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

Security Target

MAUVECORP MAUVEVPN CLIENT
Version 2.11

MauveCorp
Fliederweg 98
50020 Köln
certification@mauvecorp.com

Dokumentversion 1.0-SNAPSHOT
[Commit 7d63d7c / master]
2020-03-02

Vorwort

Die vorliegende *MauveCorp MauveVPN Client* wird nach dem Schutzprofil *Schutzprofil: Anforderungen an den VPN Client* [BSI-CC-PP-00zz] zertifiziert…

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einführung in das Security Target

Der TOE, der in diesem Dokument beschrieben wird, ist der *MauveVPN Client 2.11*. Der TOE ist eine sichere Komponente, die als MauveVPN Client eingesetzt wird.

Dieses Dokument ist das *Security Target*, in dem die funktionalen und organisatorischen Sicherheitsanforderungen des TOE und seiner Einsatzumgebung beschrieben werden. Dieses Dokument findet seine formale Grundlage in:

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

1.1. ST Referenz

Titel des Dokuments	Security Target / MauveVPN Client
Version des Dokuments	1.0-SNAPSHOT
Datum des Dokuments	2. März 2020
Allgemeiner Status:	
Autor	Mauve Corporation
Editor	

1.2. TOE Referenz

Evaluierungsgegenstand	MauveVPN Client 2.11
Version des EVG	2.11
Hersteller	Mauve Corporation
Vertrauenswürdigkeitsstufe	EAL3 erweitert um AVA_VAN.3, ADV_IMP.1, ADV_TDS.3, ADV_FSP.4, ALC_TAT.1, and ALC_FLR.2 (Kurzbezeichnung „EAL3+“)
CC Version	3.1 Release 5

1.3. Überblick über den TOE

Der Evaluierungsgegenstand ist der MauveVPN Client 2.11.

Der Lieferumfang des TOE umfasst ebenfalls die Betriebsdokumentation für MauveVPN Client. Somit entspricht der TOE dem im Schutzprofil [BSI-CC-PP-00zz] genannten Umfang und Aufbau.

1.3.1. TOE Typ

MauveVPN Client implementiert – konform zu [BSI-CC-PP-00zz] – den Produkttyp eines VPN-Routers.

1.3.2. Verwendung und Hauptfunktionalität des TOE

1.3.3. Erforderliche Non-TOE Hardware/Software/Firmware

1.4. Beschreibung des TOE

1.4.1. Hauptziele des TOE

1.4.2. Aufbau des TOE

Das Betriebssystem des MauveVPN Client ist GNU/Linux. Teile des Betriebssystems setzen Sicherheitsanforderungen an den TOE um und sind somit SFR-enforcing.

1.4.3. Einsatzumgebung des TOE

1.4.4. Hardware des MauveVPN Client

1.4.5. Schnittstellen des MauveVPN Client

1.4.5.1. Physische Schnittstellen

Alle Schnittstellen des thisproduct sind physisch am Gehäuse des Geräts untergebracht. Die außen sichtbaren Schnittstellen sind auf dem Foto des TOE in Abbildung **??** zu erkennen.

PS.LAN ist die Schnittstelle ins LAN…

PS.WAN ist die Schnittstelle ins WAN…

PS.LED repräsentiert die LEDs an der Außenseite des Geräts.

1.4.5.2. Logische Schnittstellen

Der TOE verfügt über die logischen Schnittstellen, die das Schutzprofil [BSI-CC-PP-00zz] beschreibt. Diese werden hier der besseren Lesbarkeit halber wiederholt.

LS.LAN ist die Schnittstelle des TOE ins lokale Netzwerk der Einsatzumgebung. Zusätzlich zu den im Schutzprofil genannten Schnittstellen werden hier weitere protokollspezifische Schnittstellen definiert. Tabelle 1.1 listet diese logischen Schnittstellen.

LS.WAN ist die Schnittstelle des TOE zum WA. Verschiedene Protokolle implementieren weitere Logische Schnittstellen in Richtung des WAN. Tabelle 1.2 listet diese logischen Schnittstellen.

LS.LED repräsentiert die logische Schnittstelle zum Display und den Bedienknöpfen über PS.LED.

Bezeichner	Rolle	Zweck der Schnittstelle
LS.LAN.Ether	—	Protokoll auf Zugangsschicht
LS.LAN.IP	—	Zugang zur Internet-Schicht
LS.LAN.TCP	—	Zugang zur Transportschicht
LS.LAN.TLS	beide	Sicherung der Verbindung mit TLS 1.2
LS.LAN.UDP	—	Zugang zur Transportschicht
LS.LAN.HTTP_MGMT	Server	HTTP-Zugriff auf Managementschnittstelle

Tabelle 1.1.: Logische Schnittstellen an LS.LAN

Bezeichner	Rolle	Zweck der Schnittstelle
LS.WAN.Ether	—	Protokoll auf Zugangsschicht
LS.WAN.IP	—	Zugang zur Internet-Schicht
LS.WAN.NTP	Client	Abruf der Uhrzeit
LS.WAN.DHCP	Client	Adressbezug im WAN
LS.WAN.TCP	—	Zugang zur Transportschicht
LS.WAN.UDP	—	Zugang zur Transportschicht
LS.WAN.IPSec	—	VPN Datenverkehr

Tabelle 1.2.: Logische Schnittstellen an LS.WAN

1.4.6. Aufbau und physische Abgrenzung des TOE

Der TOE besteht aus folgenden Subsystemen:

VPN Client enthält die VPN-Funktionen wie IPSec und IKE.

NTP Client synchronisiert die Systemzeit mit einem Zeitserver.

Protection enthält Schutzmechanismen für den TOE.

Administrationssystem wird für die Administration des TOE verwendet.

Kryptodienste bietet kryptografische Basisfunktionen.

TLS-Server erstellt TLS-Verbindungen für die Administrationsschnittstelle.

1.4.7. Logische Abgrenzung: Vom TOE erbrachte Sicherheitsdienste

1.4.8. Physischer Umfang des TOE

Der physische Umfang des TOE umfasst die in Tabelle 1.3 aufgelisteten Komponenten.

Komponente	Beschreibung	Version
Firmware Image	Die Firmware des TOE	2.11
Guidance Documentation („Administrationshandbuch“)	Die Guidance Documentation beschreibt die sichere Verwendung des TOE	2.11
Benutzerhandbuch („Allgemeine Gebrauchsanleitung MauveVPN Client“)	Das Benutzerhandbuch beschreibt die allgemeine Verwendung, sowohl dessen TOE Anteile als auch die nicht-TOE Anteile	2.11

Tabelle 1.3.: Physischer Umfang des TOE

2. Postulat der Übereinstimmung

2.1. Konformität zu Common Criteria

Das Security Target wurde gemäß Common Criteria, Version 3.1, Revision 5, erstellt und ist

- CC Part 2 [CC Part 2] erweitert (extended) und
- CC Part 3 [CC Part 3] konform (conformant).

2.2. Konformität zu Schutzprofilen

Dieses Security Target behauptet strikte Konformität zu:

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

Dieses Security Target behauptet keine Konformität zu weiteren Schutzprofilen.

2.3. Konformität zu Paketen

Das Schutzprofil fordert die Vertrauenswürdigkeitsstufe EAL3, erweitert um die Komponenten in Tabelle 2.1. Dieses Security Target behauptet Konformität zu genau diesen Paketen. Diese Konformität wird als „EAL3+“ bezeichnet und ist somit „package-augmented“ gegenüber EAL3.

Paket	Erläuterung
AVA_VAN.5	Resistenz gegen Angriffspotential „Enhanced-Basic“
ADV_FSP.4	Vollständige Funktionale Spezifikation
ADV_TDS.3	Einfaches Modulares Design
ADV_IMP.1	TSF-Implementierung
ALC_TAT.1	Wohldefinierte Entwicklungswerkzeuge
ALC_FLR.2	Verfahren für Problemreports

Tabelle 2.1.: Ergänzungen zur Vertrauenswürdigkeit EAL3

2.4. Erklärung der Konformität

Dieses Security Target behauptet strikte Konformität zu [BSI-CC-PP-00zz]. Durch diese Feststellung sind Widersprüche und Inkonsistenzen zu anderen Schutzprofilen ausgeschlossen. Diese Behauptung basiert auf der Betrachtung des TOE Typs, der Definition des Sicherheitsproblems und schließlich

der Sicherheitsziele sowie der Sicherheitsanforderungen. Weiterhin behauptet dieses Security Target Konformität zu allen Security Assurance Requirements (SARs), die von [BSI-CC-PP-00zz] gefordert werden.

TOE Typ Das Schutzprofil fordert, dass der TOE ein …ist. Der vorliegende TOE ist ein…

Definition des Sicherheitsproblems Die Definition des Sicherheitsproblems, d. h. die Bedrohungen, Annahmen und die organisatorischen Sicherheitspolitiken sind direkt aus dem Schutzprofil [BSI-CC-PP-00zz] übernommen.

Sicherheitsziele und Sicherheitsanforderungen Die Sicherheitsziele und Sicherheitsanforderungen sind dem Schutzprofil [BSI-CC-PP-00zz] entnommen. Die Operationen an den SFR sind deutlich gekennzeichnet.

Kapitel 5 bescheibt die über CC Teil 2 [CC Part 2] hinausgehenden funktionalen Anforderungen an die Vertrauenswürdigkeit. Es werden keine Anforderungen definiert, die über CC Teil 3 [CC Part 3] hinausgehen.

3. Definition des Sicherheitsproblems

In diesem Abschnitt wird zunächst beschrieben, welche Werte der TOE schützen muss, welche externen Einheiten mit ihm interagieren und welche Objekte von Bedeutung sind. Auf dieser Basis wird danach beschrieben, welche Bedrohungen der TOE abwehren muss, welche organisatorischen Sicherheitspolitiken zu beachten sind und welche Annahmen an seine Einsatzumgebung getroffen werden können.

3.1. Werte

3.1.1. Zu Schützende Werte

Die *zu schützenden Werte* – also Ressourcen und Daten, die der TOE schützt – werden in [BSI-CC-PP-00zz] beschrieben. Die dort beschriebenen Werte gelten ohne Anpassung.

3.1.2. Benutzer des TOE

Die *externen Entitäten, Subjekte und Objekte* des TOE werden in [BSI-CC-PP-00zz] beschrieben. Die *Benutzer* des TOE werden in [BSI-CC-PP-00zz, Abschnitt 3.1.1] beschrieben. Diese Beschreibung gilt ohne Anpassung. Die Subjekte, die im Auftrag des Benutzers agieren, werden in [BSI-CC-PP-00zz, Abschnitt 6.1.2] modelliert. Auch diese Darstellung wird ohne Anpassung in das Security Target übernommen.

3.2. Bedrohungen

T.WAN.Client (Bedrohungen aus dem WAN)
Die in Abschnitt 3.2 von [BSI-CC-PP-00zz] beschriebene Bedrohung T.WAN.Client gilt ohne Anpassung.

T.LAN.Admin (Datenverkehr zur Managementschnittstelle abhören)
Die in Abschnitt 3.2 von [BSI-CC-PP-00zz] beschriebene Bedrohung T.LAN.Admin gilt ohne Anpassung.

T.Zert_Prüf (Manipulierte Zertifikate)
Die in Abschnitt 3.2 von [BSI-CC-PP-00zz] beschriebene Bedrohung T.Zert_Prüf gilt ohne Anpassung.

T.TimeSync (Manipulierte Zeitstempel)
Die in Abschnitt 3.2 von [BSI-CC-PP-00zz] beschriebene Bedrohung T.TimeSync gilt ohne Anpassung.

3.3. Organisatorische Sicherheitspolitiken

OSP.Zeitdienst (Zeitdienst)
Die in Abschnitt 3.3 von [BSI-CC-PP-00zz] beschriebene organisatorische Sicherheitspolitik OSP.Zeitdienst gilt ohne Anpassung.

OSP.TLS (TLS-Kanäle mit sicheren kryptographische Algorithmen)
Die in Abschnitt 3.3 von [BSI-CC-PP-00zz] beschriebene organisatorische Sicherheitspolitik OSP.TLS gilt ohne Anpassung.

3.4. Annahmen

A.Guidance (Befolgen der Guidance)
Die in Abschnitt 3.4 von [BSI-CC-PP-00zz] beschriebene Annahme A.Guidance gilt ohne Anpassung.

4. Sicherheitsziele

4.1. Sicherheitsziele des TOE

O.TLS_Krypto (TLS-Kanäle mit sicheren kryptographische Algorithmen)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-00zz] beschriebene Sicherheitsziel O.TLS_Krypto muss erfüllt werden.

O.Schutz (Selbstschutz, Selbsttest und Schutz von Benutzerdaten)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-00zz] beschriebene Sicherheitsziel O.Schutz muss erfüllt werden.

O.Admin (Administration nur nach Autorisierung und über sicheren Kanal)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-00zz] beschriebene Sicherheitsziel O.Admin muss erfüllt werden.

O.VPN_Auth (Gegenseitige Authentisierung im VPN-Tunnel)
Das in Abschnitt 4.1.2 von [BSI-CC-PP-00zz] beschriebene Sicherheitsziel O.VPN_Auth muss erfüllt werden.

O.VPN_Integrität (Integritätsschutz von Daten im VPN-Tunnel)
Das in Abschnitt 4.1.2 von [BSI-CC-PP-00zz] beschriebene Sicherheitsziel O.VPN_Integrität muss erfüllt werden.

O.VPN_Vertraul (Schutz der Vertraulichkeit von Daten im VPN-Tunnel)
Das in Abschnitt 4.1.2 von [BSI-CC-PP-00zz] beschriebene Sicherheitsziel O.VPN_Vertraul muss erfüllt werden.

O.Zeitdienst (Nutzung eines sicheren Zeitdienstes)
Das in Abschnitt 4.1.1 von [BSI-CC-PP-00zz] beschriebene Sicherheitsziel O.Zeitdienst muss erfüllt werden.

O.Zert_Prüf (Gültigkeitsprüfung für VPN-Zertifikate)
Das in Abschnitt 4.1.2 von [BSI-CC-PP-00zz] beschriebene Sicherheitsziel O.Zert_Prüf muss erfüllt werden.

4.2. Sicherheitsziele für die Umgebung des TOE

OE.Echtzeituhr (Bereitstellung einer Echtzeituhr)
Das in Abschnitt 4.4 von [BSI-CC-PP-00zz] beschriebene Sicherheitsziel OE.Echtzeituhr muss erfüllt werden.

4.3. Erklärung der Sicherheitsziele des TOE

4.3.1. Abbildung der Bedrohungen, OSPs und Annahmen auf Ziele

Die Abbildung der Bedrohungen, organisatorischen Sicherheitspolitiken und Annahmen auf Sicherheitsziele für den TOE entspricht den in [BSI-CC-PP-00zz] beschriebenen Relationen. Tabelle 4.1 entspricht grundsätzlich der Übersicht im Schutzprofil.

Das Schutzprofil beschreibt darüber hinaus, dass einige Bedrohungen durch Assurance-Komponenten der CC abgewehrt werden. Diese zusätzliche Sicherung gilt auch für dieses Security Target.

4.3.2. Erklärung der Abweichungen gegenüber dem Schutzprofil

Für alle unmodifizierten Beziehungen, die dem Schutzprofil entnommen sind (in Tabelle 4.1 mit „✓“ markiert) gelten die Erklärungen, die im Schutzprofil beschrieben sind.

4.3.2.1. Abwehr der Bedrohungen durch die Sicherheitsziele

4.3.2.2. Abbildung der organisatorischen Sicherheitspolitiken auf Sicherheitsziele

Die Abbildungen der organisatorischen Sicherheitspolitiken auf Sicherheitsziele wird unverändert aus dem Schutzprofil übernommen.

4.3.2.3. Abbildung der Annahmen auf Sicherheitsziele für die Umgebung

Die Abbildung der Annahmen auf Sicherheitsziele der Umgebung wird unverändert aus dem Schutzprofil übernommen.

	O.Admin	O.Schutz	O.TLS_Krypto	O.VPN_Auth	O.VPN_Integrität	O.VPN_Vertraul	O.Zeitdienst	O.Zert_Prüf	OE.Echtzeituhr
T.WAN.Client	.	.	.	✓	✓	✓	.	.	.
T.LAN.Admin	✓	✓	✓	.	.	.	.	.	.
T.Zert_Prüf	.	.	.	.	.	.	.	✓	.
T.TimeSync	.	.	.	.	.	.	.	.	✓
OSP.TLS	.	✓	✓	.	.	.	.	.	.
OSP.Zeitdienst	.	.	.	.	.	.	.	.	✓
A.Guidance	.	.	.	.	.	.	.	.	.

Tabelle 4.1.: Abbildung der Sicherheitsziele auf Bedrohungen und Annahmen

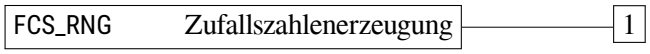
5. Definition der erweiterten Komponenten

5.1. Definition der erweiterten Familie FCS_RNG

Familienverhalten

Diese Familie definiert Anforderungen an die Erzeugung von Zufallszahlen, die für kryptographische Anwendungen vorgesehen sind.

Komponentenabstufung



FCS_RNG.1 „Zufallszahlenerzeugung“ erfordert die Identifizierung des Typs des verwendeten Zufallszahlengenerators und eine Auflistung seiner Sicherheitsmerkmale. Für die erzeugten Zufallszahlen ist eine Qualitätsmetrik anzugeben, auf die sich ihre nachfolgende Verarbeitung und Bewertung abstützen kann.

Management: FCS_RNG.1

Für diese Komponente sind keine Management-Aktivitäten vorgesehen.

Protokollierung: FCS_RNG.1

Es sind keine Ereignisse identifiziert, die protokollierbar sein sollen, wenn FAU_GEN Generierung der Sicherheitsprotokolldaten Bestandteil des PP/des ST ist.

FCS_RNG.1
Zufallszahlenerzeugung

Hierarchical to:	Keine andere Komponente
Dependencies:	Keine Abhängigkeiten
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].

Erklärung für die Einführung der erweiterten Familie

Laut der Definition von OE.Echtzeituhr in [BSI-CC-PP-00zz] ist der TOE für die Zulieferung von Zufallszahlen verantwortlich.

6. Sicherheitsanforderungen

6.1. Hinweise und Definitionen

Der größte Teil der Sicherheitsanforderungen wird ohne Anpassungen aus dem Schutzprofil übernommen. Anpassungen werden kenntlich gemacht. Bei denjenigen SFR, die das Schutzprofil bereits vorsieht, wird in diesem Security Target darauf verzichtet, die Hierarchie der Komponenten sowie deren Abhängigkeiten zu wiederholen. Diese Informationen sind dem Schutzprofil [BSI-CC-PP-00zz] zu entnehmen. Bei Sicherheitsanforderungen, die durch das Security Target hinzugefügt werden, sind die Hierarchie- und Abhängigkeitsinformationen aufgeführt.

6.1.1. Hinweise zur Notation

Die typographischen Auszeichnungen für die Operationen an den SFR sind in Tabelle 6.1 beschrieben. ST-seitige Löschungen werden immer von einem Hinweis begleitet, wie die Löschung motiviert ist.

Quelle	Art der Anpassung	Typographische Eigenschaften
PP	Zuweisung (Assignment)	Zuweisungen sind unterstrichen gesetzt.
	Auswahl (Selection)	Auswahlen sind *kursiv und unterstrichen* gesetzt.
	Verfeinerung (Refinement)	Verfeinerungen sind **fett** gesetzt.
	Löschung (Deletion)	Löschungen sind ~~**fett und durchgestrichen**~~ gesetzt.
ST	Zuweisung (Assignment)	Zuweisungen sind in blauer Schrift gesetzt.
	Auswahl (Selection)	Auswahlen sind *in blauer Schrift und kursiv* gesetzt.
	Verfeinerung (Refinement)	Verfeinerungen sind **in blauer Schrift und fett** gesetzt.
	Löschung (Deletion)	Löschungen sind ~~**in blauer Schrift, fett und durchgestrichen**~~ gesetzt.

Tabelle 6.1.: Typographische Konventionen

6.1.2. Modellierung von Subjekten, Objekten, Attributen und Operationen

Die Modellierungen des Schutzprofils [BSI-CC-PP-00zz] gelten auch für dieses Security Target.

6.2. Funktionale Sicherheitsanforderungen

6.2.1. VPN Client

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

FTP_ITC.1.1/VPN	Die in [BSI-CC-PP-00zz, Abschnitt 6.2.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.2/VPN	Die in [BSI-CC-PP-00zz, Abschnitt 6.2.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FTP_ITC.1.3/VPN	Die in [BSI-CC-PP-00zz, Abschnitt 6.2.1] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

6.2.2. Netzdienste

FPT_STM.1
Reliable time stamps

FPT_STM.1.1	Die in [BSI-CC-PP-00zz, Abschnitt 6.2.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
Refinement:	Die Zuverlässigkeit (reliable) des Zeitstempels wird durch Zeitsynchronisation der Echtzeituhr (gemäß OE.Echtzeituhr) mit Zeitservern unter Verwendung des Protokolls NTPv4 [RFC 5905] erreicht. Der EVG verwendet den verlässlichen Zeitstempel für sich selbst.

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

FPT_TDC.1.1/Zert	Die in [BSI-CC-PP-00zz, Abschnitt 6.2.3] formulierten Sicherheitsanforderungen gelten ohne Anpassung.
FPT_TDC.1.2/Zert	The TSF shall use *interpretation rules* when interpreting the TSF data from another trusted IT product. **The interpretation rules are defined in …**

ST-Anwendungshinweis 1

6.2.3. Stateful Packet Inspection

(This section intentionally left blank.)

6.2.4. Selbstschutz

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:	Die sensitive Daten müssen mit konstanten oder zufälligen Werten überschrieben werden, sobald sie nicht mehr verwendet werden. **These sensitive objects are overwritten with constant or pseudo-random 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 *stored TSF executable code*[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 *the TSF, local users*[7] to initiate communication via the trusted path.
FTP_TRP.1.3/Admin	Die in [BSI-CC-PP-00zz, Abschnitt 6.2.6] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

[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. Kryptographische Basisdienste

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-SHA1, 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 — Die in [BSI-CC-PP-00zz, Abschnitt 6.2.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_CKM.2/TLS
Cryptographic key distribution / TLS

FCS_CKM.2.1/TLS — Die in [BSI-CC-PP-00zz, Abschnitt 6.2.7] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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-Kanäle unter Nutzung sicherer kryptographischer Algorithmen

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

FTP_ITC.1.1/TLS — Die in [BSI-CC-PP-00zz, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FTP_ITC.1.2/TLS — Die in [BSI-CC-PP-00zz, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

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 B.4.[15]

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

(1) X.509-Zertifikate für TLS-Verbindungen

(2) eine Liste gültiger CA-Zertifikate (Trust-Service Status List TSL)

(3) Sperrinformationen zu Zertifikaten für TLS-Verbindungen, die via OCSP erhalten werden

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

(4) 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 — Die in [BSI-CC-PP-00zz, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

FCS_COP.1/TLS.Auth
Cryptographic operation for TLS

FCS_COP.1.1/TLS.Auth — Die in [BSI-CC-PP-00zz, Abschnitt 6.2.8] formulierten Sicherheitsanforderungen gelten ohne Anpassung.

6.2.7. Zusätzliche Sicherheitsanforderungen

Dieser Abschnitt enthält Sicherheitsanforderungen, die zusätzlich zu denen des Schutzprofils definiert werden. Die Anforderungen werden hier um die in Kapitel 5.1 definierte Anforderung FCS_RNG.1/Hash_DRBG erweitert.

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. Sicherheitsanforderungen an die Vertrauenswürdigkeit des EVG

Die Sicherheitsanforderungen an die Vertrauenswürdigkeit für dieses Security Target entsprechen denen, die in [BSI-CC-PP-00zz] definiert sind.

6.4. Erklärung der Sicherheitsanforderungen

6.4.1. Erklärung der Abhängigkeiten der SFR

Die Abhängigkeiten der in Abschnitt 6.2 aufgestellten funktionalen Sicherheitsanforderungen sind erfüllt. Es gelten dieselben Auflösungen von Abhängigkeiten, wie sie im Schutzprofil [BSI-CC-PP-00zz][Abschnitt 6.4.2] beschrieben sind.

Die Abhängigkeiten der über das Schutzprofil hinaus aufgenommenen Sicherheitsanforderungen sind bei der Definition des jeweiligen SFR notiert. Die zusätzlich aufgenommenen SFR sind Iterationen bestehender Komponenten, sodass sich durch diese keine neuen Abhängigkeiten ergeben.

Die in Abschnitt 5.1 neu eingeführte Komponente FCS_RNG.1 hat keine Abhängigkeiten, die aufgelöst werden müssen.

6.4.2. Überblick der Abdeckung von Sicherheitszielen

Die Zuordnung von Sicherheitszielen zu Sicherheitsanforderungen entspricht weitestgehend der Zuordnung, die in [BSI-CC-PP-00zz] getroffen wurde. Tabelle 6.2 zeigt den Zusammenhang.

6.4.3. Detaillierte Erklärung für die Sicherheitsziele

Die detaillierte Erklärung der Sicherheitsziele wird unverändert aus [BSI-CC-PP-00zz] übernommen.

6.5. Erklärung für die gewählte EAL-Stufe

Die Erklärung der gewählten EAL-Stufe wird unverändert aus dem Schutzprofil [BSI-CC-PP-00zz] übernommen.

	O.Admin	O.Schutz	O.TLS_Krypto	O.VPN_Auth	O.VPN_Integrität	O.VPN_Vertraul	O.Zeitdienst	O.Zert_Prüf
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	✓	.	✓	.	.	.	.	.

Tabelle 6.2.: Abbildung der Sicherheitsziele auf Sicherheitsanforderungen

7. TOE Summary Specification

Dieses Kapitel vermittelt einen Überblick über die IT-Sicherheitsfunktionen des TOE, wie sie in der funktionalen Spezifikation beschrieben sind. Es enthält Beschreibungen der allgemeinen technischen Verfahren, die der TOE anwendet, um die Sicherheitsanforderungen zu erfüllen.

Der Abschnitt 7.7 zeigt tabellarisch die Zusammenhänge zwischen den Sicherheitsfunktionen des TOE und den Sicherheitsanforderungen, die dieses Security Target in den Abschnitten 6.2 aufstellt.

7.1. VPN-Client (SF.VPN)

Die Sicherheitsfunktion SF.VPN erstellt sichere Kommunikationskanäle zwischen dem TOE und einem entfernten, vertrauenswürdigen IT-Produkt.

Umgesetzte SFR	
FTP_ITC.1/VPN	FCS_CKM.2/IKE

Zertifikate werden mathematisch geprüft

Umgesetzte SFR
FPT_TDC.1/Zert

7.2. Netzbasierte Sicherheitsfunktionen (SF.NetworkServices)

Die Sicherheitsfunktion SF.NetworkServices stellt dem TOE zuverlässige Zeitstempel zur Verfügung. Eine Referenzzeit wird über den VPN-Kanal von einem vertrauenswürdigen NTP-Server bezogen. Dabei wird NTP in Version 4 verwendet [RFC 5905]. Die Abweichung zwischen der Netzwerkzeit und der lokalen Zeit im TOE darf maximal 1 Stunde betragen. Der TOE verwendet die Uhrzeit hauptsächlich, um die Gültigkeit von Zertifikaten zu prüfen.

Umgesetzte SFR
FPT_STM.1

7.3. Selbstschutz (SF.SelfProtection)

Die Sicherheitsfunktion SF.SelfProtection ist dafür verantwortlich, den TOE und die Daten, die er verarbeitet, vor Angriffen und Manipulation zu schützen.

Sensible Daten werden aus dem Arbeitsspeicher gelöscht, sobald sie nicht mehr verwendet werden. Das umfasst kryptographische Schlüssel, Session Keys, kurzlebige Schlüssel während des Ver- und Entschlüsselungsvorgangs, aber auch sensible Benutzerddaten. Das Löschen wird durch aktives Überschreiben der entsprechenden Speicherbereiche mit einer Konstante oder pseudo-zufälligen Werten umgesetzt.

Umgesetzte SFR
FDP_RIP.1

Der TOE kann eine Reihe von Selbsttests ausführen, um seine Integrität und die Funktionsfähigkeit seiner eigenen Sicherheitsfunktionen und Komponenten zu beweisen. Abhängig von deren Ausprägung werden die Selbsttests entweder beim Systemstart, während des normalen Betriebs oder zu beiden Gelegenheiten ausgeführt. Der Administrator kann die Selbsttests ebenfalls starten.

Umgesetzte SFR
FPT_TST.1

7.4. Administration (SF.Administration)

Die Sicherheitsfunktionen des TOE definieren eine Rolle „Administrator“. Benutzer greifen zur Verwaltung des TOE über eine TLS-Verbindung auf den TOE zu. Die TLS-Verbindung wird von der Funktion SF.CryptographicServices bereit gestellt. Ist ein Administrator authentisiert, ist er autorisiert, verschiedene TSF-Parameter zu konfigurieren und TSF-bezogene Operationen durchzuführen.

- Die Systemzeit/Echtzeituhr modifizieren
- Die Selbsttests des TOE auslösen (vgl. SF.SelfProtection)

Es ist zu beachten, dass die Web-Anwendung in der Umgebung des TOE ausgeführt wird. Die Sicherheitsleistungen werden von der Management-Schnittstelle erbracht, die den Authentisierungsstatus des Administrators prüft.

Der TOE informiert den Administrator über kritische Betriebszustände über die LEDs an der Gehäusefront (PS.LED).

Umgesetzte SFR
FTP_TRP.1/Admin

7.5. Kryptografische Dienste (SF.CryptographicServices)

Die Sicherheitsfunktion SF.CryptographicServices stellt Implementierungen verschiedener kryptographischer Basisalgorithmen zur Verfügung, die von anderen Sicherheitsfunktionen des TOE verwendet werden können.

Schlüsselbehandlung

Die Sicherheitsfunktionalität stellt alle Algorithmen zur Erzeugung, Verteilung und Vernichtung von Schlüsseln zur Verfügung.

Umgesetzte SFR	
FCS_CKM.1	FCS_CKM.4

Zufallszahlen

Der TOE enthält einen DRNG nach FCS_RNG.1/Hash_DRBG, um Zufallszahlen hoher Qualität zu erzeugen. Die so erzeugten Zufallszahlen werden für verschiedene Zwecke verwendet, u.a. beim TLS-Verbindungsaufbau (FCS_CKM.1 und FCS_COP.1/TLS.AES)

Umgesetzte SFR
FCS_RNG.1/Hash_DRBG

Hash-Algorithmen

Die Funktion bietet Implementierungen für die Hash-Algorithmen SHA-1, SHA-256 und SHA-512. Im Kontext von TLS implementiert der TOE außerdem SHA-384 für bestimmte Cipher Suites.

Umgesetzte SFR
FCS_COP.1/Hash

HMAC Generierung

Die Funktion bietet darüber hinaus Algorithmen für die HMAC-Generierung, wobei die genannten Hash-Algorithmen zum Tragen kommen: HMAC-SHA-1(-96), HMAC-SHA-256(-128).

Umgesetzte SFR
FCS_COP.1/HMAC

7.6. TLS-Service (SF.TLS)

Der TOE stellt die Umsetzung des TLS-Protokolls in der Version 1.2 bereit. Die Funktion stellt die Integrität und Vertraulichkeit der Verbindungen zum Web-Browswer des Administrators sicher. Die genaue Verwendung der TLS-Verbindungen und eine Auflistung der Kommunikationspartner befindet sich in Tabelle B.4 auf Seite 34.

Umgesetzte SFR		
FTP_ITC.1/TLS	FCS_COP.1/TLS.AES	FCS_CKM.2/TLS

Die Sicherheitsfunktion SF.CryptographicServices bietet Algorithmen zur Verifikation von Signaturen. X.509-Zertifikate werden unter Verwendung des RSA-PKCS1-v1.5- bzw RSASSA-PSS-Algorithmus geprüft.

Umgesetzte SFR	
FPT_TDC.1/TLS.Zert	FCS_COP.1/TLS.Auth

Für die Generierung von Nonces und Schlüsseln verwendet der TOE den Hash_DRBG Zufallsgenerator aus SF.CryptographicServices. Session Keys werden durch das Überschreiben mit konstanten oder pseudozufälligen Werten sicher aus dem Speicher entfernt, ebenfalls durch Aufruf von SF.CryptographicServices.

7.7. Verhältnis von SFR zu SF

Tabelle 7.1 zeigt, in welchem Verhältnis die im Abschnitt Abschnitt 6.2 definierten Sicherheitsanforderungen an den TOE zu den in Abschnitt 7 beschriebenen Sicherheitsfunktionen stehen. Die verwendeten Symbole sind in der Legende in Tabelle A.1 beschrieben.

	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	✓	.	.	.	.	.

Tabelle 7.1.: Abbildung der SFR auf Sicherheitsfunktionalität

A. Erklärung der tabellarischen Darstellung

Tabelle A.1 zeigt die in den Tabellen dieses Dokuments verwendeten Symbole. Diese kommen in allen Tabellen zum Einsatz, in denen Entitäten der Common Criteria aufeinander abgebildet werden.

Symbol	Beschreibung
✓	Vom Schutzprofil vorgesehene Beziehung / vorgesehenes SFR
•	Vom Schutzprofil als optional vorgesehene Beziehung / vorgesehenes SFR
◦	Nicht umgesetzte, vom Schutzprofil als optional vorgesehene Beziehung / vorgesehenes SFR
✓	Vom Security Target zusätzlich angenommene Beziehung / zusätzlich angenommenes SFR

Tabelle A.1.: Legende der Abbildungstabellen

B. TLS Verbindungen

Für die TLS-Verbindungen werden die im Schutzprofil genannten Cipher Suiten verwendet. Der TOE beherrscht genau diese Cipher Suiten und keine darüber hinaus. Tabelle B.1 listet diese Cipher Suiten auf. Tabelle B.2 zeigt die elliptischen Kurven, die beim ECDHE Schlüsselaustausch zur Anwendung kommen.

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`	✓

Tabelle B.1.: Cipher Suites der TLS Verbindungen des TOE

Elliptische Kurve	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]

Tabelle B.2.: Elliptische Kurven für die TLS Verbindungen des TOE

Der TOE kommuniziert mit anderen vertrauenswürdigen IT-Produkten über gesicherte Verbindungen. Die Integrität und die Vertrauenswürdigkeit der Verbindungen wird durch die Verwendung von TLS in der Version 1.2 und die in Tabelle B.1 genannten Algorithmen und Cipher Suiten sichergestellt. Tabelle B.4 listet die Verbindungen auf, die der TOE eingeht. Die Spalten dieser Tabelle werden in Tabelle B.3 beschrieben.

Spalte	Beschreibung
ID	Symbolischer Name der Verbindung
Schnittstelle	Logische Schnittstelle, deren Kommunikation abgesichert wird.
Rolle	Beschreibt, ob der TOE in dieser Verbindung Client oder Server ist.
Peer	Beschreibung des Partners in der TLS-Verbindung
Protokoll	Anwendungsprotokoll, das für die Verbindung genutzt wird.
Subsystem::Modul	Name des Subsystems und des Moduls, von dem die Verbindung ausgeht, bzw. das die Verbindung empfängt und behandelt.
Port	Port, den der TOE öffnet, um die Verbindung aufzubauen. Für Verbindungen, bei denen der TOE Server ist, steht hier eine Portnummer. Wenn der TOE Client ist, steht „dyn.“ für die ephemerische Portvergabe bei TCP-Verbindungen. „konfig.“ steht dafür, dass der Zielport konfigurierbar ist.
Schnittstelle	Logische Schnittstelle des TOE , über die die Verbindung läuft.
Identität des TOE	Zertifikat, mit dem sich der TOE gegenüber dem Peer authentisiert.
Identität des Peer	Zertifikat/Verfahren, mit dem sich der Peer gegenüber dem TOE authentisiert.
Authentifizierung des Peer durch	Verfahren, Datenquelle oder Subsystem/Modul, mit dem der TOE die Identität des Peers verifiziert.

Tabelle B.3.: Legende zu den TLS Verbindungen

ID	Schnittstelle (Protokoll)	Rolle	Peer	Subsystem::Modul	Port	Identität des TOE	Identität des Peer	Authentifizierung des Peer durch
TLS.1	LS.LAN.HTTP_MGMT	Server	Browser	Administrationssystem::HTTP-Server	443	Zertifikat aus Mauve CA	Benutzername/Passwort	Benutzerverwaltung im TOE

Tabelle B.4.: TLS Verbindungen des MauveVPN Client

Literatur

[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, 16. Nov. 2005.

[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), 5. Feb. 2020.

[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, Sep. 2012. 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, Sep. 2012. URL: http://www.commoncriteriaportal.org/thecc.html.

[FIPS PUB 180-4] National Institute of Standards und 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 und Technology. *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication. Information Technology Laboratory, Juli 2013. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[RFC 2404] C. Madson und 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 und M. Kojo. *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*. RFC 3526 (Proposed Standard). RFC. Fremont, CA, USA: RFC Editor, Mai 2003. DOI: 10.17487/RFC3526. URL: https://www.rfc-editor.org/rfc/rfc3526.txt.

[RFC 4868] S. Kelly und 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, Mai 2007. DOI: 10.17487/RFC4868. URL: https://www.rfc-editor.org/rfc/rfc4868.txt.

[RFC 5246] T. Dierks und 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 und J. Merkle. *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*. RFC 5639 (Informational). RFC. Fremont, CA, USA: RFC Editor, März 2010. DOI: 10.17487/RFC5639. URL: https://www.rfc-editor.org/rfc/rfc5639.txt.

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

[RFC 5996] C. Kaufman u. a. *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, Sep. 2010. DOI: 10.17487/RFC5996. URL: https://www.rfc-editor.org/rfc/rfc5996.txt.

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

[RFC 8422] Y. Nir, S. Josefsson und 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.

[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), 21. Sep. 2018. URL: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html.

Verzeichnis der ST-Anwendungshinweise

Index der SFR