
**Common Criteria Certification**
**BSI-DSZ-CC-xyz BSI-CC-PP-00zz**

# Security Target

**MAUVECORP MAUVEVPN CLIENT**
**Version 2.11**

MauveCorp
Fliederweg 98
D-50020 Köln
certification@mauvecorp.com

Document Version 1.0-SNAPSHOT
2022-09-13
[Commit cc54422 / main]

# Preface

The *MauveCorp MauveVPN Client* is evaluated according to the the protection profile *Schutzprofil: Anforderungen an den VPN Client* [BSI-CC-PP-00zz]…

# Contents

# List of Tables

# List of Figures

# 1. Introduction to the Security Target

The TOE described in this document is the *MauveVPN Client 2.11*. The TOE is a secure component used as a VPN client.

This document is the *security target*, which describes the functional and organizational security requirements of the TOE and its operating environment. This document is formally based on:

- *Schutzprofil: Anforderungen an den VPN Client* [BSI-CC-PP-00zz]

## 1.1. ST Reference

| | |
|---|---|
| Title of the document | Security Target / MauveVPN Client |
| Version of the document | 1.0-SNAPSHOT |
| Date of the document | 2022-09-13 |
| Author | Mauve Corporation |
| Editor | Mauve Corporation |

## 1.2. TOE Reference

| | |
|---|---|
| Target of evaluation | MauveVPN Client 2.11 |
| Version of the TOE | 2.11 |
| Manufacturer | Mauve Corporation |
| Assurance level | EAL3 extended by AVA_VAN.3, ADV_IMP.1, ADV_TDS.3, ADV_FSP.4, ALC_TAT.1, and ALC_FLR.2 („EAL3+“) |
| CC Version | 3.1 Release 5 |

## 1.3. TOE Overview

The target of evaluation is the MauveVPN Client 2.11. MauveVPN Client implements—conformant to [BSI-CC-PP-00zz]—the product type of a VPN router. The TOE deliverables are the TOE and its operating instructions. Thus the TOE fulfills the scope required in [BSI-CC-PP-00zz].

## 1.4. TOE description

The operating system of the MauveVPN Client is GNU/Linux. Parts of the operating system implement security requirements of the TOE and are SFR-enforcing.

### 1.4.1. Operation Environment of the TOE

### 1.4.2. Hardware of the MauveVPN Client

The TOE has custom made hardware…

### 1.4.3. Interfaces of theMauveVPN Client

#### Physical Interfaces

All interfaces of the MauveVPN Client are physically placed on the case of the device. The interfaces of the TOE are visible in the pictures in Figure **??**.

**PS.LAN** is the interface to the LAN…

**PS.WAN** is the interface to the WAN…

**PS.LED** represents the LEDs on the front of the case.

#### Logical Interfaces

The TOE provides the logical interfaces described in the protection profile [BSI-CC-PP-00zz]. They are repeated here.

**LS.LAN** is the TOE's interface to the local area network of the operating environment. In addition to the interfaces described in the protection profile, there are further protocol specific interfaces described here. Table 1.1 lists these logical interfaces.

**LS.WAN** is the TOE's interface to the wide area network of the operating environment, the Internet. In addition to the interfaces described in the protection profile, there are further protocol specific interfaces described here. Table 1.2 lists these logical interfaces.

**LS.LED** represents the logical interface to the display and the buttons of PS.LED.

| Label | Client/Server | Purpose of the interface |
|---|---|---|
| LI.LAN.Ether | — | media access |
| LI.LAN.IP | — | access to the Internet layer |
| LI.LAN.TCP | — | access to the transport layer |
| LI.LAN.TLS | server | transport security with TLS 1.2 |
| LI.LAN.UDP | — | access to the transport layer |
| LI.LAN.HTTP_MGMT | server | HTTP access to the management console |

Table 1.1.: Logical Interfaces on LI.LAN

| Label | Client/Server | Purpose of the interface |
|---|---|---|
| LI.WAN.Ether | — | media access |
| LI.WAN.IP | — | access to the Internet layer |
| LI.WAN.TCP | — | access to the transport layer |
| LI.WAN.NTP | client | Obtaining time |
| LI.WAN.DHCP | client | Obtaining IP addresses in the WAN |
| LI.WAN.UDP | — | access to the transport layer |
| LI.WAN.IPSec | — | VPN data traffic |

Table 1.2.: Logical Interfaces on LI.WAN

### 1.4.4. TOE Architecture and Functionalities

The TOE consists of the following subsystems:

**VPN Client** contains VPN functionalities such as enthält die VPN-Funktionen IPSec and IKE.

**NTP Client** synchronizes system time with an NTP server in the WAN.

**Protection** contains protection mechanisms for the TOE.

**Administration** provides the management functions of the TOE.

**Crypto Services** provides cryptographic functionalities.

**TLS-Server** creates TLS connections for the management console.

### 1.4.5. Physical Scope of the TOE

The physical scope of the TOE comprises the components listed in Table 1.3.

| Component | Description | Version |
|---|---|---|
| Firmware Image | The firmware of the TOE | 2.11 |
| Guidance Documentation | The guidance documentation describes the secure usage of the TOE | 2.11 |
| User Manual | The manual describes the functionalities and operating instructions of the TOE | 2.11 |

Table 1.3.: Physiscal Scope of the TOE

# 2. Conformance Claims

## 2.1. Common Criteria Conformance Claim

This Security Target claims conformance to the Common Criteria for Information Technology Security Evaluation version 3.1 according to Common Criteria, Version 3.1, Revision 5 and is

- CC Part 2 [CC Part 2] extended and
- CC Part 3 [CC Part 3] conformant.

## 2.2. Protection Profile Conformance Claim

This Security Target claims strict conformance to

- "*Schutzprofil: Anforderungen an den VPN Client*" [BSI-CC-PP-00zz]

This Security Target claims no conformance to any other Protection Profile.

## 2.3. Package Conformance Claim

The Protection Profile requires assurance level EAL3, augmented by the components listed in Table 2.1. This Security Target claims Conformance to exactly these packages. This conformance is refered to as „EAL3+“ and is package-augmented to EAL3.

| Paket | Erläuterung |
|---|---|
| AVA_VAN.5 | Resistance to attack potential „Enhanced-Basic“ |
| ADV_FSP.4 | Functional specification with complete summary |
| ADV_TDS.3 | Basic modular design |
| ADV_IMP.1 | Implementation representation of the TSF |
| ALC_TAT.1 | Well-defined development tools |
| ALC_FLR.2 | Flaw reporting procedures |

Table 2.1.: Augmentation of assurance level EAL3

## 2.4. Conformance Rationale

This Security Target claims strict Conformance to [BSI-CC-PP-00zz]. By this claim there are no contradictions to and inconsistencies with other Protection Profiles. This claim is based on the description

of the TOE type, the definition of the security problem and the security requirements. Furthermore, this Security Target claims Conformance to all Security Assurance Requirements (SARs) that are required by [BSI-CC-PP-00zz].

**TOE Type** The Protection Profile requires that the TOE be a VPN router. The present TOE is a VPN router.

**Definition of the security problem** The definition of the security problem, i. e. the threats, assumptions and organizational security policies are adopted from the Protection Profile [BSI-CC-PP-00zz].

**Objectives and Requirements** The security objectives and requirements are adopted from the Protection Profile. The operations fulfilled by this Security Target are marked clearly.

Chapter 5 describes the functional requirement extending CC Part 2 [CC Part 2]. There are no requirements that extend CC Part 3 [CC Part 3].

# 3. Definition Of The Security Problem

This section firstly describes the assets that the TOE must protect and which external entities interact with the TOE. Following that, we discuss the threats to the TOE, the organizational security polices that have to be considered, and the assumptions about the operating environment.

## 3.1. Assets

### 3.1.1. Assets of the TOE

The *assets* (resources and data), that are protected by the TOE, are described in the Protection Profile [BSI-CC-PP-00zz]. These assets are valid without modification.

### 3.1.2. Users of the TOE

The *external entities, subjects and objects* of the TOE are in described in [BSI-CC-PP-00zz]. *Users* are described in [BSI-CC-PP-00zz, Section 3.1.1]. The description holds without modification. The *subjects*, that interact on behalf of the user, are modelled in [BSI-CC-PP-00zz, Section 6.1.2]. This model is valid in this Security Target without moodification.

## 3.2. Threats

**T.WAN.Client**
The threat T.WAN.Client described in 3.2 of [BSI-CC-PP-00zz] is valid without modification.

**T.LAN.Admin**
The threat T.LAN.Admin described in 3.2 of [BSI-CC-PP-00zz] is valid without modification.

**T.Mani_Cert**
The threat T.Mani_Cert described in 3.2 of [BSI-CC-PP-00zz] is valid without modification.

**T.Mani_Time**
The threat T.Mani_Time described in 3.2 of [BSI-CC-PP-00zz] is valid without modification.

## 3.3. Organisational Security Policies

**OSP.Time_Service**
The organizational security policy OSP.Time_Service described in 3.3 of [BSI-CC-PP-00zz] is valid without modification.

**OSP.TLS**

The organizational security policy OSP.TLS described in 3.3 of [BSI-CC-PP-00zz] is valid without modification.

## 3.4. Assumptions

**A.Guidance**

The assumption A.Guidance described in 3.4 of [BSI-CC-PP-00zz] is valid without modification.

# 4. Objectives

## 4.1. Objectives of the TOE

**O.TLS_Crypto**
The objective O.TLS_Crypto described in 4.1.1 of [BSI-CC-PP-00zz] must be fulfilled.

**O.Protection**
The objective O.Protection described in 4.1.1 of [BSI-CC-PP-00zz] must be fulfilled.

**O.Admin**
The objective O.Admin described in 4.1.1 of [BSI-CC-PP-00zz] must be fulfilled.

**O.VPN_Auth**
The objective O.VPN_Auth described in 4.1.2 of [BSI-CC-PP-00zz] must be fulfilled.

**O.VPN_Integrity**
The objective O.VPN_Integrity described in 4.1.2 of [BSI-CC-PP-00zz] must be fulfilled.

**O.VPN_Conf**
The objective O.VPN_Conf described in 4.1.2 of [BSI-CC-PP-00zz] must be fulfilled.

**O.Time_Service**
The objective O.Time_Service described in 4.1.1 of [BSI-CC-PP-00zz] must be fulfilled.

**O.Cert_Check**
The objective O.Cert_Check described in 4.1.2 of [BSI-CC-PP-00zz] must be fulfilled.

## 4.2. Objectives for the environment of the TOE

**OE.Real_Time_Clock**
The objective OE.Real_Time_Clock described in 4.4 of [BSI-CC-PP-00zz] must be fulfilled.

## 4.3. Rationale for the Objectives of the TOE

### 4.3.1. Mapping Threats, OSPs and Assumptions to Objectives

The mapping of threats, OSPs and assumptions to objectives is the same as in the Protection Profile [BSI-CC-PP-00zz]. Table 4.1 is a rendition of the table in the Protection Profile.

### 4.3.2. Explanation of deviations from the Proctection Profile

For all unmodified relations that are taken from the Proctection Profile (marked with "✓" in Table 4.1), the explanations are valid in this Security Target.

| | O.Admin | O.Cert_Check | O.Protection | O.Time_Service | O.TLS_Crypto | O.VPN_Auth | O.VPN_Conf | O.VPN_Integrity | OE.Real_Time_Clock |
|---|---|---|---|---|---|---|---|---|---|
| T.WAN.Client | . | . | . | . | . | ✓ | ✓ | ✓ | . |
| T.LAN.Admin | ✓ | . | ✓ | . | ✓ | . | . | . | . |
| T.Mani_Cert | . | ✓ | . | . | . | . | . | . | . |
| T.Mani_Time | . | . | . | . | . | . | . | . | ✓ |
| OSP.TLS | . | . | ✓ | . | ✓ | . | . | . | . |
| OSP.Time_Service | . | . | . | . | . | . | . | . | ✓ |
| A.Guidance | . | . | . | . | . | . | . | . | . |

Table 4.1.: Mapping of objectives to threats, OSPs and assumptions

#### 4.3.2.1. Defense against the Threats by the Objectives

#### 4.3.2.2. Mapping of OSPs to Objectives

The mapping of organizational security policies to objectives in [BSI-CC-PP-00zz] is valid without modification.

#### 4.3.2.3. Mapping of Assumptions to Objectives

The mapping of assumptions to objectives in [BSI-CC-PP-00zz] is valid without modification.

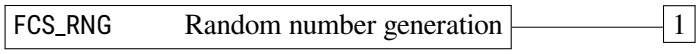
# 5. Definition of Extended Components

## 5.1. Definition of the extended family FCS_RNG

### Family Behaviour

This family defines requirements to the creation of random numbers that are used for cryptographic applications.

### Component Leveling




FCS_RNG.1 "random number generation" requires the identification of the type of the random number generator and a list of its security capabilities. A quality metric for the generated random numbers must be specified. The evaluation and processing of the random numbers has to rely upon this quality metric.

### Management: FCS_RNG.1

There are not management activities foreseen for this component.

### Audit: FCS_RNG.1

There are no events identified that must be audited, if FAU_GEN is part of the PP/ST.

**FCS_RNG.1**
**Random number generation**

| | |
|---|---|
| Hierarchical to: | No other component |
| Dependencies: | No dependencies |
| FCS_RNG.1.1 | The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: list of security capabilities]. |
| FCS_RNG.1.2 | The TSF shall provide random numbers that meet [assignment: a defined quality metric]. |

### Rationale for the introduction of the extended family

According to the definiton of OE.Real_Time_Clock in [BSI-CC-PP-00zz] the TOE is responsible for the generation of random numbers.

# 6. Security Requirements

## 6.1. Definitions

Most security requirements are adopted from the Protection Profile without modification. For those SFR that are adopted from the PP, the hierarchy and dependencies are not repeated in this Security Target. For SFRs (Security Functional Requirements) that are added in the ST, the information is given.

### 6.1.1. Notation

The typographic styles for the operations of the SFR are described in Table 6.1. Deletions in the ST are always accompanied by an explanation why the deletion is necessary.

| Source | Operation | Typographic Styles |
|---|---|---|
| PP | Assignment | Assignments made by the PP are typeset underlined. |
| | Selection | Selections made by the PP are typeset *italics and underlined*. |
| | Refinement | Refinments made by the PP are typeset **in bold face**. |
| | Deletion | Deletions made by the PP are typeset ~~**in bold face and struck through**~~. |
| ST | Assignment | Assignments made by the ST are typeset in blue colour and underlined. |
| | Selection | Selections made by the ST are typeset *in blue colour, italics and underlined*. |
| | Refinement | Refinments made by the ST are typeset **in blue colour and in bold face**. |
| | Deletion | Deletions made by the ST are typeset ~~**in blue colour, bold face and struck through**~~. |

Table 6.1.: Typographische Konventionen

### 6.1.2. Modelling of Subjects, Objects, Attributes and Operations

The modellings of the Protection Profile [BSI-CC-PP-00zz] are valid in this Security Target. In addition to these modellings, this Security Target assumes the subjects, objects, attributes and operations in Table 6.2.

| Subject | Description | Attribute |
|---|---|---|
| S_Administrator | Subject that acts for an administrator. | (none) |
| S_Time_Service | Subject that provides time. | (none) |

Table 6.2.: Subjects

## 6.2. Security Functional Requirements

### 6.2.1. VPN Client

#### FTP_ITC.1/VPN
**Inter-TSF trusted channel / VPN**

| | |
|---|---|
| FTP_ITC.1.1/VPN | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.1] are valid without modification. |
| FTP_ITC.1.2/VPN | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.1] are valid without modification. |
| FTP_ITC.1.3/VPN | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.1] are valid without modification. |

### 6.2.2. Network Services

#### FPT_STM.1
**Reliable time stamps**

| | |
|---|---|
| FPT_STM.1.1 | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.3] are valid without modification. |
| Refinement: | Reliability of time stamps is achieved by synchronisation of the real time clock (OE.Real_Time_Clock) with time servers using the NTPv4 protocol [RFC 5905]. The TOE uses the reliable time stamps for itself. |

#### FPT_TDC.1/Zert
**Inter-TSF basic TSF data consistency**

| | |
|---|---|
| FPT_TDC.1.1/Zert | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.3] are valid without modification. |
| FPT_TDC.1.2/Zert | The TSF shall use *interpretation rules* when interpreting the TSF data from another trusted IT product.<br>**The interpretation rules are defined in …** |

### 6.2.3. Stateful Packet Inspection

(This section intentionally left blank.)

### 6.2.4. Self Protection

#### FDP_RIP.1
**Subset residual information protection**

| | |
|---|---|
| FDP_RIP.1.1 | The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* |

| | |
|---|---|
| | the following objects: cryptographic keys (and session keys) used for the VPN or for TLS-connections, no other objects[1]. |
| Refinement: | Sensitive data muse be overwritten with constant or random values as soon as they are not in use anymore.<br>**These sensitive objects are overwritten with constant values.** |

### FPT_TST.1
**TSF testing**

| | |
|---|---|
| FPT_TST.1.1 | The TSF shall run a suite of self tests *during initial start-up, at the request of the authorised user*[2] to demonstrate the correct operation of *stored TSF executable code*[3]. |
| FPT_TST.1.2 | The TSF shall provide authorised users with the capability to verify the integrity of TSF data. |
| FPT_TST.1.3 | The TSF shall provide authorised users with the capability to verify the integrity of *the TSF*[4]. |

### FTP_TRP.1/Admin
**Trusted path**

| | |
|---|---|
| FTP_TRP.1.1/Admin | The TSF shall provide a communication path between itself and *local*[5] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure*[6]. |
| FTP_TRP.1.2/Admin | The TSF shall permit *local users*[7] to initiate communication via the trusted path. |
| FTP_TRP.1.3/Admin | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.6] are valid without modification. |
| ST Application Note 1 | The TOE supports mutual authentication with certificates in the TLS handshake. |

[1] Assignment: *list of objects*
[2] Selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*
[3] Selection: *[assignment: parts of TSF], the TSF*
[4] Selection: *[assignment: parts of TSF], the TSF*
[5] Selection: *remote, local*
[6] Selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*
[7] Selection: *the TSF, local users, remote users*

### 6.2.5. Cryptographic Services

#### FCS_COP.1/Hash
**Cryptographic operation**

FCS_COP.1.1/Hash

The TSF shall perform hash value calculation in accordance with a specified cryptographic algorithm ~~**SHA-1,**~~ SHA-256, SHA-512[8] and cryptographic key sizes none that meet the following: FIPS PUB 180-4 [FIPS PUB 180-4].

#### FCS_COP.1/HMAC
**Cryptographic operation**

FCS_COP.1.1/HMAC

The TSF shall perform HMAC value generation and verification in accordance with a specified cryptographic algorithm HMAC with ~~**SHA-1,**~~ SHA-256[9] and cryptographic key sizes 160 and 256 bit[10] that meet the following: FIPS PUB 180-4 [FIPS PUB 180-4], RFC 2404 [RFC 2404], RFC 4868 [RFC 4868], RFC 5996 [RFC 5996].

#### FCS_CKM.1
**Cryptographic key generation**

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm PRF-HMAC-SHA256[11] and specified cryptographic key sizes 256 bit[12] that meet the following: TR-03116 [TR-03116-1].

**The following algorithms and preferences are supported for TLS key negotiation**

- **Diffie-Hellman Group 14 according to RFC 3526 [RFC 3526] for key establishment during TLS**
- **DH exponent shall have a minimum length of 384 bits**
- **Forward secrecy shall be provided**
- **Ephemeral elliptic curve DH key exchange supports the P-256 and the P-384 curves according to FIPS186-4 [FIPS PUB 186-2] as well as the brainpoolP256r1 and the brainpoolP384r1 curves according to RFC 5639 and RFC 7027 [RFC 5639; RFC 7027]**
- **Peer authentication (if required): X.509 certificate with RSA 2048 bit keys**

[8] Assignment: *list of SHA-2 Algorithms with more than 256 bit size*
[9] Assignment: *list of SHA-2 Algorithms with 256bit size or more*
[10] Assignment: *cryptographic key sizes*
[11] Assignment: *cryptographic key generation algorithm*
[12] Assignment: *cryptographic key sizes*

### FCS_CKM.2/IKE
**Cryptographic key distribution / IKE**

| | |
|---|---|
| FCS_CKM.2.1/IKE | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.7] are valid without modification. |

### FCS_CKM.2/TLS
**Cryptographic key distribution / TLS**

| | |
|---|---|
| FCS_CKM.2.1/TLS | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.7] are valid without modification. |

### FCS_CKM.4
**Cryptographic key destruction**

| | |
|---|---|
| FCS_CKM.4.1 | The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method by overwriting with zeros[13] that meets the following: none[14]. |

## 6.2.6. TLS-Channels With Secure Cyptographic Algorithms

### FTP_ITC.1/TLS
**Inter-TSF trusted channel / TLS**

| | |
|---|---|
| FTP_ITC.1.1/TLS | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.8] are valid without modification. |
| FTP_ITC.1.2/TLS | The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.8] are valid without modification. |
| FTP_ITC.1.3/TLS | The TSF shall initiate communication via the trusted channel for communication required by the administration interface any connection specified in Table A.4.[15] |
| ST Application Note 2 | The TOE supports key exchange with elliptic curves.The supported curves are list in Table A.2. |

### FPT_TDC.1/TLS.Zert
**Inter-TSF basic TSF data consistency**

| | |
|---|---|
| FPT_TDC.1.1/TLS.Zert | The TSF shall provide the capability to consistently interpret<br>(1) X.509 certificates for TLS connections<br>(2) Revocation information for certificates for TLS connections received via OCSP. |

[13] Assignment: *cryptographic key destruction method*
[14] Assignment: *list of standards*
[15] Assignment: *list of other functions for which a trusted channel is required*

(3) no other data types[16]

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/TLS.Zert — The TSF shall use *interpretation rules* when interpreting the TSF data from another trusted IT product.

### FCS_COP.1/TLS.AES
**Cryptographic operation**

FCS_COP.1.1/TLS.AES — The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.8] are valid without modification.

### FCS_COP.1/TLS.Auth
**Cryptographic operation for TLS**

FCS_COP.1.1/TLS.Auth — The requirements defined in [BSI-CC-PP-00zz, Abschnitt 6.2.8] are valid without modification.

## 6.2.7. Additional Requirements

This section contains security requirements that are defined in addition to the Protection Profile. The requirements are extended by the component FCS_RNG.1/Hash_DRBG defined in Chapter 5.1.

### FCS_RNG.1/Hash_DRBG
**Zufallszahlenerzeugung**

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RNG.1.1/Hash_DRBG — The TSF shall provide a *deterministic*[17] random number generator that implements: [18]

(1) If initialized with a random seed using PTRNG of class PTG.2 as random source, the internal state of the RNG shall have at least 100 bits min-entropy.

(2) The RNG provides forward secrecy.

(3) The RNG provides backward secrecy even if the current internal state is known.

FCS_RNG.1.2/Hash_DRBG — The TSF shall provide random numbers that meet: [19]

[16] Assignment: *additional list of data types*
[17] Selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*
[18] Assignment: *list of security capabilities*
[19] Assignment: *a defined quality metric*

(1) The RNG gets initialized during every startup and after 2048 requests with a random seed of minimal 384 bits using a PTRNG of class PTG.2. The RNG generates output for which more than $2^{34}$ strings of bit length 128 are mutually different with probability $w > 1 - 2^{(-16)}$.

(2) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.

## 6.3. Security Assurance Requirements for the TOE

The security assurance requirements for the TOE are defined in the Protection Profile [BSI-CC-PP-00zz].

## 6.4. Security Requirements Rationale

### 6.4.1. Overview of the coverage of SFR

This Security Target adopts the mapping of objectives to SFR as defined in the Protection Profile. Table 6.3 shows these relations.

| | O.Admin | O.Cert_Check | O.Protection | O.Time_Service | O.TLS_Crypto | O.VPN_Auth | O.VPN_Conf | O.VPN_Integrity |
|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1 | . | . | . | . | ✓ | ✓ | ✓ | ✓ |
| FCS_CKM.2/IKE | . | . | . | . | . | ✓ | ✓ | ✓ |
| FCS_CKM.2/TLS | . | . | . | . | ✓ | . | . | . |
| FCS_CKM.4 | . | . | . | . | ✓ | ✓ | ✓ | ✓ |
| FCS_COP.1/Hash | . | ✓ | . | . | . | . | . | . |
| FCS_COP.1/HMAC | . | ✓ | . | . | . | . | . | . |
| FCS_COP.1/TLS.AES | . | . | . | . | ✓ | . | . | . |
| FCS_COP.1/TLS.Auth | . | . | . | . | ✓ | . | . | . |
| FCS_RNG.1/Hash_DRBG | . | . | . | . | ✓ | ✓ | ✓ | ✓ |
| FDP_RIP.1 | . | . | ✓ | . | . | . | . | . |
| FPT_TDC.1/TLS.Zert | . | . | . | . | ✓ | . | . | . |
| FPT_TDC.1/Zert | . | ✓ | . | . | . | . | . | . |
| FPT_STM.1 | . | . | . | ✓ | . | . | . | . |
| FPT_TST.1 | . | . | ✓ | . | . | . | . | . |
| FTP_ITC.1/TLS | . | . | . | . | ✓ | . | . | . |
| FTP_ITC.1/VPN | . | . | . | . | . | ✓ | ✓ | ✓ |
| FTP_TRP.1/Admin | ✓ | . | . | . | ✓ | . | . | . |

Table 6.3.: Mapping of objectives to SFR

### 6.4.2. SFR Dependency Rationale

The dependencies of the security functional requirements in Section 6.2 are fulfilled. This Security Target assumes the same resolutions as defined in the Protection Profile in [BSI-CC-PP-00zz][Section 6.4.2].

The extended component FCS_RNG.1 defined in Section 5.1 has no dependencies that need to be resolved.

Table 6.4 and Table 6.5 show the relations of the subjects defined in Table 6.2 to the SFR.

| | FCS_CKM.1 | FCS_CKM.2/IKE | FCS_CKM.2/TLS | FCS_CKM.4 | FCS_COP.1/Hash | FCS_COP.1/HMAC | FCS_COP.1/TLS.AES | FCS_COP.1/TLS.Auth | FCS_RNG.1/Hash_DRBG | FDP_RIP.1 | FPT_TDC.1/TLS.Zert | FPT_TDC.1/Zert | FPT_STM.1 | FPT_TST.1 | FTP_ITC.1/TLS | FTP_ITC.1/VPN | FTP_TRP.1/Admin |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S_Administrator | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | ✓ |
| S_Time_Service | . | . | . | . | . | . | . | . | . | . | . | . | ✓ | . | . | . | . |

Table 6.4.: Mapping of subjects to SFR

| | S_Administrator | S_Time_Service |
|---|---|---|
| FCS_CKM.1 | . | . |
| FCS_CKM.2/IKE | . | . |
| FCS_CKM.2/TLS | . | . |
| FCS_CKM.4 | . | . |
| FCS_COP.1/Hash | . | . |
| FCS_COP.1/HMAC | . | . |
| FCS_COP.1/TLS.AES | . | . |
| FCS_COP.1/TLS.Auth | . | . |
| FCS_RNG.1/Hash_DRBG | . | . |
| FDP_RIP.1 | . | . |
| FPT_TDC.1/TLS.Zert | . | . |
| FPT_TDC.1/Zert | . | . |
| FPT_STM.1 | . | ✓ |
| FPT_TST.1 | . | . |
| FTP_ITC.1/TLS | . | . |
| FTP_ITC.1/VPN | . | . |
| FTP_TRP.1/Admin | ✓ | . |

Table 6.5.: Mapping of SFR to subjects

## 6.5. Rationale for the selected EAL

The rationale for the selected EAL is adopted from the Protection Profile.

# 7. TOE Summary Specification

This chapter provides an overview of the TOE's IT security functionalities as described in the Functional Specification. It contains descriptions of the general technical processes the TOE uses to fulfill the security requirements.

Section 7.7 shows the relation between the security functionalities of the TOE and the SFR in a tabular form.

## 7.1. VPN Client (SF.VPN)

The security function SF.VPN provides secure communication channels between the TOE and a remote trusted IT product.

| Implemented SFR | |
|---|---|
| FTP_ITC.1/VPN | FCS_CKM.2/IKE |

Certificates are mathematically checked and validated against a PKI (Public Key Infrastructure).

| Implemented SFR |
|---|
| FPT_TDC.1/Zert |

## 7.2. Network Services (SF.NetworkServices)

The security function SF.NetworkServices provides reliable time stamps to the TOE. A reference time is received from a trusted NTP server via NTP in version 4 [RFC 5905]. The deviation between network time and local time must not exceed 10 minutes. If the deviation is bigger, the TOE will terminate the connection. The TOE uses time stamps to check the validity of certificates.

| Implemented SFR |
|---|
| FPT_STM.1 |

## 7.3. Self Protection (SF.SelfProtection)

The security function SF.SelfProtection is responsible to protect the TOE and its data from manipulation.

Sensitive data are deleted from memory as soon as they are not used anymore. This comprises cryptographic keys, ephemeral keys, session keys, and sensitive user data. Deletion is conducted overwriting memory areas with constant values.

| Implemented SFR |
|---|
| FDP_RIP.1 |

The TOE can run a number of self tests to verify its integrity and and the functionality of itself and its components. Tests are run automatically at boot up. The administrator can run the tests at any time.

| Implemented SFR |
| --- |
| FPT_TST.1 |

## 7.4. Administration (SF.Administration)

The security functions define the role *Administrator*. Users with the role *Administrator* access the TOE via a mutually authenticated TLS connection. This connection is provided by SF.CryptographicServices bereit gestellt. Upon authentication, administrators are authorized to configure TSF parameters and run TSF-related operations:

- Modify the clock
- Run self-tests (cf. SF.SelfProtection)

The TOE informs the administrator about critical operational states with the LEDs on the front of the case (PS.LED).

| Implemented SFR |
| --- |
| FTP_TRP.1/Admin |

## 7.5. Cryptographic Services (SF.CryptographicServices)

The security function SF.CryptographicServices provides implementations of cryptographic algorithms that can be used by other TSF.

### Key Management

The SF provides algorithms for creation, distribution and destruction of cryptographic keys. und Vernichtung von Schlüsseln zur Verfügung.

| Implemented SFR |
| --- |
| FCS_CKM.1 FCS_CKM.4 |

### Random Numbers

The TOE contains a DRNG according to FCS_RNG.1/Hash_DRBG to create random numbers of high quality. The random numbers generated by the SF are used for TLS establishing connections (FCS_CKM.1 and FCS_COP.1/TLS.AES).

| Implemented SFR |
| --- |
| FCS_RNG.1/Hash_DRBG |

### Hash-Algorithms

The SF provides implementations for hash algorithms SHA-256 and SHA-512.

| Implemented SFR |
| --- |
| FCS_COP.1/Hash |

### HMAC Generation

The SF provides algorithms for HMAC generation with HMAC-SHA-256(-128).

| Implemented SFR |
| --- |
| FCS_COP.1/HMAC |

## 7.6. TLS Service (SF.TLS)

The TOE provides an implementation of the TLS protocol in version 1.2. The SF ensures the integrity and confidentiality of connections to the administrator's web browser. Table A.4 on page 34 lists all parameters and connections.

| Implemented SFR | | |
| --- | --- | --- |
| FTP_ITC.1/TLS | FCS_COP.1/TLS.AES | FCS_CKM.2/TLS |

The SF SF.CryptographicServices provides algorithms for signature verification. X.509 certificates are validated with RSA-PKCS1-v1.5 or RSASSA-PSS.

| Implemented SFR | |
| --- | --- |
| FPT_TDC.1/TLS.Zert | FCS_COP.1/TLS.Auth |

## 7.7. Relation of SFR to SF

Table 7.1 shows the relation between the SFR defined in Section 6.2 and the SF defined in this chapter.

| | SF.Administration | SF.CryptographicServices | SF.NetworkServices | SF.SelfProtection | SF.TLS | SF.VPN |
|---|---|---|---|---|---|---|
| FCS_CKM.1 | . | ✓ | . | . | . | . |
| FCS_CKM.2/IKE | . | . | . | . | . | ✓ |
| FCS_CKM.2/TLS | . | . | . | . | ✓ | . |
| FCS_CKM.4 | . | ✓ | . | . | . | . |
| FCS_COP.1/Hash | . | ✓ | . | . | . | . |
| FCS_COP.1/HMAC | . | ✓ | . | . | . | . |
| FCS_COP.1/TLS.AES | . | . | . | . | ✓ | . |
| FCS_COP.1/TLS.Auth | . | . | . | . | ✓ | . |
| FCS_RNG.1/Hash_DRBG | . | ✓ | . | . | . | . |
| FDP_RIP.1 | . | . | . | ✓ | . | . |
| FPT_TDC.1/TLS.Zert | . | . | . | . | ✓ | . |
| FPT_TDC.1/Zert | . | . | . | . | . | ✓ |
| FPT_STM.1 | . | . | ✓ | . | . | . |
| FPT_TST.1 | . | . | . | ✓ | . | . |
| FTP_ITC.1/TLS | . | . | . | . | ✓ | . |
| FTP_ITC.1/VPN | . | . | . | . | . | ✓ |
| FTP_TRP.1/Admin | ✓ | . | . | . | . | . |

Table 7.1.: Mapping of SFR to SF

# A. TLS Connections

The Protection Profiles defines the cipher suites required for TLS connections. The TOE uses provides exactly those cipher suites and no other. Table A.1 lists these cipher suites. Table A.2 lists the elliptic curves used for ECDHE.

| Algorithmen / Cipher Suite | IANA ID | TLS 1.2 [RFC 5246] |
|---|---|---|
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA | 0x00,0x33 | ✓ |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA | 0x00,0x39 | ✓ |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | 0xc0,0x13 | ✓ |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | 0xc0,0x14 | ✓ |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | 0xc0,0x27 | ✓ |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | 0xc0,0x28 | ✓ |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | 0xc0,0x2f | ✓ |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | 0xc0,0x30 | ✓ |

Table A.1.: Cipher suites for TLS connections

| Elliptic curve | IANA ID | Standard |
|---|---|---|
| secp256r1 (P-256) | 23 | [RFC 8422; ANSI X9.62] |
| secp384r1 (P-384) | 24 | [RFC 8422; ANSI X9.62] |
| brainpoolP256r1 | 26 | [RFC 7027] |
| brainpoolP384r1 | 27 | [RFC 7027] |

Table A.2.: Elliptic curves for TLS connections

The TOE communicates with other trusted IT products over secure connections. Integrity and confidentiality of these connections is ensured by TLS v1.2. Table A.4 lists all connections the TOE can participate in. Table A.3 describes the columns of this table.

| Column | Descriptions |
|---|---|
| ID | Smybolic name of this connection |
| Interface | Logical interface whose communication is secured. |
| Role | Describes client/serer role of the TOE. |
| Peer | Describes the peer in this TLS connection. |
| Protocol | Application protocol used in this connection. |
| Subsystem::Module | Name of the subsystem and the module from which the connection originates or that accepts the connections. |
| Port | IP-Port that the TOE opens for the connection. If the TOE is client, “dyn.” stands for ephemeral port assignment. “config” stands for a confgurable port number. |
| Identity of TOE | Certificate that the TOE uses to authenticate itself to the peer. |
| Identity of Peer | Certificate that the peer uses to authenticate itself to the TOE. |
| Authentication by | Process, data source or subsystem/module used by the TOE for authentication/verification. |

Table A.3.: Legend for TLS connections

| ID | Interface (protocol) | Role | Peer | Subsystem::Module | Port | Identity of TOE | Identity of Peer | Authentication by |
|---|---|---|---|---|---|---|---|---|
| TLS.1 | LI.LAN.HTTP_MGMT | Server | Browser | Administration::HTTP-Server | 443 | Certificate from Mauve CA | Username/password | User administration in TOE |

Table A.4.: TLS connections of MauveVPN Client

# Bibliography

## Protection Profiles And Technical Guidelines


[BSI-CC-PP-00zz] Bundesamt für Sicherheit in der Informationstechnik. *Schutzprofil: Anforderungen an den VPN Client. BSI-CC-PP-00zz*. Common Criteria Schutzprofil (Protection Profile). Version 1.1. Bundesamt für Sicherheit in der Informationstechnik (BSI), Feb. 5, 2020.

[TR-03116-1] Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 1: Telematikinfrastruktur*. Technische Richtlinie BSI TR-03116-1. Technical Guideline. Version 3.20. Bundesamt für Sicherheit in der Informationstechnik (BSI), Sept. 21, 2018. URL: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html.


## Standards


[ANSI X9.62] Accredited Standards Committee X9. *ANSI X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*. Standard. ANSI, Nov. 16, 2005.

[CC Part 2] The Common Criteria Recognition Agreement Members. *Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components*. Common Criteria. Version 3.1R5. Common Criteria Portal, Apr. 2017. URL: http://www.commoncriteriaportal.org/thecc.html.

[CC Part 3] The Common Criteria Recognition Agreement Members. *Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components*. Common Criteria. Version 3.1R5. Common Criteria Portal, Apr. 2017. URL: http://www.commoncriteriaportal.org/thecc.html.

[FIPS PUB 180-4] National Institute of Standards and Technology. *Secure Hash Standard (SHS)*. Federal Information Processing Standards Publication. Information Technology Laboratory, Aug. 2015. URL: http://dx.doi.org/10.6028/NIST.FIPS.180-4.

[FIPS PUB 186-2] National Institute of Standards and Technology. *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication. Information Technology Laboratory, July 2013. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

## RFC


[RFC 2404] C. Madson and R. Glenn. *The Use of HMAC-SHA-1-96 within ESP and AH*. RFC 2404 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Nov. 1998. DOI: 10.17487/RFC2404. URL: https://www.rfc-editor.org/rfc/rfc2404.txt.

[RFC 3526] T. Kivinen and M. Kojo. *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*. RFC 3526 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, May 2003. DOI: 10.17487/RFC3526. URL: https://www.rfc-editor.org/rfc/rfc3526.txt.

[RFC 4868] S. Kelly and S. Frankel. *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*. RFC 4868 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, May 2007. DOI: 10.17487/RFC4868. URL: https://www.rfc-editor.org/rfc/rfc4868.txt.

[RFC 5246] T. Dierks and E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246 (Proposed Standard). RFC. Updated by RFCs 5746, 5878, 6176, 7465, 7507, 7568, 7627, 7685, 7905, 7919. Fremont, CA, USA: RFC Editor, Aug. 2008. DOI: 10.17487/RFC5246. URL: https://www.rfc-editor.org/rfc/rfc5246.txt.

[RFC 5639] M. Lochter and J. Merkle. *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*. RFC 5639 (Informational). RFC. Fremont, CA, USA: RFC Editor, Mar. 2010. DOI: 10.17487/RFC5639. URL: https://www.rfc-editor.org/rfc/rfc5639.txt.

[RFC 5905] D. Mills et al. *Network Time Protocol Version 4: Protocol and Algorithms Specification*. RFC 5905 (Proposed Standard). RFC. Updated by RFC 7822. Fremont, CA, USA: RFC Editor, June 2010. DOI: 10.17487/RFC5905. URL: https://www.rfc-editor.org/rfc/rfc5905.txt.

[RFC 5996] C. Kaufman et al. *Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 5996 (Proposed Standard). RFC. Obsoleted by RFC 7296, updated by RFCs 5998, 6989. Fremont, CA, USA: RFC Editor, Sept. 2010. DOI: 10.17487/RFC5996. URL: https://www.rfc-editor.org/rfc/rfc5996.txt.

[RFC 7027] J. Merkle and M. Lochter. *Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)*. RFC 7027 (Informational). RFC. Fremont, CA, USA: RFC Editor, Oct. 2013. DOI: 10.17487/RFC7027. URL: https://www.rfc-editor.org/rfc/rfc7027.txt.

[RFC 8422] Y. Nir, S. Josefsson, and M. Pegourie-Gonnard. *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*. RFC 8422 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Aug. 2018. DOI: 10.17487/RFC8422. URL: https://www.rfc-editor.org/rfc/rfc8422.txt.

# List of ST Application Notes

# Glossary

**PKI** Public Key Infrastructure 28

**SFR** Security Functional Requirement 19

# Index of SFR