform and its configuration without verification.

These conclusions are limited to the versions that are mentioned on the OpenVPN-NL download site, section "Lifecycle" (https://openvpn.fox-it.com/lifecycle.html). All advice from appendices 1 and 2 of this document is recommended. All deviations from this advice should be acknowledged and documented by the organisation that deploys OpenVPN-NL, to enable proper risk management.

This evaluation addresses the cases of *peer-to-peer* and *hub-spoke* networks. The conclusions for both scenario's are identical, with the caveat that in a hub-spoke network, the hub or concentrator may provide a high profile target for attacks. Hub-spoke networks sometimes consist of loosely managed platforms, i.e. the nodes on the spokes are likely not under direct control of the system administrators responsible for the hub and the VPN.

5 Important information for governmental organizations only

Governmental organizations considering taking advantage of OpenVPN-NL should contact the NLNCSA to obtain additional (security related) technical information about configuration and administration of the product. **These can be requested by sending an E-mail to the NBV-mailbox: NBV@MinBZK.NL.**
See "8 Technical appendices".

6 Guidance on policy and management

6.1 Risks that need to be accepted

OpenVPN-NL is a software product that relies on an operating system and its settings to function correctly. This means that the whole system is susceptible to bugs, configuration errors, incompatibilities between software components and unexpected interactions between hardware and software.
Although open source software means that there are many people identifying bugs and fixing them and various public audits are performed by other parties, it also implicates that attackers can study it in detail.

Paragraph 3.3 'Absent or Limited Security Features' and paragraph 3.4 'Disclaimer' contain a number of – unavoidable – limitations of the OpenVPN-NL and limitations of the evaluation. These limitations lead to residual risks and, before the product is used, informed choices will have to be made about this. The most important choice lies in balancing of the hardening and configuration of the host platform and functional requirements.

6.2 Distribution

An evaluation by the NLNCSA covers many aspects, including cryptographic aspects, source code inspection and supply chain control. The OpenVPN releases as found on the openvpn.net website or elsewhere on the net or the installation disk of various operating systems, though possibly of great protection value, cannot get an approval of the NLNCSA. The two most important reasons are:

1. The product allows many insecure configurations, including, but not limited to, turning off encryption, or the use of outdated cryptographic functions at security critical places.
2. Trust in the supply chain of the software is not guaranteed. The Dutch government cannot verify whether all the versions and releases 'out in the wild' are legitimate (i.e. secure and uncompromised) versions of OpenVPN. Please note that this list of reasons is not exhaustive.

To address these issues, NLNCSA has commissioned Fox-IT to create a special Dutch version of OpenVPN: OpenVPN-NL. Fox-IT has stripped and hardened the product, and has set up a controlled distribution channel on https://openvpn.fox-it.com. Fox-IT has acted as the maintainer and distributor of OpenVPN-NL under direction of the NLNCSA, and will do so for the foreseeable future.

OpenVPN-NL meets the evaluation criteria of the NLNCSA for handling classified information up to the level of "Dep. VERTROUWELIJK" (similar to the "RESTRICTED" classification as for example at NATO). Safe use of OpenVPN-NL requires compliance with the conditions set in this deployment advisory, published by the NLNCSA.

NLNCSA has evaluated the protection offered by the product against breaches of confidentiality and integrity. The evaluation has not included availability (e.g. robustness) of the VPN tunnel provided by OpenVPN-NL.

6.2.1 Practical actions

System administrators who wish to use OpenVPN-NL are advised to:

- Download the latest OpenVPN-NL for their platform from the website https://openvpn.fox-it.com;
- Verify the fingerprint of the downloaded package on the NLNCSA website: https://www.aivd.nl/organisatie/eenheden/nationaal-bureau/artikel/inzetadviezen/;
- Subscribe to the OpenVPN-NL mailinglist;
- Create a system which is in compliance with the requirements of this Deployment Advisory.
- Install OpenVPN-NL on this system in compliance with this Deployment Advisory.

6.2.2 New releases

The following events can trigger new releases:

- a new release of one of the packages on which OpenVPN-NL is based;
- a new release of one of the platforms for which OpenVPN-NL is packaged.

Releases which address security issues will be released as quickly as possible, other releases will be dealt with at a more planned pace.
In line with the mainstream OpenVPN policy, new releases of OpenVPN-NL will if anywhere possible, be backwards compatible in the sense that two different OpenVPN(-NL) releases can connect to one another (they do not break the protocol), and that new OpenVPN(-NL) releases can read the configuration files of older versions of OpenVPN(-NL).

6.2.2.1 Announcements

When a new release of OpenVPN-NL is available, this will always be announced by means of the OpenVPN-NL mailing list. This is a low-volume read-only mailing list for this purpose only. Announcements include a statement on whether the new release addresses security issues.

6.2.3 Lifecycle

A specific release of OpenVPN-NL for a platform is always in one of the following three states:

- *Current*: this release is up-to-date. This one is the recommended release for that platform.
- *Deprecated*: this is an old version of OpenVPN-NL for that platform, which is not up-to-date, but has no security issues. If a current version exists for the platform, that version is recommended for general reasons. There are no short term security-related reasons to advise against using an deprecated version.
- *Untrusted/insecure*: this is an old release of OpenVPN-NL, for which reasons exist to very strongly advise against using it.
  There are two typical cases:
  - The release which has become that much different from the current version of OpenVPN-NL, that it is no longer practical to determine whether a vulnerability found in a current (or deprecated) release applies to the old release.
  - The version has known vulnerabilities or is for other reasons sufficiently suspect to very strongly advise against using it.

The state of a release always moves down (from "Current" via "Deprecated" to "Untrusted"), and may skip the deprecated state. For example, a current release might directly become untrusted/insecure, skipping the deprecated state. A release in the deprecated state may (quickly) advance into the untrusted/insecure state.

On the OpenVPN-NL website, current and deprecated releases will be available for download, but untrusted/insecure versions and their corresponding source code will never be available for download. Untrusted/insecure versions or corresponding source code will also not be available via other channels from NLNCSA or Fox-IT.

Under all circumstances, NLNCSA advises to use a current OpenVPN-NL release. When system administrators depend on a specific release of OpenVPN, they should be aware that it may become untrusted/insecure at some time in the future and, therefore, no longer available for download. While work-arounds might exist which mitigate the vulnerabilities in a specific context to some extent, hanging on to an old code base is discouraged.

When an OpenVPN-NL release moves into the untrusted/insecure state, this will be announced on the OpenVPN-NL mailing list. This announcement will typically be complemented with the announcement of a new release.

6.3 Management

Management falls into three categories: management of OpenVPN itself, management of the platform that runs OpenVPN, and key management. The evaluation identifies the following requirements based on the evaluation results:

R_cryptosuite_1	Ciphers and cipher modes for use with OpenVPN: AES-256-CBC 256 bit key AES-256-GCM 256 key key Message digest for use with OpenVPN: SHA256 256 bit key TLS Ciphers for control channel: TLS-ECDHE-RSA-WITH-AES-GCM-SHA384, TLS-DHE-RSA-WITH-AES-GCM-SHA384 and TLS-DHE-RSA-WITH-AES-256-CBC-SHA (SSL-EDH-RSA-AES-256-SHA) with a 256 or 384-bit elliptic curve or 2048 bit moduli for both RSA and EDH
R_Public_Key_Infrastructure	OpenVPN must be configured to use an existing or ad hoc PKI implementation at security level two of the NLNCSA Criteria. This corresponds to "Departementaal Vertrouwelijk"
R_platform_1	The platform must be configured to monitor and log unexpected traffic or attempts to bypass routing and firewall rules.
R_platform_2	The platform must be hardened according to industry and government standards.
R_platform_3	The platform must be patched with all relevant security patches provided by the manufacturer.
R_platform_4	The platform must be configured to monitor and log unexpected traffic or attempts to bypass system policies.

R_configuration_1	OpenVPN must be configured to only allow the required cipher suites as outlined in this report as requirement R_cryptosuite_1.
R_configuration_2	OpenVPN must be configured to use the least amount of privileges needed to run.
R_routing_1	The platform's routing tables must preclude any route that bypasses OpenVPN.
R_firewall_1	The platform's firewall rules must preclude any traffic other than the traffic to and from OpenVPN or traffic required to let OpenVPN function.
R_firewall_2	The platform must only accept traffic from known peers in the VPN the platform belongs to.

Reference for these requirements is security level two according to the NLNCSA criteria. When any aspect of these requirements cannot be met, or not be met in full, in specific OpenVPN deployments, the responsible security officer should be consulted, who can relay specific questions to the NLNCSA.

6.4 Instructions for users

End-users of OpenVPN-NL generally need no additional instruction for the product itself as the operation of OpenVPN-NL is mostly transparent to end-users. End-users do need to be instructed on basic security aspects such as how to handle credentials – e.g. passwords, smartcards, certificates – needed to access the host that runs OpenVPN-NL, and how to start the VPN tunnel where needed. Instructing users on how to recognize correct behavior and where to report deviations or incidents, is recommended.

6.5 Use – general guidance

OpenVPN allows many settings to be determined at runtime. Some of the options have been eliminated as part of the hardening patches by Fox-IT. Using configuration files rather than command line options is recommended for deployment outside of test environments. These configuration files should be made read only and stored such that a minimum subset of processes can access these files.

Log files should likewise be protected from unnecessary access through restrictions on access rights for these files. Log levels should always be set as low as possible in the OpenVPN-NL configuration.

The use of UDP as the carrier protocol for OpenVPN is recommended, unless only TCP can be used.

Use of the TLS-AUTH option is mandatory, unless the TLS-CRYPT option is used. TLS-AUTH helps OpenVPN to determine whether packets are sent by legitimate peers or not, allowing them to drop packets immediately. This helps shield the software from traffic from unknown origin.

On top of the protection offered by TLS-AUTH, TLS-CRYPT encrypts the client- and server-certificates, preventing an attacker from learning the identities of the communicating parties. Using TLS-CRYPT provides a limited form of post-quantum security if the shared TLS-CRYPT secret is kept secret. The mechanism does not provide forward secrecy against quantum adversaries.

The use of compression at the level of OpenVPN-NL is discouraged. This feature will be removed in future versions of OpenVPN-NL.

The use of TUN or TAP devices for the virtual network device is at the user's discretion. This choice needs to be made for all VPN endpoints as TUN and TAP are mutually incompatible (they operate at different levels in the OSI stack).

6.5.1 Special attention for use of OpenVPN-NL in virtual environments

Users are advised to use hardware random number generators or entropy gathering daemons via the interfaces and conventions that the host offers. These feed into the system entropy pool. This is recommended on concentrators and systems that run in virtual environments.

Enabling the use-prediction-resistance configuration option is recommended. Note that this may deplete kernel entropy sources more quickly.
Users are advised not to adjust the configuration option min-platform-entropy below the value 10.

6.6 Incidents

Incidents can occur in the context of communication security and system security.

Communication security incidents imply the loss of security functionality of a single connection, this would be the case where an attacker gains access to key material of some kind or the encryption mechanisms fail.

The underlying PKI infrastructure is assumed to provide procedures for revocation of compromised smartcards.

System security incidents where an attacker gains access to the system that hosts OpenVPN are more serious. Unauthorized access may compromise the software or the operating system, which leads to complete breakdown of security. The requirements that pertain to monitoring of the system, its users, and the dataflow, help detect possible incidents early on.

7 OpenVPN-NL options

This appendix is meant as checklist for the network operator to create a proper configuration for a sufficient secure VPN connection. Only the security related options are listed here. The next paragraphs contain options that must be specified and options that should at least be considered to be included for further hardening the VPN. More information about the various options can be found in the public OpenVPN documentation (see https://openvpn.net).

7.1 Options required for OpenVPN-NL

The configuration of a secure OpenVPN-NL connection must at least specify the following options:

- --tls-auth (OpenVPN 2.1+) / tls-crypt OpenVPN 2.4+) *file number*
- --dh *file*
- --ca *file*
- --cert *file*
- --key *file*
- One of following options:
  - --remote-cert-tls client | server (--ns-cert-type is depricated)
  - --verify-x509-name name type (--tls-remote name is deprecated)

7.2 Recommended options

For further hardening the vpn at least following options should be considered to be part of the configuration:

Options related to the SSL-connection setup:

- --crl-verify

Options related to OpenVPN data/control connection:

- --user nobody
- --group nobody
- --chroot *dir*
- --block-outside-dns (Windows)

Options related to monitoring:

- --log *file*
- --log-append *file*
- --syslog
- --status
- --verb *number*
- --client-connect *script*
- --ipchange *script*
- --explicit-exit-notify
- It is further recommended not to use compression (--compress / -

8 References

[NIST 800-123]
NIST special publication 800-123 "Guide to General Server Security" July 2008

[Fox-IT documentation]
OpenVPN: high-level overview v0.9.1, 20 December 2010
OpenVPN - Security Overview v0.9.1, 3 January 2011
OpenVPN Test Plan v0.9, 20 December 2010
OpenVPN-NL System Design, v 1.3, 22 April 2018

OpenVPN: data channel control module v0.9, 20 December 2010
OpenVPN: data channel fragmentation module v0.9.1, 20 December 2010
OpenVPN: data channel crypto module v0.9.1, 20 December 2010
OpenVPN: data channel compression module v0.9.1, 20 December 2010
OpenVPN: external multiplexer v0.9.1, 20 December 2010
OpenVPN: internal multiplexer v0.9.1, 20 December 2010
OpenVPN: control channel processor module v0.9.1, 20 December 2010
OpenVPN: control channel reliability module v0.9.1, 20 December 2010
OpenVPN: control channel TLS module v0.9.1, 20 December 2010

PolarSSL Documentation – High Level Design, v0.9, 21 December 2010
PolarSSL Documentation – X.509 Module, v0.9, 21 December 2010
PolarSSL Documentation – Hashing Module, v0.9, 21 December 2010
PolarSSL Documentation – Random Number Generator Module, v0.9, 21 December 2010
PolarSSL Documentation – Symmetric Cipher Module, v0.9, 21 December 2010
PolarSSL Documentation – SSL/TLS Module, v0.9, 21 December 2010
PolarSSL Documentation – TCP/IP Module, v0.9, 21 December 2010
mbed TLS High Level Design, as published on tls.mbed.org on 19 April 2017

mbed TLS Module Level Designs, as published on tls.mbed.org on 19 April 2017
mbed TLS Doxygen generated reference manual v2.8.0
OpenVPN-NL Doxygen generated reference manual, v2.4.6

[OpenSSL]
OpenSSL homepage: http://www.openssl.org/

[PolarSSL/mbed TLS]
OpenSSL homepage: http://www.polarssl.org/
mbed TLS Homepage tls.mbed.org

[SSL random]
OpenSSL Function documentation:
http://www.openssl.org/docs/crypto/RAND_bytes.html
PolarSSL HAVEGE documentation:
http://www.irisa.fr/caps/projects/hipsor/publi.php

[lzo library]
The LZO homepage: http://www.oberhumer.com/opensource/lzo/

[Virtual tun/tap network device]
Project homepage: http://vtun.sourceforge.net/tun/index.html
OpenVPN specific information: http://openvpn.net/tuntap.html

9 Technical appendices

These are available for governmental organizations only.
Governmental organizations considering taking advantage of OpenVPN-NL should contact the NLNCSA to obtain additional (security related) technical information about configuration and administration of the product. **These can be requested by sending an E-mail to the NBV-mailbox: NBV@MinBZK.NL.**