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

TOE Design Specification

MAUVECORP MAUVEVPN CLIENT
Version 2.11

MauveCorp
Fliederweg 98
50020 Köln
certification@mauvecorp.com

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

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einleitung

Dieses Dokument enthält die notwendigen Informationen zur Evaluation der Vertrauenswürdigkeitskomponente ADV_TDS.3 für die Evaluation des MauveCorp MauveVPN Client.

Das Dokument beschreibt das TOE Design auf zwei Abstraktionsebenen: Subsysteme und Module, wie durch den vom Schutzprofil geforderten Assurance Level ADV_TDS.3 vorgegeben. Die Subsysteme werden, den Vorgaben in Abschnitt „A.4.2 Modules“ des dritten Teils der CC folgend [CC Part 3], lediglich auf hoher Abstraktionsebene beschrieben. Die Beschreibungen der Module fallen entsprechend ausführlicher aus.

Anmerkungen zur Notation

Tabelle 1.1 auf der nächsten Seite listet die in diesem Dokument verwendeten typographischen Auszeichnungen und ihre Verwendung auf. Oftmals ist die Abgrenzung zwischen den in der Tabelle aufgeführten Kategorien nicht ganz leicht: So kommt es gelegentlich vor, dass auf verschiedenen Abstraktionsebenen dieselben Begriffe verwendet werden. Es ist in solchen Fällen nicht auf den ersten Blick zu erkennen, auf welcher Abstraktionsebene der Begriff gerade verwendet wird. Beispielsweise kann ein Begriff gleichzeitig ein Konfigurationsparameter aus der Spezifikation und gleichzeitig der Name einer Variable im Code sein. Durch eine möglichst hohe typographische Konsistenz soll der jeweilige Kontext verdeutlicht werden. Die Hinweise in Tabelle 1.1 sollen helfen, die Begrifflichkeiten einzuordnen und voneinander abzugrenzen.

Module und Subsysteme werden durch doppelte Doppelpunkte in der Form Subsystem::Modul notiert. Wird in einem solchen Kontext auf eine Schnittstelle verwiesen, wird der Name der Schnittstelle durch zwei Schrägstriche vom Namen des Moduls getrennt: Subsystem::Modul//Schnittstelle.

Die ihm Text zitierten Namen von Code-Elementen – besonders die Komponenten im Java-Umfeld – können zum Teil lang werden. In solchen Fällen werden die Namen der besseren Lesbarkeit halber mit Trennstrichen versehen, die in dieser Form nicht im Code sichtbar sind. Diese minimale Abweichung wird in Kauf genommen, um dem Text ein harmonisches Gesamtbild zu verleihen, das nicht durch übermäßigen Weißraum gestört wird.

Typographische Auszeichnung	Verwendung
Schlüsselwörter	*Schlüsselwörter* sind solche Begriffe, die z. B. direkt aus der Spezifikation entnommen sind, dies können Konfigurationsparameter und ihre Werte sein. Aber auch andere Begriffe, die im Kontext des TOE eine hervorgehobene Bedeutung haben, sind so ausgezeichnet.
`Code-Elemente`	`Code-Elemente` sind solche Begriffe, die unmittelbar aus dem Source-Code des TOE entnommen sind. Dies können beispielsweise Java-Bundles, Klassen- oder Methodennamen sein, aber auch deren Parameter oder logische Strukturen in einer der verwendeten Programmiersprachen.
Dateinamen	*Dateinamen* beziehen sich auf Namen oder Namensteile von Elementen im Dateisystem.
Sicherheitsbezogene Begriffe	Begriffe, die in direktem Bezug zum Rahmenwerk der Common Criteria stehen, sind als Sicherheitsbezogene Begriffe gesetzt. Dies sind SFR, die Namen der SF und TSFI, aber auch die Namen der Subsysteme, Module und Schnittstellen, die den TOE konstituieren. Weiterhin sind Namen der vom TOE verwendeten Zertifikate und sonstigen Schlüsselmaterials in dieser Form gesetzt.

Tabelle 1.1.: Typographische Konventionen

2. Beschreibung der Subsysteme

Dieses Kapitel beschreibt die Unterteilung des TOE in seine Subsysteme.

2.1. Subsystem VPN Client

Beschreibung

Das Subsystem VPN Client stellt den VPN-Client bereit, mit dem VPN-Tunnel im WAN aufgebaut werden können.

Umgesetzte SFR

Das Subsystem erfüllt die Anforderungen, die durch die SFR in Tabelle 2.1 und Tabelle 2.2 an den EVG gestellt werden.

Interaktion mit anderen Subsystemen

Das Subsystem ruft Funktionalität aus dem Subsystem Kryptodienste auf.

Enforcing SFR	Beschreibung
FCS_CKM.2/IKE	Verbindungsaufbau, Schlüsselverteilung für VPN
FPT_TDC.1/Zert	Zertifikatsprüfung
FTP_ITC.1/VPN	VPN-Verbindungen starten/beenden

Tabelle 2.1.: Enforcing SFR des Subsystems VPN Client

Supporting SFR	Beschreibung
FTP_TRP.1/Admin	VPN-Verbindungen starten/beenden

Tabelle 2.2.: Supporting SFR des Subsystems VPN Client

2.2. Subsystem NTP Client

Beschreibung

Das Subsystem NTP Client stellt den VPN-Client bereit, mit dem die Systemzeit synchronisiert werden kann.

Umgesetzte SFR

Das Subsystem erfüllt die Anforderungen, die durch die SFR in Tabelle 2.3 und Tabelle 2.4 an den EVG gestellt werden.

Interaktion mit anderen Subsystemen

Enforcing SFR	Beschreibung
FPT_STM.1	Zeitdienst

Tabelle 2.3.: Enforcing SFR des Subsystems NTP Client

Supporting SFR	Beschreibung
(Keine)	

Tabelle 2.4.: Supporting SFR des Subsystems NTP Client

2.3. Subsystem Protection

Beschreibung

Das Subsystem Protection enthält die Funktionen zum Selbstschutz des TOE. Das Subsystem sorgt für Speicherbereinigung (Speicherschutz) und Selbsttests (Selbsttest).

Umgesetzte SFR

Das Subsystem erfüllt die Anforderungen, die durch die SFR in Tabelle 2.5 und Tabelle 2.6 an den EVG gestellt werden.

Interaktion mit anderen Subsystemen

Enforcing SFR	Beschreibung
FDP_RIP.1	Speicher bereinigen
FPT_TST.1	Selbsttest ausführen

Tabelle 2.5.: Enforcing SFR des Subsystems Protection

Supporting SFR	Beschreibung
FPT_TST.1	Selbsttest aufrufen

Tabelle 2.6.: Supporting SFR des Subsystems Protection

2.4. Subsystem Administrationssystem

Beschreibung

Das Subsystem Administrationssystem stellt die Administrationsanwendung und Managementfunktionen des TOE bereit.

Umgesetzte SFR

Das Subsystem erfüllt die Anforderungen, die durch die SFR in Tabelle 2.7 und Tabelle 2.8 an den EVG gestellt werden.

Interaktion mit anderen Subsystemen

Das Subsystem ruft die Selbsttests des Subsystems Protection auf.

Enforcing SFR	Beschreibung
FTP_TRP.1/Admin	Managementanwendung bereitstellen

Tabelle 2.7.: Enforcing SFR des Subsystems Administrationssystem

Supporting SFR	Beschreibung
FTP_ITC.1/VPN	VPN-Verbindungen managen

Tabelle 2.8.: Supporting SFR des Subsystems Administrationssystem

2.5. Subsystem Kryptodienste

Beschreibung

Umgesetzte SFR

Das Subsystem erfüllt die Anforderungen, die durch die SFR in Tabelle 2.9 und Tabelle 2.10 an den EVG gestellt werden.

Interaktion mit anderen Subsystemen

Enforcing SFR	Beschreibung
FCS_CKM.1	Schlüsselerstellung für VPN und TLS
FCS_CKM.4	Schlüsselzerstörung für VPN und TLS
FCS_COP.1/Hash	Hash-Algorithmen bereitstellen
FCS_COP.1/HMAC	HMAC-Algorithmen bereitstellen
FCS_RNG.1/Hash_DRBG	Zufallszahlen erzeugen

Tabelle 2.9.: Enforcing SFR des Subsystems Kryptodienste

Supporting SFR	Beschreibung
(Keine)	

Tabelle 2.10.: Supporting SFR des Subsystems Kryptodienste

2.6. Subsystem TLS-Server

Beschreibung

Umgesetzte SFR

Das Subsystem erfüllt die Anforderungen, die durch die SFR in Tabelle 2.11 und Tabelle 2.12 an den EVG gestellt werden.

Interaktion mit anderen Subsystemen

Enforcing SFR	Beschreibung
FCS_CKM.2/TLS	Verbindungsaufbau, Schlüsselverteilung für TLS
FCS_COP.1/TLS.AES	AES für TLS bereitstellen
FCS_COP.1/TLS.Auth	Authentisierung des TLS-Partners
FPT_TDC.1/TLS.Zert	Zertifikatsprüfung
FTP_ITC.1/TLS	TLS-Verbindungen starten/beenden

Tabelle 2.11.: Enforcing SFR des Subsystems TLS-Server

Supporting SFR	Beschreibung
(Keine)	

Tabelle 2.12.: Supporting SFR des Subsystems TLS-Server

3. Beschreibung der Module

Dieses Kapitel beschreibt die verschiedenen Module des TOE, sortiert nach Subsystemen.

3.1. Module für Subsystem VPN Client

In diesem Kapitel werden die Module des Subsystems VPN Client beschrieben.

3.1.1. Modul VPN Client::Core

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.1 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR	
FCS_CKM.2/IKE	FTP_ITC.1/VPN
Supporting SFR	
FTP_TRP.1/Admin	

Tabelle 3.1.: SFR des Moduls VPN Client::Core

3.1.1.1. Beschreibung

Über das Modul Core des Subsystems VPN Client stellt der TOE Schnittstellen .....

3.1.1.2. Abläufe des Moduls

3.1.1.2.1. Verbindung zum VPN-Konzentrator aufbauen Der Ablauf baut die Verbindung zum VPN-Konzentrator auf. Das Zertifikat des Konzentrators wird über die Schnittstelle VPN Client::-Zertifikatsdienst//Check-VPN-Certificate geprüft.

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

3.1.1.2.2. Verbindung zum VPN-Konzentrator abbbauen Der Ablauf baut die Verbindung zum VPN-Konzentrator ab.

Umgesetzte SFR
FTP_ITC.1/VPN

3.1.1.3. Schnittstellen zu anderen Modulen

3.1.1.3.1. Connect-to-VPN (Provided) Über diese Schnittstelle wird die VPN-Verbindung aufgebaut (vgl. Abschnitt 3.1.1.2.1).

3.1.1.3.2. Disconnect-from-VPN (Provided) Über diese Schnittstelle wird die VPN-Verbindung abgebaut (vgl. Abschnitt 3.1.1.2.2).

3.1.1.3.3. Check-VPN-Certificate (Required) Die Schnittstelle VPN Client::Zertifikatsdienst//-Check-VPN-Certificate wird verwendet, um das Zertifikat des VPN-Konzentrators zu prüfen.

3.1.1.3.4. Create-DHE-Key (Required) Die Schnittstelle Kryptodienste::Key-Services//Create-DHE-Key wird verwendet, um einen Verbindungsschlüssel zu erzeugen.

3.1.1.3.5. Destroy-Key (Required) Die Schnittstelle Kryptodienste::Key-Services//Destroy-Key wird verwendet, um einen Verbindungsschlüssel zu zerstören.

3.1.2. Modul VPN Client::Zertifikatsdienst

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.2 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR
FPT_TDC.1/Zert
Supporting SFR
(Keine)

Tabelle 3.2.: SFR des Moduls VPN Client::Zertifikatsdienst

3.1.2.1. Beschreibung

Über das Modul Zertifikatsdienst des Subsystems VPN Client stellt der TOE Schnittstellen .....

3.1.2.2. Abläufe des Moduls

3.1.2.2.1. Prüfung des Zertifikats des VPN-Konzentrators Das Zertifikat wird auf mathematische Gültigkeit geprüft. Der Hash des Zertifikats wird über die Funktion Kryptodienste::Algorithmen//Get-Hash berechnet.

Umgesetzte SFR
FPT_TDC.1/Zert

3.1.2.3. Schnittstellen zu anderen Modulen

3.1.2.3.1. Check-VPN-Certificate (Provided) Über diese Schnittstelle das Zertifikat des VPN-Konzentrators geprüft (vgl. Abschnitt 3.1.2.2.1).

3.1.2.3.2. Get-Hash (Required) Die Schnittstelle Kryptodienste::Algorithmen//Get-Hash wird verwendet, um den Hash über das Zertifikat zu berechnen.

3.2. Module für Subsystem NTP Client

In diesem Kapitel werden die Module des Subsystems NTP Client beschrieben.

3.2.1. Modul NTP Client::Core

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.3 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR
FPT_STM.1
Supporting SFR
(Keine)

Tabelle 3.3.: SFR des Moduls NTP Client::Core

3.2.1.1. Beschreibung

Über das Modul Core des Subsystems NTP Client stellt der TOE Schnittstellen .....

3.2.1.2. Abläufe des Moduls

3.2.1.2.1. Synchronisieren der Systemzeit

Umgesetzte SFR
FPT_STM.1

3.2.1.3. Schnittstellen zu anderen Modulen

3.2.1.3.1. Sync-Time (Provided) Über diese Schnittstelle wird die Synchroniation der Systemzeit gestartet (vgl. Abschnitt 3.2.1.2.1).

3.3. Module für Subsystem Protection

In diesem Kapitel werden die Module des Subsystems Protection beschrieben.

3.3.1. Modul Protection::Speicherschutz

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.4 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR
FDP_RIP.1
Supporting SFR
(Keine)

Tabelle 3.4.: SFR des Moduls Protection::Speicherschutz

3.3.1.1. Beschreibung

Über das Modul Speicherschutz des Subsystems Protection stellt der TOE Verfahren .....

3.3.1.2. Abläufe des Moduls

3.3.1.2.1. Löschen des Speichers

Umgesetzte SFR
FDP_RIP.1

3.3.1.3. Schnittstellen zu anderen Modulen

3.3.1.3.1. Clean-Memory (Provided) Über diese Schnittstelle wird das sichere Löschen des Speichers aufgerufen.

3.3.2. Modul Protection::Selbsttest

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.5 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR
FPT_TST.1
Supporting SFR
FPT_TST.1

Tabelle 3.5.: SFR des Moduls Protection::Selbsttest

3.3.2.1. Beschreibung

Über das Modul Selbsttest des Subsystems Protection stellt der TOE Schnittstellen .....

3.3.2.2. Abläufe des Moduls

3.3.2.2.1. Selbsttest der TSF

Umgesetzte SFR
FPT_TST.1

3.3.2.3. Schnittstellen zu anderen Modulen

3.3.2.3.1. Run-Selftest (Provided) Über diese Schnittstelle wird der Selbsttest gestartet.

3.4. Module für Subsystem Administrationssystem

In diesem Kapitel werden die Module des Subsystems Administrationssystem beschrieben.

3.4.1. Modul Administrationssystem::HTTP-Server

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.6 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR
FTP_TRP.1/Admin
Supporting SFR
(Keine)

Tabelle 3.6.: SFR des Moduls Administrationssystem::HTTP-Server

3.4.1.1. Beschreibung

Über das Modul HTTP-Server des Subsystems Administrationssystem stellt der TOE Schnittstellen .....

3.4.1.2. Abläufe des Moduls

3.4.1.2.1. HTTP-Kommunikation mit dem Administrator

Umgesetzte SFR
FTP_TRP.1/Admin

3.4.1.3. Schnittstellen zu anderen Modulen

3.4.1.3.1. HTTP-Endpoint (Provided) Über diese Schnittstelle wird die logische Schnittstelle LS.LAN.HTTP_MGMT umgesetzt.

3.4.1.3.2. Set-Configuration (Required) Über die Schnittstelle Administrationssystem::-Management-Anwendung//Set-Configuration speichert der HTTP-Server die Konfigurationsparameter.

3.4.1.3.3. Connect-Disconnect-VPN (Required) Über die Schnittstelle Administrationssystem::Management-Anwendung//Connect-Disconnect-VPN ruft HTTP-Server die Funktion zum Auf- und Abbau der VPN-Verbindung auf.

3.4.2. Modul Administrationssystem::Management-Anwendung

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.7 an den EVG gestellt werden. Das Modul ist SFR-supporting für den TOE.

Enforcing SFR
(Keine)
Supporting SFR
FTP_ITC.1/VPN

Tabelle 3.7.: SFR des Moduls Administrationssystem::Management-Anwendung

3.4.2.1. Beschreibung

Über das Modul Management-Anwendung des Subsystems Administrationssystem stellt der TOE Schnittstellen .....

3.4.2.2. Abläufe des Moduls

3.4.2.2.1. Speichern der Konfiguration

3.4.2.2.2. Auf- und Abbau der VPN-Verbindung Dieser Ablauf ruft den Verbindungsauf- und abbau auf. Die Schnittstelle VPN Client::Core//Connect-to-VPN wird verwendet, um die VPN-Verbindung aufzubauen. Die Schnittstelle VPN Client::Core//Disconnect-from-VPN wird verwendet, um die VPN-Verbindung abzubauen.

3.4.2.2.3. Aufruf des Selbsttests Die Schnittstelle Protection::Selbsttest//Run-Selftest wird verwendet, um den Selbsttest zu starten.

3.4.2.3. Schnittstellen zu anderen Modulen

3.4.2.3.1. Set-Configuration (Provided) Über diese Schnittstelle wird die Konfiguration des Moduls Management-Anwendung verwaltet. Die Konfiguration kann darüber entweder gelesen oder geschrieben werden.

3.4.2.3.2. Connect-Disconnect-VPN (Provided)

3.4.2.3.3. Connect-to-VPN (Required) Die Schnittstelle VPN Client::Core//Connect-to-VPN wird verwendet, um die VPN-Verbindung aufzubauen.

3.4.2.3.4. Disconnect-from-VPN (Required) Die Schnittstelle VPN Client::Core//Disconnect-from-VPN wird verwendet, um die VPN-Verbindung abzubauen.

3.4.2.3.5. Run-Selftest (Required) Die Schnittstelle Protection::Selbsttest//Run-Selftest wird verwendet, um den Selbsttest zu starten.

3.5. Module für Subsystem Kryptodienste

In diesem Kapitel werden die Module des Subsystems Kryptodienste beschrieben.

3.5.1. Modul Kryptodienste::Algorithmen

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.8 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR	
FCS_COP.1/Hash	FCS_COP.1/HMAC
Supporting SFR	
(Keine)	

Tabelle 3.8.: SFR des Moduls Kryptodienste::Algorithmen

3.5.1.1. Beschreibung

Über das Modul Algorithmen des Subsystems Kryptodienste stellt der TOE Verfahren .....

3.5.1.2. Abläufe des Moduls

3.5.1.2.1. Hashwerte berechnen

Umgesetzte SFR
FCS_COP.1/Hash

3.5.1.2.2. HMAC berechnen

Umgesetzte SFR
FCS_COP.1/HMAC

3.5.1.3. Schnittstellen zu anderen Modulen

3.5.1.3.1. Get-Hash (Provided) Über diese Schnittstelle werden Hashwerte berechnet.

3.5.1.3.2. Get-HMAC (Provided) Über diese Schnittstelle werden HMAC berechnet.

3.5.2. Modul Kryptodienste::Key-Services

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.9 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR	
FCS_CKM.1	FCS_CKM.4
Supporting SFR	
(Keine)	

Tabelle 3.9.: SFR des Moduls Kryptodienste::Key-Services

3.5.2.1. Beschreibung

Über das Modul Key-Services des Subsystems Kryptodienste stellt der TOE Verfahren .....

3.5.2.2. Abläufe des Moduls

3.5.2.2.1. Schlüssel erzeugen

Umgesetzte SFR
FCS_CKM.1

3.5.2.2.2. Schlüssel zerstören

Umgesetzte SFR
FCS_CKM.4

3.5.2.3. Schnittstellen zu anderen Modulen

3.5.2.3.1. Create-DHE-Key (Provided) Über diese Schnittstelle wird ein Schlüssel erstellt.

3.5.2.3.2. Destroy-Key (Provided) Über diese Schnittstelle wird ein Schlüssel zerstört.

3.5.3. Modul Kryptodienste::Zufallszahlen

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.10 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR
FCS_RNG.1/Hash_DRBG
Supporting SFR
(Keine)

Tabelle 3.10.: SFR des Moduls Kryptodienste::Zufallszahlen

3.5.3.1. Beschreibung

Über das Modul Zufallszahlen des Subsystems Kryptodienste stellt der TOE Verfahren .....

3.5.3.2. Abläufe des Moduls

3.5.3.2.1. Erstellen einer Zufallszahl

Umgesetzte SFR
FCS_RNG.1/Hash_DRBG

3.5.3.3. Schnittstellen zu anderen Modulen

3.5.3.3.1. Create-Random (Provided) Über diese Schnittstelle wird eine Zufallszahl erzeugt.

3.6. Module für Subsystem TLS-Server

In diesem Kapitel werden die Module des Subsystems TLS-Server beschrieben.

3.6.1. Modul TLS-Server::Core

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.11 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR	
FCS_CKM.2/TLS	FCS_COP.1/TLS.Auth
FCS_COP.1/TLS.AES	FTP_ITC.1/TLS
Supporting SFR	
(Keine)	

Tabelle 3.11.: SFR des Moduls TLS-Server::Core

3.6.1.1. Beschreibung

Über das Modul Core des Subsystems TLS-Server stellt der TOE Schnittstellen .....

3.6.1.2. Abläufe des Moduls

3.6.1.2.1. Aufbau einer TLS-Verbindung

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

3.6.1.2.2. Authentisieren des Kommunikationspartners

Umgesetzte SFR
FCS_COP.1/TLS.Auth

3.6.1.2.3. Abbau einer TLS-Verbindung

Umgesetzte SFR
FTP_ITC.1/TLS

3.6.1.3. Schnittstellen zu anderen Modulen

3.6.1.3.1. TLS-Connection-Accept (Provided) Über diese Schnittstelle wird eine TLS-Verbindung aufgebaut.

3.6.1.3.2. TLS-Disconnect (Provided) Über diese Schnittstelle wird eine TLS-Verbindung abgebaut.

3.6.1.3.3. Check-TLS-Certificate (Required) Die Schnittstelle TLS-Server::Zertifikatsdienst//-Check-TLS-Certificate wird verwendet, um das Zertifikat des Kommunikationspartners zu prüfen.

3.6.1.3.4. Create-DHE-Key (Required) Die Schnittstelle Kryptodienste::Key-Services//Create-DHE-Key wird verwendet, um einen Verbindungsschlüssel zu erzeugen.

3.6.1.3.5. Destroy-Key (Required) Die Schnittstelle Kryptodienste::Key-Services//Destroy-Key wird verwendet, um einen Verbindungsschlüssel zu zerstören.

3.6.2. Modul TLS-Server::Zertifikatsdienst

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.12 an den EVG gestellt werden. Das Modul ist SFR-enforcing für den TOE.

Enforcing SFR
FPT_TDC.1/TLS.Zert
Supporting SFR
(Keine)

Tabelle 3.12.: SFR des Moduls TLS-Server::Zertifikatsdienst

3.6.2.1. Beschreibung

Über das Modul Zertifikatsdienst des Subsystems TLS-Server stellt der TOE Schnittstellen .....

3.6.2.2. Abläufe des Moduls

3.6.2.2.1. Prüfung des Zertifikats

Umgesetzte SFR
FPT_TDC.1/TLS.Zert

3.6.2.3. Schnittstellen zu anderen Modulen

3.6.2.3.1. Check-TLS-Certificate (Provided) Über diese Schnittstelle wird das Zertifikat des Kommunikationspartners geprüft.

3.6.2.3.2. Get-Hash (Required) Die Schnittstelle Kryptodienste::Algorithmen//Get-Hash wird verwendet, um den Hash über das Zertifikat zu berechnen.

A. 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 A.1 listet diese Cipher Suiten auf. Tabelle A.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 A.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 A.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 A.1 genannten Algorithmen und Cipher Suiten sichergestellt. Tabelle A.4 listet die Verbindungen auf, die der TOE eingeht. Die Spalten dieser Tabelle werden in Tabelle A.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 A.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 A.4.: TLS Verbindungen des MauveVPN Client

B. Liste der TSFI

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 B.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 B.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 B.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 B.2.: Logische Schnittstellen an LS.WAN

C. Zuordnung von Modulen zu SFRs

In der folgenden Tabelle werden den einzelnen SFRs ihre *supporting* oder *enforcing* Module zugeordnet.

SFR	Relation	Subsystem::Modul
FCS_CKM.1	Enforcing Supporting	Kryptodienste::Key-Services (Keine)
FCS_CKM.2/IKE	Enforcing Supporting	VPN Client::Core (Keine)
FCS_CKM.2/TLS	Enforcing Supporting	TLS-Server::Core (Keine)
FCS_CKM.4	Enforcing Supporting	Kryptodienste::Key-Services (Keine)
FCS_COP.1/Hash	Enforcing Supporting	Kryptodienste::Algorithmen (Keine)
FCS_COP.1/HMAC	Enforcing Supporting	Kryptodienste::Algorithmen (Keine)
FCS_COP.1/TLS.AES	Enforcing Supporting	TLS-Server::Core (Keine)
FCS_COP.1/TLS.Auth	Enforcing Supporting	TLS-Server::Core (Keine)
FCS_RNG.1/Hash_DRBG	Enforcing Supporting	Kryptodienste::Zufallszahlen (Keine)
FDP_RIP.1	Enforcing Supporting	Protection::Speicherschutz (Keine)
FPT_TDC.1/TLS.Zert	Enforcing Supporting	TLS-Server::Zertifikatsdienst (Keine)
FPT_TDC.1/Zert	Enforcing Supporting	VPN Client::Zertifikatsdienst (Keine)
FPT_STM.1	Enforcing Supporting	NTP Client::Core (Keine)
FPT_TST.1	Enforcing Supporting	Protection::Selbsttest Protection::Selbsttest
FTP_ITC.1/TLS	Enforcing	TLS-Server::Core

Weiter auf der nächsten Seite

SFR	Relation	Subsystem::Modul
	Supporting	(Keine)
FTP_ITC.1/VPN	Enforcing	VPN Client::Core
	Supporting	Administrationssystem::Management-Anwendung
FTP_TRP.1/Admin	Enforcing	Administrationssystem::HTTP-Server
	Supporting	VPN Client::Core

Tabelle C.1.: Zuordnung von Modulen zu SFRs

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 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.

[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 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.

Index der SFR