Sicherheitsvorgaben

für das

Produkt

VPNConnect Version 1.2.650

von

I-MOTION GmbH

Gesellschaft für Kommunikation & Service

Nordring 23, 90765 Fürth

Zertifizierungs-ID: **BSI-DSZ-CC-0288**

Datum: **14.02.2006**

Version Nr.: **1.11**

Autoren: **Eike Gehler, Matthias Faltenbacher**
AccSys GmbH, Lichtenbergstr. 8, 85748 Garching

http://www.accsys.de

Inhaltsangabe

Revision des Dokuments

Version	Datum	Änderungen	Autor
0.7	01.07.2004	Erstentwurf	Matthias Faltenbacher Eike Gehler
1.0	02.08.2004	Änderungen nach initialem Prüfbericht des Evaluators	Eike Gehler
1.1	26.11.2004	Einbringen von SNMP für Windows XP SP2 Support Änderungen nach BSI-Anforderungen	Matthias Faltenbacher Eike Gehler
1.2	02.12.2004	Änderungen nach Zuteilung Zertifizierungs-ID	Eike Gehler
1.3	10.01.2005	Änderungen nach Prüfbericht des Evaluators	Eike Gehler
1.4	10.03.2005	Änderungen nach Kommentar des BSI	Eike Gehler
1.5	29.03.2005	Rechtschreibfehler beseitigt	Eike Gehler
1.6	13.05.2005	Umformulierung T.7	Eike Gehler
1.7	12.07.2005	Endgültige Bezeichnung des EVG	Eike Gehler
1.8	22.08.2005	Änderung Tabelle 6.4	Eike Gehler
1.9	20.10.2005	Mindestvoraussetzung Windows 2000 geändert	Matthias Faltenbacher
1.10	17.11.2005	Versionsnummer auf 1.10 geändert	Eike Gehler
1.11	14.02.2006	A.AUTH, OE.6 modifiziert	Eike Gehler

1 ST-Einführung

1.1 ST Identifikation

Titel: Sicherheitsvorgaben für das Produkt VPNConnect Version 1.2.650 von I-MOTION GmbH, Version 1.11

Vertrauenswürdigkeitsstufe: EAL2

1.2 Konventionen, Terminologie und Abkürzungen

In diesem Abschnitt werden Formatierungskonventionen, Terminologie und Abkürzungen beschrieben, die im übrigen Teil des Dokuments Verwendung finden.

1.2.1 Konventionen

Dieser Abschnitt beschreibt die Konventionen, die im Kapitel 5 benutzt werden, um die Ausführung von CC Operationen auf Sicherheitsanforderungen zu kennzeichnen. Die CC erlauben es, dass mehrere Operationen auf funktionalen Anforderungen durchgeführt werden; *Zuweisung*, *Iteration*, *Verfeinerung* und *Auswahl* sind im Kapitel 2.1.4 im Teil 2 der CC definiert:

- Die Operation *Auswahl* erlaubt die Spezifikation von Bestandteilen, die aus einer in der Sicherheitsanforderung angegebenen Liste ausgewählt werden. Die Ergebnisse einer Operation *Auswahl* sind durch *unterstrichenen, kursiven Text* gekennzeichnet.

- Die Operation *Zuweisung* erlaubt die Spezifikation eines Parameters, der bei Spezifikation der Sicherheitsanforderung eingesetzt werden kann. Die Ergebnisse einer Operation *Zuweisung* sind durch Einschluss der Werte in eckigen Klammern [Werte(e)] gekennzeichnet.

- Die Operation *Verfeinerung* erlaubt es, Details zu einer Sicherheitsanforderung hinzuzufügen und dadurch die Anforderung einzuschränken. Verfeinerungen sind durch **fetten Text** gekennzeichnet.

1.2.2 Terminologie

Blowfish	Von Bruce Schneier entwickelter, lizenzfreier Verschlüsselungsalgorithmus (64-bit Blockchiffrierung, variable Schlüssellänge bis 448bit)
Branding	Eine Produktausprägung, die Defaultwerte für sicherheitsrelevante Einstellungen und Grafiken durch Konfigurationsdateien erhält.
Challenge	Zur Laufzeit generierter, eindeutiger Wert
Gateway	Übergangsrechner zwischen Netzwerken mit heterogener Netzwerkarchitektur.
Herstellerautorisierte Administratoren	Vertrauenswürdige Administratoren mit Herstellerautorisierung, die den EVG und sicherheitsrelevante Parameter vorkonfigurieren. Diese Administratoren erhalten durch den Hersteller spezifische zusätzliche Information die Konfiguration des EVG betreffend
Konfigurationsdatei	Von VPNConnect zur Speicherung von Default-Werten genutzte, verschlüsselte Datei
Produktivtunnel	Stehende VPN-Verbindung, die für den Produktivbetrieb genutzt wird.
Router	Ein Router stellt eine spezielle Art eines Gateways dar, da er nur die ersten 3 Schichten der beteiligten Teilnetze vorhalten muss. Ein Router wird deshalb auch als Level-3-Gateway bezeichnet. Mit ihm lassen sich nur Verbindungen zwischen IP-basierten Netzen herstellen
Spoofer	Eine Person oder ein Programm, die versucht, eine Identität eines Anderen anzunehmen.
Vertrautes Netz	Netzwerk oder Server, der nur durch den Tunnel erreichbar ist und durch Konfigurationsdateien oder Steuerfiles als vertrauenswürdig gekennzeichnet ist.
Authentifizierungstunnel	Stehende VPN-Verbindung, in der die Zertifikate für den Aufbau des endgültigen VPN-Tunnels von einem Zertifizierungsserver aus dem vertrauten Netz geladen werden können.

1.2.3 Abkürzungen

3DES	Triple-DES, dreifache (168 Bit) Schlüssellänge (RFC 3217)
AH	IP Authentication Header (RFC 2402)
CC	Common Criteria
CM	Configuration Management
CHAP	Challenge Authentication Protocol (RFC 1994)
DES	Data Encryption Standard, (56 Bit) Schlüssellänge (RFC 2419)
ESP	IP Encapsulating Security Payload (RFC 2406)
EVG	Evaluationsgegenstand
DTAG	Deutsche Telekom AG
ICMP	Internet Control Message Protocol (RFC 792)
IKE	Internet Key Exchange (RFC 2409)
IP	Internet Protocol (RFC 760)
IPSEC	Secure Internet Protocol (RFC 2401)
ISAKMP	Internet Security Association and Key Management Protocol (RFC 2408)
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol (RFC2661, 3193)
MD5	digital Message Digests - Version 5 (RFC 2403)
MFC	Microsoft Foundation Classes
NAT	Network Address Translation (RFC 2663, 2766)
NAT-T	Network Address Translation – Traversal (RFC 3193, draft-02)
RADIUS	Remote Authentication Dial-in User Service (RFC 2865)
RAS	Remote Access Service
RFC	Request For Comment
TCP/IP	Transmission Control Protocol/Internet Protocol (RFC 793)
SFP	Security Functional Policy
SNMP	Simple Network Management Protocol (RFC 1157)
TOE	Target of Evaluation
TSF	TOE Security Function(s)
VISP	Virtual Internet Service Provider
VPN	Virtual Private Network
www	World Wide Web
X.509	Standard für Echtheitsbestätigungen von/mit Zertifikaten (RFC 2510)

1.3 ST Übersicht

Bei VPNConnect handelt sich um eine Anwendung, die auf Basis der Betriebssysteme Microsoft Windows 2000 und Windows XP betrieben werden kann. VPNConnect stellt dieselben Anforderungen an die Hardware wie die Betriebssysteme Microsoft™ Windows 2000 und Microsoft™ Windows XP.

VPNConnect ermöglicht es Benutzern mittels VPN einen gesicherten Datenaustausch einzuleiten.

Zum Aufbau der VPN-Verbindungen werden die im Betriebssystem vorhandenen IP-Sicherheitsrichtlinien verwendet, für die Zertifikatsverwaltung werden die vom Betriebsystem zur Verfügung gestellten Zertifikatsspeicher benutzt.

Das gesamte Management der IP-Sicherheitsrichtlinien und das Zertifikatsmanagement werden von VPNConnect übernommen.

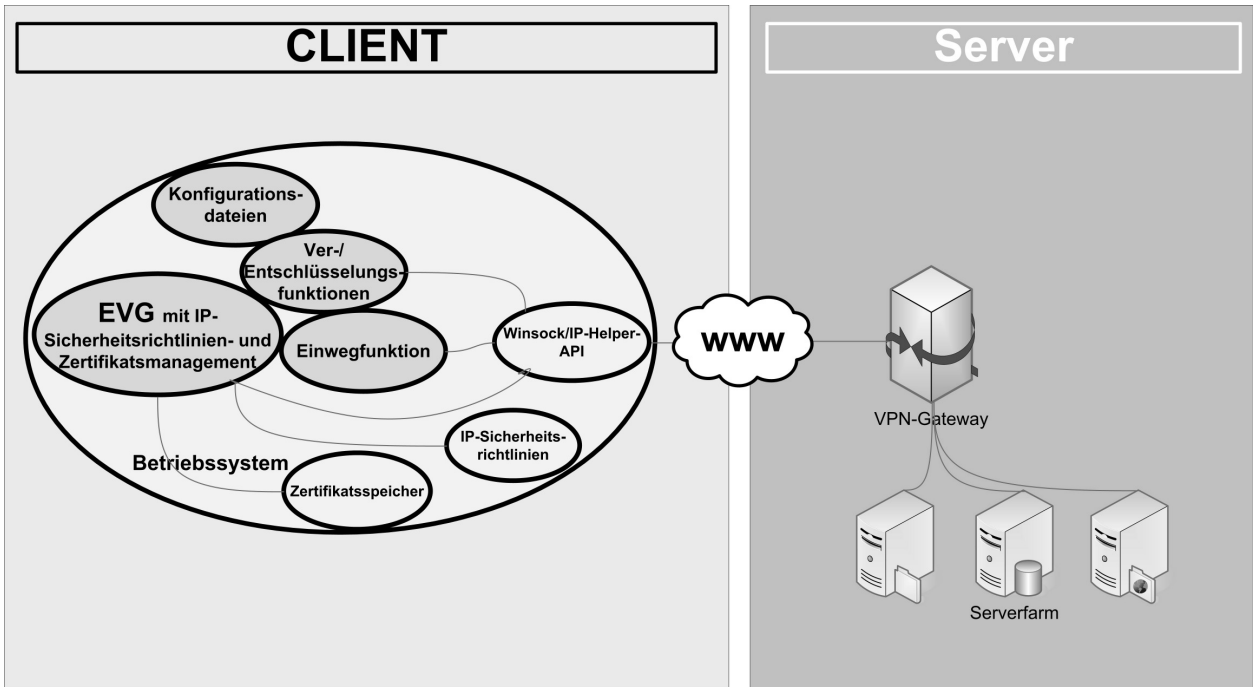

Abbildung 1-1 – EVG im Betriebssystemumfeld

Wie aus der Abbildung ersichtlich ist, benutzt der EVG zur Kommunikation in das WWW clientseitig Funktionsbibliotheken des Betriebssystems, wie die Winsock oder die IP-Helper-API. Zertifikate werden vom EVG mittels Aufrufen in Funktionsbibliotheken in den betriebssystemeigenen Zertifikatsspeicher importiert oder daraus gelöscht.

Der eigentliche Tunnelaufbau wird ebenso mittels IP-Sicherheitsrichtlinienbibliotheken durch das Betriebssystem initiiert.

VPNConnect ist für Benutzer ohne besondere Sachkenntnis im Bereich EDV konzipiert und für den Einsatz in normaler Büro- bzw. Praxisumgebung geeignet.

1.4 Postulat der Übereinstimmung mit CC

Diese Sicherheitsvorgaben basieren auf den „Common Criteria“ (ISO 15408), die in der deutschen Übersetzung aus den drei folgenden Teilen bestehen:

> [CC_P1] Common Criteria, Teil 1: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik – Teil 1: Einführung und allgemeines Modell, Version 2.1, August 1999
>
> [CC_P2] Common Criteria, Teil 2: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik – Teil 2: Funktionale Sicherheitsanforderungen, Version 2.1, August 1999
>
> [CC_P3] Common Criteria, Teil 3: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik – Teil 3: Anforderungen an die Vertrauenswürdigkeit, Version 2.1, August 1999.

Der EVG ist Teil 2 erweitert.

Der EVG ist konform zu Teil 3 und erfüllt die Anforderungen des Vertrauenswürdigkeitspaketes EAL2.

2 EVG Beschreibung

2.1 Einführung

VPNConnect ist eine Zugangssoftware für das Betriebssystem Microsoft Windows (Windows 2000 oder Microsoft Windows XP), die es den Benutzern ermöglicht, gesicherte VPN-Verbindungen zu von I-MOTION verwalteten Servern aufzubauen. Dies kann über bereits vorhandene Endgeräte wie etwa einem analogen Modem, mit ISDN, DSL, oder aus einer vorhandenen LAN-Verbindung erfolgen.

Eine Einführung in die Thematik VPN findet man im Anhang A (Einführung in VPN).

VPNConnect bietet umfassende Sicherheitsfunktionen, die für einen sicheren Datenaustausch notwendig sind:

- Identifikation und Authentisierung
- Zugriffskontrolle
- Kryptographisches Schlüsselmanagement
- Schutz von Konfigurationsdateien
- IP-Sicherheitsrichtlinienverwaltung
- Spezifikation der Geheimnisse

Die Sicherheitsfunktionen im einzelnen werden im Kapitel 6.1 erläutert.

Bei der Umsetzung der einzelnen Funktionen bedient sich VPNConnect Funktionen und Komponenten des Betriebssystems (in den Bereichen „Kryptographisches Schlüsselmanagement“ und „IP-Sicherheitsrichtlinienverwaltung“).

Hierauf wird in den Beschreibungen der einzelnen Sicherheitsfunktionen verwiesen.

Im Kapitel 2.6 wird der Gesamtablauf von VPNConnect beschrieben.

2.2 Kurzzusammenfassung der Sicherheitsfunktionen

2.2.1 Identifikation und Authentisierung

Die Identität des Benutzers muss eindeutig nachgewiesen sein. Dies geschieht im EVG sowohl über Benutzername und Kennwort als auch mit sog. „Zertifikaten“, die individuell auf den Benutzer ausgestellt werden. Die Identifikation und Authentisierung der Benutzer erfolgt hierbei extern gegenüber einem RADIUS-Server (bei Interneteinwahlverbindungen) und mittels einem Client/Server-Mechanismus gegenüber einem Authentifizierungsserver.

Die Funktionalität der Authentisierung und Identifikation gegenüber dem Authentifizierungsserver wird im EVG durchgeführt. Das Passwort wird hierbei nicht an den Authentifizierungsserver übermittelt. Zur Absicherung der Kommunikation zwischen EVG und Authentifizierungsserver wird neben der getunnelten Verbindung und dem verschlüsselt übertragen Usernamen zusätzlich eine Funktion zur Generierung von Challenges benutzt.

Zertifikate im X.509 Standard werden von einer I-MOTION-eigenen Zertifizierungsstelle (Trust Center) erstellt und ihre Berechtigung überprüft. VPNConnect und die von I-MOTION benutzten Gateways authentifizieren sich gegenseitig über Zertifikate. Ein Aufbau eines Tunnels kann nur erfolgen wenn die verwendeten Zertifikate als gültig verifiziert sind.

Nach Start von VPNConnect wird, wenn benötigt, eine Internetverbindung aufgebaut und der Benutzer gegenüber einem RADIUS-Server authentifiziert. Anschließend wird ein generischer VPN-Tunnel (Authentifizierungstunnel) zu einem VPN-Gateway von I-MOTION aufgebaut. Nach diesem Aufbau wird der Benutzer im EVG gegenüber einem Authentifizierungsserver, der im geschützten Netz hinter dem VPN-Gateway steht, identifiziert und authentisiert.

2.2.2 Zugriffskontrolle

Nach der erfolgreichen Authentifizierung wird über ein Konfigurationsfile das Regelwerk geladen. Dieses Regelwerk enthält alle benötigten Informationen für den Aufbau des Produktivtunnels, insbesondere erlaubtes Zielnetz und Download-URL für den Download der Benutzer-Zertifikate für den Produktivtunnel.

2.2.3 Kryptographisches Schlüsselmanagement

VPNConnect enthält umfangreiche Routinen zum Management von Zertifikaten. Es werden die benötigten privaten Zertifikate zum Aufbau der Tunnel in die Zertifikatsspeicher des Betriebssystems importiert und nach Ende der VPN-Verbindung wieder gelöscht. Ebenso werden die öffentlichen Zertifikate der I-Motion Gateways zur Laufzeit in die Zertifikatsspeicher des Betriebssystems importiert.

2.2.4 Schutz von Konfigurationsdateien

Sicherheitsrelevante Bestandteile der Zugangssoftware sind verschlüsselt. Dies dient zum Schutz vor Veränderung der Initialwerte zum Aufbau der VPN-Tunnel.

Ebenso erfolgen die Rückgaben des Authentifizierungsservers an den EVG verschlüsselt und können nur vom EVG entschlüsselt werden.

2.2.5 IP-Sicherheitsrichtlinienverwaltung

Umfangreiche Netzdefinitionen werden über das Sicherheitspolitikmanagement abgebildet. So wird sichergestellt, dass bei einem Aufbau eines VPN nur Zugriff auf das geschützte Netz hinter dem VPN-Gateway und das evtl. vorhandene lokale Netz zugegriffen werden kann.

Die Vertraulichkeit der Daten im Produktivtunnel wird mittels verschlüsselter Datenpakete wie z.B. der sog. Triple DES Chiffrierung (3DES) gewährleistet. Die Verschlüsselung der Daten wird durch das Betriebssystem übernommen.

Die Integrität der Datenpakete innerhalb eines Tunnels wird mit einer Checksumme geprüft. Dieses Verfahren wird mit Hash-Algorithmen wie z.B. MD5 oder SHA-1 durchgeführt. Die Integrität der Daten wird durch Funktionen des Betriebssystems sichergestellt.

Das gesamte Management der IP-Sicherheitsrichtlinienverwaltung (Anlegen, Löschen, Modifizieren, Aktivieren und Deaktivieren von Sicherheitsrichtlinien) ist Bestandteil des EVG.

2.2.6 Spezifikation der Geheimnisse

Für die Authentifizierung am Authentifizierungsserver verwendet VPNConnect einen Challenge-Responsemechanismus. Hierzu werden vom EVG Mechanismen zur Laufzeitgenerierung von Geheimnissen bereitgestellt, die bei diesem Authentifizierungsmechanismus verwendet werden.

2.3 Systemvoraussetzungen

VPNConnect kann auf Basis der Betriebssysteme Microsoft™ Windows 2000, und Microsoft Windows XP betrieben werden.

2.4 Lieferumfang

Zum Lieferumfang von VPNConnect gehören:

Nr.	Typ	Bezeichnung	Auslieferungsmedium
1	Software	VPNConnect Version 1.2.650	CD
2	Dokument	Handbuch für Systemverwalter und Benutzer	CD
3	Dokument	Benutzerhandbuch	CD

Tabelle 2.1 - Lieferumfang

2.5 Installation

VPNConnect ist für Benutzer ohne besondere Kenntnisse der EDV entwickelt worden und für den Einsatz in normaler Büroumgebung bzw. Arztpraxis geeignet.

Die Installation der Software muss durch einen Administrator erfolgen, der die Parametrierung des Betriebssystems vornimmt.

Die Grundeinstellungen der Konfigurationsdateien können nur von Administratoren mit Herstellerautorisierung geändert werden.

2.6 Beschreibung des Gesamtablaufs

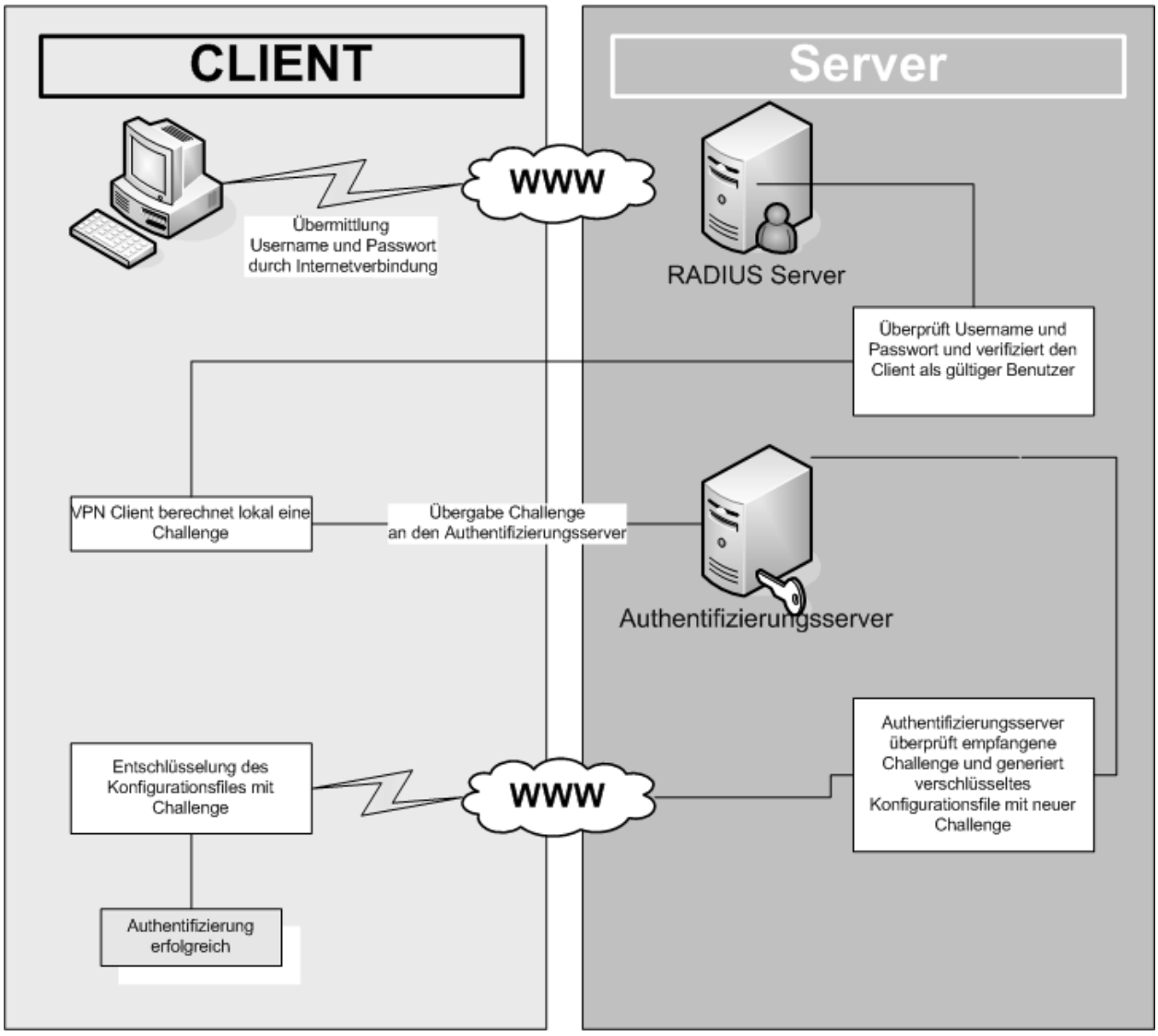

Abbildung 2-1 - Gesamtablauf

Sämtliche ausgelagerte Informationen in Konfigurationsdateien (Defaultwerte) sind mittels des Blowfish-Algorithmus verschlüsselt.

Nach erfolgreicher Konfiguration von VPNConnect wird bei Start der Applikation ein Benutzerdialog angezeigt, in dem der Benutzer Benutzername und Kennwort eingeben muss. Die Eingabe des Kennworts wird auf dem Bildschirm durch das Windowstypische Zeichen „*“ wiedergegeben, so dass das Kennwort nicht im Klartext sichtbar ist.

Bei Klick auf den Button Verbinden wird zunächst eine IP-Sicherheitsrichtlinie (DialIn) für die Interneteinwahl erstellt, die außer den gängigen Zugriffen nach außen alle Zugriffe auf das System blockt. Diese Sicherheitsrichtlinie wird nun aktiviert. Anschließend erfolgt (bei Konfiguration einer Einwahl- oder DSL-Verbindung) der Internet-Verbindungsaufbau. Hier werden die vom Benutzer eingegebenen Benutzerdaten am I-MOTION RADIUS-Server mittels CHAP authentifiziert. Bei falsch eingegebenen Benutzernamen/Kennwort wird die Internetverbindung serverseitig getrennt und ein RAS-Error zurückgegeben, aus dem nicht ersichtlich ist, ob Benutzername oder Kennwort falsch waren.

Bei erfolgreicher Einwahl werden nun die initial ausgelieferten Zertifikate in die Windowseigenen Zertifikatsspeicher importiert. Das Client-Zertifikat, das passwortgeschützt ist, wird automatisiert ohne Benutzerinteraktion importiert und ist nicht exportierbar.

Nun wird eine IP-Sicherheitsrichtlinie (VPN-Certserver) auf die in den Konfigurationsdateien angegebenen VPN-Server angelegt. Diese beinhaltet zwei IPSEC basierte Tunnel, bei denen als Verschlüsselungsalgorithmus z.B. 3DES mit MD5-Hash angewandt wird und blockiert jeglichen anderen IP-Verkehr. Diese neue IP-Sicherheitsrichtlinie (VPN-Certserver) wird nun aktiviert was die bisherige Aktivierung der Sicherheitsrichtlinie DialIn überschreibt.

Anschließend wird ein in den Konfigurationsdateien angegebener Rechner hinter dem Servertunnelendpunkt mittels SNMP oder ICMP kontaktiert, was den Clientrechner und den VPN-Server zum Aufbau der in der IP-Sicherheitsrichtlinie (VPN-Certserver) angegebenen Tunnel bringt. Ist die SNMP/ICMP-Kommunikation nach 10 Versuchen nicht erfolgreich, wird wieder die IP-Sicherheitsrichtlinie DialIn aktiviert und es wird ein Fehler ausgegeben.

Nach erfolgreichem VPN-Verbindungsaufbau wird - initiiert vom EVG - von einem Authentifizierungsserver nach dem Tunnelendpunkt unter Verwendung eines Challenge-Responsemechanismus und weiteren im Konfigurationsfile angegebenen Informationen eine Steuerdatei heruntergeladen, die mittels des Blowfish-Algorithmus verschlüsselt ist, lediglich im Speicher von VPNConnect interpretiert und nur vom EVG entschlüsselt werden kann.

Das Passwort des Benutzers wird hierbei nicht an den Authentifizierungsserver übermittelt. Der Authentifizierungsserver verschlüsselt u.a. mit der übertragenen Challenge. Der EVG kann unter Zuhilfenahme der in einer Funktion zur Generierung von Challenges generierten Challenge das übertragene Steuerfile entschlüsseln.

Dieses Steuerfile enthält den Downloadpfad zu den Zertifikaten des Produktivtunnels sowie die IP-Adressen und Subnetzmasken des Produktivtunnels. Die Informationen erhält der Authentifizierungsserver aus den I-MOTION Benutzerdatenbanken, die im Rechenzentrum von I-MOTION befindlich sind. Ist der übergebene Benutzername falsch oder ist der Benutzer in der Datenbank als nicht für VPN gestattet markiert wird im Steuerfile eine Fehlernummer zurückgegeben, was die Aktivierung der IP-Sicherheitsrichtlinie DialIn bewirkt, womit der VPN-Tunnel abgebaut wird. Weiterhin wird ein Fehler ausgegeben.

Bei falsch eingegebenem Kennwort führt die Entschlüsselung des vom Authentifizierungsserver generierten Konfigurationsfiles zu keinem gültigen Ergebnis. Auch in diesem Fall wird die IP-Sicherheitsrichtlinie DialIn aktiviert, womit der VPN-Tunnel abgebaut wird. Ebenso wird auch hier ein Fehler ausgegeben, aus dem nicht hervorgeht, ob Benutzername oder Kennwort falsch eingegeben worden sind.

Nach Download der Zertifikate werden diese auf dem Datenträger gespeichert. Die Zertifikate werden zur Laufzeit des EVG unverschlüsselt auf der Festplatte des Benutzers gespeichert, das zum Import der Zertifikate benötigte Passwort ist nur dem EVG bekannt und wird während der Laufzeit im Speicher des EVG gehalten.

Die IP-Sicherheitsrichtlinie DialIn wird wieder aktiviert, was den Abbau des Tunnels zum Authentifizierungsserver mit sich bringt. Die downgeloadeten Zertifikate werden nun in die Windows-Zertifikatsspeicher importiert, das bisherige private Zertifikat gelöscht. Nun wird mit den im Steuerfile übermittelten IP-Adressen und Subnetzmasken die IP-Sicherheitsrichtlinie VPN-Produktiv erstellt und aktiviert. Je nach verwendetem Szenario kann auch ein IPSEC/L2TP-Tunnel aufgebaut werden, in dem dann der Client eine private IP-Adresse aus einem privaten Adressraum zugewiesen bekommt. Der übermittelte Zielserver wird nun mittels SNMP/ICMP kontaktiert. Schlägt der Kontakt zum Zielserver mittels SNMP/ICMP fehl (Zielserver nicht erreichbar), wird der Tunnel abgebaut, die IP-Sicherheitsrichtlinie DialIn aktiviert und es wird ein Fehler ausgegeben.

Der Produktivtunnel steht nach erfolgreichem Kontakt zum Zielserver - vor weiterem IP-Verkehr gesichert - zur Verfügung. Timergesteuert überprüft der EVG (über eine Betriebssystemfunktion) wiederkehrend den Tunnel auf Verfügbarkeit und baut diesen ab, wenn keine SNMP- oder ICMP-Verbindung mehr möglich ist.

Solange ein- und dieselbe Instanz von VPNConnect läuft, ist nach einem VPN-Verbindungsabbau und auch nach einem Internetverbindungsabbau kein Aufbau zum Authentifizierungsserver zum erneuten Download der Zertifikate notwendig, da diese bereits auf dem Datenträger temporär gespeichert werden. Im Fehlerfall (SNMP/ICMP nicht erfolgreich) werden die zwischengespeicherten Zertifikate gelöscht. Bei erneuter Einwahl wird eine Authentisierung beim Authentifizierungsserver mit nachfolgendem Download der Zertifikate durchgeführt.

3 EVG Sicherheitsumgebung

Dieses Kapitel beschreibt die Annahmen über den Betrieb des EVG im Teilkapitel 3.1, führt die adressierten Bedrohungen im Teilkapitel 3.2 auf und beschreibt im Teilkapitel 3.3 die organisatorische Sicherheitspolitiken, mit denen der EVG übereinstimmen muss.

3.1 Annahmen

A.RADIUS Netzseitig steht ein RADIUS-Server zur Verfügung, an dem sich Clients, die eine Interneteinwahlverbindung aufbauen müssen, um Zugriff zum Internet zu erhalten, authentifizieren müssen. Die Authentifizierung muss über CHAP erfolgen.

A.VISP Clients, die eine DSL-Einwahlverbindung aufbauen müssen, um Zugriff zum Internet zu erhalten, müssen netzseitig über die VISP (Virtual ISP)-Struktur der DTAG oder einer vergleichbaren Struktur zur Verifizierung der eingegebenen Daten authentifiziert werden.

A.VPNGATE Als VPN-Gateway werden herstellerseitig Standard-NAT-T-fähige IPSEC VPN-Gateways verwendet (z.B. TelcoTech LISS pro).[1]

A.AUTH Zur Authentifizierung aller Clients wird herstellerseitig ein geeigneter Authentifizierungsserver verwendet. I-MOTION stellt sicher, dass sich der Authentifizierungsserver in einem eigenen Subnetz befindet, in dem sich kein weiterer Rechner findet.[2]

A.CREATECERT I-MOTION erstellt eindeutige X.509-Zertifikate für jeden Benutzer von VPNConnect. Diese Zertifikate werden als fortgeschrittene Zertifikate auf Basis des Root-Zertifikats von I-MOTION erstellt.

A.ACCESSCERT Die erstellten Benutzer-Zertifikate, stehen im Zugriff des Authentifizierungsservers, um zur Laufzeit von den Clients heruntergeladen werden zu können. Dieser Zugriff ist ausschließlich über ein aufgebautes VPN möglich.

A.CREATEGENCERT I-MOTION erstellt für jedes Branding ein generisches Zertifikat, das für den Aufbau des Authentifizierungstunnels benutzt wird. Dieses Zertifikat wird durch die Installationsroutine von VPNConnect auf den physikalischen Datenträger aufgespielt.

---

[1] Hinweis: Die VPN-Tunnelverbindungen werden zu im Client in der Konfiguration verschlüsselt angegebenen IP-Adressen aufgebaut. Der serverseitige Tunnelendpunkt ist durch diese angegebene IP-Adresse vorgegeben.

[2] Hinweis: Der Authentifizierungsserver gibt die pro Benutzer erlaubten Netze in einem definierten Konfigurationsfile an den Client zurück. Die Verbindung zwischen Client und Authentifizierungsserver erfolgt gesichert durch den Zertifizierungs-Tunnel.

A.TRUSTEDADMIN Mit der Administration des EVG ist mindestens eine kompetente und vertrauenswürdige, und ausgebildete Person zu betrauen. Diese Administratoren müssen ihre Aufgaben gewissenhaft, umsichtig und verantwortungsbewusst wahrnehmen.

A.TRUSTEDUSER Alle Benutzer des EVG sollen ihn im Rahmen ihrer Aufgabenerfüllung nutzen. Sie sollen im Rahmen ihrer Möglichkeiten sicherstellen, dass vertrauliche Informationen (insbesondere Passwörter) nicht zur Kenntnis Anderer gelangen.

A.LOCKEDCOMPUTER Es muss durch geeignete technische und organisatorische Maßnahmen sichergestellt sein, dass die verwendeten Hardwarekomponenten, insbesondere Magnetplatte(n), durch geeignete bauliche oder andere physische Sicherungsmaßnahmen vor Entwendung geschützt sind und Unberechtigte keinen Zugriff auf physikalischen Speicherort des EVG erhalten.

3.2 Bedrohungen

Unter Berücksichtigung der in Kapitel 3.1 aufgeführten Annahmen verbleiben die in den nachfolgenden Teilkapiteln aufgeführten relevanten Bedrohungen. Im Teilkapitel 3.2.1 werden diejenigen Bedrohungen identifiziert, denen der EVG zu begegnen hat und im Teilkapitel 3.2.2 jene, denen von der Betriebsumgebung zu begegnen ist.

3.2.1 Bedrohungen, denen vom EVG zu begegnen ist

Nachfolgend werden zunächst die schutzwürdigen Objekte, die Subjekte und die Urheber von Bedrohungen definiert.

Schutzwürdige Objekte

- Datenpakete die über den EVG gesendet oder empfangen werden
- Konfigurationsdaten, die den sicheren Betrieb des EVG ermöglichen
- Zertifikate

Subjekte

- Autorisierte Personen, die den EVG nutzen, um eine VPN Verbindung aufzubauen.
- Vertrauenswürdige Administratoren des Betriebssystems, die den EVG installieren und nicht-sicherheitsrelevante Parameter konfigurieren.
- Vertrauenswürdige Administratoren mit Herstellerautorisierung, die den EVG und sicherheitsrelevante Parameter vorkonfigurieren

Urheber von Bedrohungen

- Angreifer mit Zugang zu einem Netz über das zu schützende Daten übertragen werden und mit der Absicht, übertragene Daten abzuhören, zu modifizieren, einzufügen oder zu löschen.

- Angreifer mit Zugang zu einer Arbeitsstation, an der VPNConnect aufgerufen werden kann und mit der Absicht, unberechtigter Weise eine VPN-Verbindung zu initiieren und/oder vorhandene Client-Zertifikate zu entwenden.

Es wird davon ausgegangen, dass ein Angreifer begrenzte technische und zeitliche Möglichkeiten besitzt und über allgemein verfügbare Kenntnisse der Informationstechnik, des Betriebssystems und des EVG verfügt.

VPNConnect sichert die Integrität und die Vertraulichkeit der mit VPNConnect aufgebauten VPN Verbindung ab. Als Bedrohungen werden dabei angenommen:

T.1 *Nicht authentifizierter Benutzer*
Zugriff auf Funktionen von VPNConnect durch Personen, die nicht zur Benutzung von VPNConnect berechtigt sind

T.2 *Nicht autorisierter Zugriff*
Zugriff auf Funktionen von VPNConnect durch authentisierte Benutzer in einer nicht autorisierten Weise

T.3 *Lesender Zugriff auf von VPNConnect verwaltete Konfigurationsdaten unter Umgehung der Anwendung VPNConnect.*

Es wird davon ausgegangen, dass ein Angreifer alle Möglichkeiten wahrzunehmen sucht, lesenden Zugriff auf Konfigurationsdaten zu erhalten ohne Zugang zur Anwendung VPNConnect zu haben.

Als mögliche Angriffsformen sind hierbei der Zugriff über andere Anwendungen, über das Betriebssystem oder über Ausnutzung des physischen Zugangs zur Festplatte zu nennen.

T.4 *Manipulation auf von VPNConnect verwaltete Konfigurationsdaten unter Umgehung der Anwendung VPNConnect.*

Es wird davon ausgegangen, dass ein Angreifer unautorisiert und unerkannt versucht, die Konfigurationsdaten zu modifizieren.

Als mögliche Angriffsformen sind hierbei der Zugriff über andere Anwendungen, über das Betriebssystem oder über Ausnutzung des physischen Zugangs zur Festplatte zu nennen.

3.2.2 Bedrohungen, denen durch den EVG und die IT-Umgebung zu begegnen sind

T.5 *Unbefugte Kenntnisnahme von Benutzerdaten auf dem Übertragungsweg*

Es wird davon ausgegangen, dass ein Angreifer unautorisiert und unerkannt versucht Informationen auf dem Übertragungsweg abzuhören, um dadurch Kenntnis der Benutzerdaten zu erlangen.

Als mögliche Angriffsformen sind hierbei der Zugriff über Spoofer oder Router mit gefälschten IP-Adressen zu nennen.

T.6 *Versuch, Benutzerdaten auf dem Übertragungsweg zu modifizieren*

Es wird davon ausgegangen, dass ein Angreifer unautorisiert und unerkannt versucht Benutzerdaten auf dem Übertragungsweg zu modifizieren, einzufügen, umzuordnen, zu löschen oder zu wiederholen.

Als mögliche Angriffsformen sind hierbei der Zugriff über Spoofer oder Router mit gefälschten IP-Adressen zu nennen.

T.7 *Vortäuschung einer Identität durch Eingriff auf dem Übertragungsweg*

Es wird davon ausgegangen, dass ein Angreifer unautorisiert und unerkannt versucht die Identität eines Benutzers auf dem Übertragungsweg anzunehmen, um dadurch eine unzulässige Kommunikationsverbindung aufzubauen.

Als mögliche Angriffsformen sind hierbei der Zugriff über Spoofer oder Router mit gefälschten IP-Adressen zu nennen.

3.3 Organisatorische Sicherheitspolitiken

In Ergänzung zur Abwehr der Bedrohungen, die in den vorhergehenden Teilkapiteln beschrieben sind, soll VPNConnect die folgenden Sicherheitspolitiken unterstützen:

P.1 **(Administratorbestimmte Zugriffskontrolle):**
Die Installation für die Benutzer soll allein durch Administratoren mit auf dem Installationszielsystem vorhanden Administrationsrechten erfolgen.

P.2 **(Administratorbestimmte Aktionen):**
Die Aktionen autorisierter Benutzer sollen von den Administratoren mit Herstellerautorisierung vorgegeben werden.

4 Sicherheitsziele

Im Teilkapitel 4.1 werden die Sicherheitsziele für den EVG und im Teilkapitel 4.2 die Sicherheitsziele für die Umgebung beschrieben.

4.1 Sicherheitsziele für den EVG

O.AUTH Der EVG muss den Zugriff auf die im EVG bereitgestellten Funktionen auf diejenigen Personen beschränken, die authentisiert sind.

O.AUTOR Der EVG muss den Zugriff auf IP-Adressbereiche (geschütztes Netz) begrenzen, für den der jeweilige Benutzer autorisiert ist.

O.CERT Der EVG muss die Funktionalität des für den Aufbau eines VPN-Tunnels benötigten Zertifikatsmangements zum Importieren und Löschen von Zertifikaten bereitstellen.

O.POLICY Der EVG muss die Funktionalität der für den Aufbau eines VPN-Tunnels benötigten Sicherheitsrichtlinienverwaltung zum Erstellen, Modifizieren, Aktivieren, Deaktivieren und Löschen von Sicherheitsrichtlinien bereitstellen.

O.CHGCONFIG Der EVG muss sicherstellen, dass unautorisiert durchgeführte Änderungen an Konfigurationsdateien erkannt werden können.

O.READCONFIG Der EVG muss sicherstellen, dass Konfigurationsdateien nur von herstellerautorisierten Personen gelesen werden können.

O.INSTALL Der EVG muss sicherstellen, dass die Installation auf ein Zielsystem nur durch Administratoren des Betriebssystems erfolgt.

4.2 Sicherheitsziele für die Umgebung

OE.1 Es muss durch geeignete technische und organisatorische Maßnahmen sichergestellt sein, dass die verwendeten Hardwarekomponenten, insbesondere Magnetplatte(n), durch geeignete bauliche oder andere physische Sicherungsmaßnahmen vor Entwendung geschützt sind und Unberechtigte keinen Zugriff auf physikalischen Speicherort des EVG erhalten.

OE.2 Das auf dem Zielsystem installierte Betriebsystem muss in der Lage sein, zertifikatsbasierte VPN-Verbindungen zu durch den EVG definierten geschützten Netzen aufzubauen. Als VPN-Verbindungsarten können z.B. IPSEC, L2TP oder IPSEC/L2TP verwendet werden.

Hierbei müssen folgende Anforderungen erfüllt werden:

- Es muss sichergestellt sein, dass die Herkunft von Datenpaketen, die von autorisierten Benutzern in geschützte Netzwerke geschickt werden, vom Empfänger verifiziert werden kann.
- Es muss sichergestellt sein, dass Datenpakete, die von autorisierten Benutzern in geschützte Netzwerke geschickt und empfangen werden, von keiner Seite wiederholt gesendet werden.

- Es muss sichergestellt sein, dass Datenpakete, die von autorisierten Benutzern in geschützte Netzwerke geschickt und empfangen werden, verschlüsselt sind.

OE.3 Zur Authentifizierung der Benutzer des EVGs bei Interneteinwahlverbindungen muss netzseitig ein RFC 2865-konformer RADIUS-Server bereitgestellt werden. Dieser Radius-Server muss eingehende RADIUS-Anfragen mittels CHAP authentifizieren.

OE.4 Zugriff auf VISP (Virtual ISP)-Struktur der DTAG oder einer vergleichbaren Struktur zur Authentifizierung von DSL-Benutzern ist erforderlich.

OE.5 Als VPN-Gateways müssen Standard-NAT-T-fähige VPN-Gateways vorhanden sein (z.B. TelcoTech LISS pro).

OE.6 Es ist ein Authentifizierungsserver bereitgestellt, der die pro Benutzer erlaubten Netze in einem definierten und verschlüsselt übertragenen Konfigurationsfile an den Client zurückgibt. Dieser Server ist im gesicherten Netz nach einem VPN-Gateway zu platzieren. Es ist sicherzustellen, dass sich der Authentifizierungsserver in einem eigenen Subnetz befindet, in dem sich kein weiterer Rechner findet.

OE.7 Es ist ein Trustcenter für die Erstellung von eindeutigen X.509-Zertifikate für jeden Benutzer von VPNConnect aufzubauen. Zu erstellende Zertifikate werden als fortgeschrittene Zertifikate erstellt.

OE.8 Die erstellten Benutzer-Zertifikate, müssen im Zugriff des Authentifizierungsservers stehen. Dieser Server ist im gesicherten Netz nach einem VPN-Gateway zu platzieren. Er kann physikalisch dem Authentifizierungsserver entsprechen.

OE.9 Für jedes Branding ist ein generisches Zertifikat für die Clients zu erstellen, das für den Aufbau des Authentifizierungstunnels benutzt wird. Dieses Zertifikat wird durch die Installationsroutine von VPNConnect auf den physikalischen Datenträger aufgespielt.

OE.10 Mit der Administration des EVG ist mindestens eine kompetente und vertrauenswürdige, und ausgebildete Person betraut. Diese Administratoren erfüllen ihre Aufgaben gewissenhaft, umsichtig und verantwortungsbewusst.

OE.11 Alle Benutzer des EVG benutzen den EVG im Rahmen ihrer Aufgabenerfüllung. Sie stellen sicher, dass vertrauliche Informationen (insbesondere Passwörter) nicht zur Kenntnis Anderer gelangen.

5 IT Sicherheitsanforderungen

Dieses Kapitel beschreibt die IT-Sicherheitsanforderungen in den Teilkapiteln 5.1 (EVG Sicherheitsanforderungen) und 5.2 (Sicherheitsanforderungen an die IT-Umgebung).

5.1 EVG Sicherheitsanforderungen

Dieses Kapitel beschreibt die funktionalen Sicherheitsanforderungen an den EVG im Teilkapitel 5.1.1 und die Anforderungen an die Vertrauenswürdigkeit des EVG im Teilkapitel 5.1.2.

5.1.1 Funktionale Sicherheitsanforderungen an den EVG

Alle Anforderungen an den EVG sind bis auf die explizit dargelegten Anforderungen FIA_UAU.EX.1, FIA_UID.EX.1, FPT_ITT.EX.1 und FDP_IFF.EX.1 dem Teil 2 der CC entnommen.

Familie FCS_CKM Kryptographisches Schlüsselmanagement

FCS_CKM.2 Verteilung des kryptographischen Schlüssels

FCS_CKM.2.1 Die TSF müssen die kryptographischen Schlüssel nach einer spezifizierten Methode zur Verteilung des kryptographischen Schlüssels [Download], die den **nachstehenden Anforderungen** entspricht, verteilen.

a) Der Download wird vom Client nach Authentisierung am Authentifizierungsserver initiiert.

b) Der Download erfolgt von einem Pfad, der dem Client vom Authentifizierungsserver als Ergebnis der Authentisierung übermittelt wird.

c) Der Download erfolgt gesichert durch den Authentifizierungstunnel.

FCS_CKM.3 Zugriff auf einen kryptographischen Schlüssel

FCS_CKM.3.1 Die TSF müssen [Lesezugriffe] gemäß einer spezifizierten Zugriffsmethode auf kryptographische Schlüssel [Import in Windows-Zertifikatsspeicher], die den **nachfolgenden Anforderungen** entspricht, durchführen.

a) Private Zertifikate sind durch Passwort geschützt.

b) Private Zertifikate lassen sich nur durch Angabe des korrekten Passworts in den Windows-Zertifikatsspeicher importieren.

c) Passwörter für generische Zertifikate zum Aufbau des Authentifizierungstunnels sind in der Konfigurationsdatei verschlüsselt gespeichert enthalten.

d) Passwörter für private Benutzer-Zertifikate zum Aufbau des Produktivtunnels werden dem Client vom Authentifizierungsserver als Ergebnis der Authentisierung übermittelt.

FCS_CKM.4 Zerstörung des kryptographischen Schlüssels

FCS_CKM.4.1 Die TSF müssen die kryptographischen Schlüssel nach einer spezifizierten Methode zur Zerstörung des kryptographischen Schlüssels [Löschen des Zertifikats von Datenträger, Entfernen des Zertifikats aus Windows-Zertifikatsspeicher], die den **nachfolgenden Anforderungen** entspricht, zerstören.

a) Nach Abbau jedes Tunnels werden die Zertifikate aus dem Windows-Zertifikatsspeicher entfernt.

b) Jede Unterbrechung der Verbindung zu dem angegebenen Produktivservern führt zu einem sofortigen Abbau des Tunnels.

c) Private Benutzer-Zertifikate zum Aufbau des Produktivtunnels werden zusätzlich bei Beendigung VPNConnect physikalisch vom Datenträger gelöscht.

Familie FDP_ACC Zugriffskontrollpolitik

FDP_ACC.2 Vollständige Zugriffskontrolle

FDP_ACC.2.1 Die TSF müssen die [Zugriffskontrollpolitik] für [den lokalen Client und das geschützte Netz] und alle durch die SFP abgedeckten Operationen zwischen den Subjekten und Objekten durchsetzen.

FDP_ACC.2.2 Die TSF müssen sicherstellen, dass alle Operationen zwischen jedem Subjekt im TSC und jedem Objekt im TSC durch eine SFP für Zugriffskontrolle abgedeckt sind.

Familie FDP_ACF Zugriffskontrollfunktionen

FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen

FDP_ACF.1.1 Die TSF müssen die [Zugriffskontrollpolitik] für Objekte **basierend auf** [IP-Adressbereichen und Zertifikaten] durchsetzen.

FDP_ACF.1.2 Die TSF müssen die folgenden Regeln durchsetzen, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist:

[

a) Ein Import eines auf dem Datenträger mitinstallierten generischen Zertifikats zum Aufbau der Authentifizierungstunnel in den Windows-Zertifikatsspeicher ist nur möglich, wenn das Zertifikat gültig ist.

b) Ein Zertifikat ist gültig, wenn der Zeitpunkt des Import-Vorgangs nach dem Startzeitpunkt des Flags ‚ValidFrom' des Zertifikats und vor dem Endzeitpunkt des Flags ‚ValidTo' des Zertifikats ist.

c) Ein Zertifikat ist gültig, wenn die Zertifizierungskette verifiziert werden kann. Dies ist nur dann der Fall, wenn dem Öffentlichen Schlüssel des ausstellenden Zertifikats als vertrauenswürdige Stammzertifizierungsstelle vertraut wurde.

d) Ein VPN-Verbindungsaufbau ist nur möglich, wenn das benötigte private Zertifikat erfolgreich importiert und validiert wurde.

e) Der lokale Client baut nur VPN-Verbindungen zu der in der Konfigurationsdatei gespeicherten IP-Adressbereichen (Authentifizierungstunnel) oder zu den zur Laufzeit vom Authentifizierungsserver übermittelten IP-Adressbereichen (Produktivtunnel) auf.

f) Ein Verbindungsaufbau zum VPN-Gateway ist nur möglich, wenn das lokale private Zertifikat und die aufzubauende Verbindung (IP-Adressbereich) mit den am VPN-Gateway eingerichteten Richtlinien korrespondieren.

g) Ein Zugriff auf die in der Konfigurationsdatei gespeicherten oder zur Laufzeit vom Authentifizierungsserver übermittelten IP-Adressbereiche ist nur möglich, wenn die VPN-Verbindung erfolgreich aufgebaut wurde.

].

FDP_ACF.1.3 Die TSF müssen den Zugriff von Subjekten auf Objekte basierend auf den folgenden zusätzlichen Regeln explizit autorisieren: [keine].

FDP_ACF.1.4 Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf [keine], explizit verweigern.

Familie FIA_UAU Benutzerauthentisierung

FIA_UAU.1 Zeitpunkt der Authentisierung

FIA_UAU.1.1 Die TSF müssen die Ausführung der [Konfiguration der Verbindungsart] für den Benutzer erlauben, bevor dieser authentisiert wird.

FIA_UAU.1.2 Die TSF müssen erfordern, dass jeder Benutzer erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

FIA_UAU.7 Geschützte Authentisierungsrückmeldung

FIA_UAU.7.1 Die TSF müssen sicherstellen, dass während der Authentisierung nur [Rückmeldungen ohne Rückgriff auf Benutzernamen und Passwort sowie Fehler bei Eingabe dieser Attribute] an den Benutzer bereitgestellt werden.

Familie FIA_UID Benutzeridentifikation

FIA_UID.1 Zeitpunkt der Identifikation

FIA_UID.1.1 Die TSF müssen die Ausführung der [Konfiguration der Verbindungsart] für den Benutzer erlauben, bevor dieser identifiziert wird.

FIA_UID.1.2 Die TSF müssen erfordern, dass jeder Benutzer erfolgreich identifiziert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

Familie FIA_SOS Spezifikation der Geheimnisse

FIA_SOS.2 Generierung von Geheimnissen durch TSF

FIA_SOS.2.1 Die TSF müssen einen Mechanismus bereitstellen, um Geheimnisse zu generieren, die [der Anforderung für die Laufzeitgenerierung von Challenges] entsprechen.

FIA_SOS.2.2 Die TSF müssen in der Lage sein, den Gebrauch der TSF-generierten Geheimnisse für [die Identifikation und Autorisierung von Benutzern] durchzusetzen.

Familie FMT_MSA Management der Sicherheitsattribute

FMT_MSA.1 Management der Sicherheitsattribute

FMT_MSA.1.1 Die TSF müssen die [Zugriffskontrollpolitik] zur Beschränkung der Fähigkeit zum **Ändern von Standardvorgaben** der Sicherheitsattribute [IP-Adressbereiche und Zertifikate] auf [Administratoren mit Herstellerautorisierung] durchsetzen.

FMT_MSA.3 Initialisierung statischer Attribute

FMT_MSA.3.1 Die TSF müssen die [Zugriffskontrollpolitik] zur Bereitstellung von vorgegebenen Standardwerten mit *einschränkenden Eigenschaften* für Sicherheitsattribute, die zur Durchsetzung der SFP benutzt werden, durchsetzen.

FMT_MSA.3.2 Die TSF müssen den [Administratoren mit Herstellerautorisierung] gestatten, bei der Erzeugung eines Objekts oder von Informationen alternative Anfangswerte zu spezifizieren, die die vorgegebenen Standardwerte ersetzen.

Familie FMT_SMF Spezifikation der Managementfunktionen[3]

FMT_SMF.1 Spezifikation der Managementfunktionen

FMT_SMF.1.1 Die TSF müssen in der Lage sein, folgende Sicherheitsmanagementfunktionen durchzusetzen:

[

a) Alternative Anfangswerte, die die vorgegebenen Standardwerte ersetzen, dürfen nur von Administratoren mit Herstellerautorisierung gesetzt werden.

b) Die Installation des TSF darf nur von Administratoren des Betriebssystems durchgeführt werden.

].

Familie FMT_SMR Rollen im Sicherheitsmanagement

FMT_SMR.1 Sicherheitsrollen

FMT_SMR.1.1 Die TSF müssen die Rollen [Benutzer, Betriebssystemadministratoren, Administratoren mit Herstellerautorisierung] erhalten.

FMT_SMR.1.2 Die TSF müssen Benutzer mit Rollen verknüpfen können.

[3] Diese Familie wurde durch Interpretation 065 hinzugefügt. Übersetzung ins Deutsche durch BSI gefordert.

Explizit dargelegte Sicherheitsanforderungen

FIA_UAU.EX.1 Externe Authentisierung der Benutzer bei Start des EVG

Ist hierarchisch zu: Keinen anderen Komponenten

FIA_UAU.EX.1.1 Die TSF müssen bei Verwendung von vom EVG aufzubauenden Interneteinwahlverbindungen die Ausführung der Konfiguration der Verbindungsart für den Benutzer erlauben, bevor dieser online gegenüber einem RADIUS-Server authentisiert wird.

FIA_UAU.EX.1.2 Die TSF müssen erfordern, dass bei Verwendung von vom EVG aufzubauenden Interneteinwahlverbindungen jeder Benutzer erfolgreich online gegenüber einem RADIUS-Server authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

Abhängigkeiten: FIA_UAU.EX.EXT.1Serverseitige Authentisierung

FIA_UID.EX. 1 Externe Identifikation der Benutzer bei Start des EVG

FIA_UID.EX.1 Externe Identifikation der Benutzer bei Start des EVG

Ist hierarchisch zu: Keinen anderen Komponenten

FIA_UID.EX.1.1 Die TSF müssen bei Verwendung von vom EVG aufzubauenden Interneteinwahlverbindungen die Ausführung der Konfiguration der Verbindungsart für den Benutzer erlauben, bevor dieser online gegenüber einem RADIUS-Server identifiziert wird.

FIA_UID.EX.1.2 Die TSF müssen erfordern, dass bei Verwendung von vom EVG aufzubauenden Interneteinwahlverbindungen jeder Benutzer erfolgreich online gegenüber einem RADIUS-Server identifiziert wurde, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

Abhängigkeiten: FIA_UID.EX.EXT.1 Serverseitige Identifikation

FPT_ITT.EX.1 Schutz von Konfigurationsdateien

Ist hierarchisch zu: Keinen anderen Komponenten

FPT_ITT.EX.1.1 Die TSF müssen gespeicherte Konfigurationsdaten gegen unbefugte Preisgabe und unerkannte Modifizierung schützen.

Abhängigkeiten: FCS_CKM.2 Verteilung des kryptographischen Schlüssels

FCS_CKM.3 Zugriff auf einen kryptographischen Schlüssel

FCS_CKM.4 Zerstörung eines kryptographischen Schlüssels

FDP_IFF.EX.1 IP-Sicherheitsrichtlinienverwaltung

Ist hierarchisch zu: Keinen anderen Komponenten

FDP_IFF.EX.1.1 Die TSF müssen in der Lage sein, während der Laufzeit IP-Sicherheitsrichtlinien anzulegen, die Verbindungen zu spezifizierten Netzen mittels IPSEC verschlüsseln.

FDP_IFF.EX.1.2 Die TSF müssen in der Lage sein, den für die Verschlüsselung zu verwendenden Algorithmus und die zu verwendende Hashing-Funktion zu setzen.

FDP_IFF.EX.1.3 Die TSF müssen in der Lage sein, Tunnelendpunkte dynamisch zur Laufzeit zu setzen.

FDP_IFF.EX.1.4 Die TSF müssen in der Lage sein, je nach vom Authentifizierungsserver zurückgegebenen Berechtigungen VPN-Zugriffe auf ganze definierte Netze oder nur einzelne definierte Server zu gewähren.

FDP_IFF.EX.1.5 Die TSF müssen in der Lage sein, in Abhängigkeit von den für die Verschlüsselung zu verwendenden privaten Zertifikaten unterschiedliche VPN-Verbindungen aufzubauen.

FDP_IFF.EX.1.6 Die TSF müssen in der Lage sein, Sicherheitsrichtlinien zu definieren, die bei aufgebautem VPN-Tunnel Zugriffe auf andere Netze als das vertraute Netz blockieren.

FDP_IFF.EX.1.7 Die TSF müssen es durch Wahl entsprechender Zertifikate für den Tunnelaufbau ermöglichen, serverseitig die Nichtabstreitbarkeit der Urheberschaft von übermittelten Daten auswerten zu können.

FDP_IFF.EX.1.8 Benutzerdaten dürfen nur dann übermittelt werden, wenn ein VPN-Tunnel besteht. Alle nachstehend aufgeführten Bedingungen müssen erfüllt sein:

a) Der Verbindungsaufbau zum definierten Netz hinter dem VPN-Gateway ist möglich.

b) Die Verbindung zum definierten Netz hinter dem VPN-Gateway besteht fort.

FDP_IFF.EX.1.9 Die TSF müssen bei fehlgeschlagenem Verbindungsversuch zum VPN-Gateway die IP-Sicherheitsrichtlinien entfernen, was zum sofortigen Tunnelabbau führt.

FDP_IFF.EX.1.10 Die IP-Sicherheitsrichtlinienverwaltung muss unabhängig vom angemeldeten Windows-Benutzer und dessen Rechten in der Lage sein, IP-Sicherheitsrichtlinien zu erstellen, zu ändern, zu aktivieren, zu deaktivieren und zu löschen.

Abhängigkeiten: FCS_CKM.2 Verteilung des kryptographischen Schlüssels

FCS_CKM.3 Zugriff auf einen kryptographischen Schlüssel

FCS_CKM.4 Zerstörung eines kryptographischen Schlüssels

5.1.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Alle Vertrauenswürdigkeitskomponenten für den EVG wurden dem Teil 3 der CC entnommen und sind nachstehend aufgeführt. Der EVG erfüllt die Anforderungen des Vertrauenswürdigkeitspaketes EAL2.

Komponente	**Komponenten Name**
ACM_CAP.2	Konfigurationsteile
ADO_IGS.1	Installations-, Generierungs-, und Anlaufprozeduren
ADV_FSP.1	Informelle funktionale Spezifikation
ADV_HLD.1	Beschreibender Entwurf auf hoher Ebene
ADV_RCR.1	Informeller Nachweis der Übereinstimmung
ADO_DEL.1	Auslieferungsprozeduren
AGD_ADM.1	Systemverwalterhandbuch
AGD_USR.1	Benutzerhandbuch
ATE_COV.1	Nachweis der Testabdeckung
ATE_FUN.1	Funktionales Testen
ATE_IND.2	Unabhängiges Testen – stichprobenartig
AVA_SOF.1	Stärke der EVG-Sicherheitsfunktionen
AVA_VLA.1	Schwachstellenanalyse des Entwicklers

Tabelle 5.1 – Anforderungen an die Vertrauenswürdigkeit des EVG

ACM_CAP.2 Konfigurationsteile

Elemente zu Entwickleraufgaben:

ACM_CAP.2.1D Der Entwickler muss einen Verweisnamen für den TOE (EVG) bereitstellen.

ACM_CAP.2.2D Der Entwickler muss ein CM-System benutzen.

ACM_CAP.2.3D Der Entwickler muss eine CM-Dokumentation bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ACM_CAP.2.1C Der Verweisname für den TOE (EVG) muss für jede Version des TOE (EVG) eindeutig sein.

ACM_CAP.2.2C Der TOE (EVG) muss mit seinem Verweisnamen gekennzeichnet sein.

ACM_CAP.2.3C Die CM-Dokumentation muss ein Konfigurationsverzeichnis enthalten.

The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.4C Das Konfigurationsverzeichnis muss die Konfigurationsteile beschreiben, aus denen der TOE (EVG) besteht.

ACM_CAP.2.5C Die CM-Dokumentation muss die zur eindeutigen Identifikation der Konfigurationsteile verwendete Methode beschreiben.

ACM_CAP.2.6C Das CM-System muss alle Konfigurationsteile eindeutig identifizieren.

Elemente zu Evaluatoraufgaben:

ACM_CAP.2.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ADO_DEL.1 Auslieferungsprozeduren

Elemente zu Entwickleraufgaben:

ADO_DEL.1.1D Der Entwickler muss die Auslieferungsprozeduren des TOE (EVG) oder von Teilen des TOE (EVG) an den Benutzer dokumentieren.

ADO_DEL.1.2D Der Entwickler muss die Auslieferungsprozeduren anwenden.

Elemente zu Inhalt und Form des Nachweises:

ADO_DEL.1.1C Die Auslieferungsdokumentation muss alle Prozeduren beschreiben, die beim Versand von Versionen des TOE (EVG) zum Einsatzort beim Benutzer zur Erhaltung der Sicherheit erforderlich sind.

Elemente zu Evaluatoraufgaben:

ADO_DEL.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ADO_IGS.1 Installations-, Generierungs-, und Anlaufprozeduren

Elemente zu Entwickleraufgaben:

ADO_IGS.1.1D Der Entwickler muss die für die sichere Installation und Generierung sowie den sicheren Anlauf des TOE (EVG) erforderlichen Prozeduren dokumentieren.

Elemente zu Inhalt und Form des Nachweises:

ADO_IGS.1.1C Die Dokumentation muss die für die sichere Installation und Generierung sowie den sicheren Anlauf des TOE (EVG) erforderlichen Schritte beschreiben.[4]

Elemente zu Evaluatoraufgaben:

ADO_IGS.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ADO_IGS.1.2E Der Evaluator muss feststellen, dass die Installations-, Generierungs- und Anlaufprozeduren zu einer sicheren Konfiguration führen.

ADV_FSP.1 Informelle funktionale Spezifikation

Elemente zu Entwickleraufgaben:

ADV_FSP.1.1D Der Entwickler muss eine funktionale Spezifikation bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ADV_FSP.1.1C Die funktionale Spezifikation muss die TSF und ihre externen Schnittstellen in einem informellen Stil beschreiben.

ADV_FSP.1.2C Die funktionale Spezifikation muss in sich konsistent sein.

ADV_FSP.1.3C Die funktionale Spezifikation muss den Zweck und die Methode des Gebrauchs aller externen TSF-Schnittstellen beschreiben, einschließlich Details der Wirkungen, Ausnahmen und Fehlermeldungen, wie jeweils angemessen.

ADV_FSP.1.4C Die funktionale Spezifikation muss die TSF vollständig darstellen.

Elemente zu Evaluatoraufgaben:

ADV_FSP.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ADV_FSP.1.2E Der Evaluator muss feststellen, dass die funktionale Spezifikation eine getreue und vollständige Umsetzung der funktionalen EVG-Sicherheitsanforderungen ist.

---

[4] Interpretation 051: In der englischen Fassung der CC wurde das Element zu Inhalt und Form des Nachweises geändert in:

"The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE."

ADV_HLD.1 Beschreibung auf hoher Ebene

Elemente zu Entwickleraufgaben:

ADV_HLD.1.1D Der Entwickler muss den Entwurf der TSF auf hoher Ebene bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ADV_HLD.1.1C Die Darstellung des Entwurfs auf hoher Ebene muss informell sein.

ADV_HLD.1.2C Der Entwurf auf hoher Ebene muss in sich konsistent sein.

ADV_HLD.1.3C Der Entwurf auf hoher Ebene muss die Strukturen der TSF anhand von Teilsystemen beschreiben.

ADV_HLD.1.4C Der Entwurf auf hoher Ebene muss die von jedem der Teilsysteme der TSF bereitgestellte Sicherheitsfunktionalität beschreiben.

ADV_HLD.1.5C Der Entwurf auf hoher Ebene muss sämtliche den TSF zugrunde liegende Hardware, Firmware und/oder Software angeben und die Funktionen darstellen, die von dem unterstützenden Schutzmechanismus bereitgestellt werden, der in dieser Hardware, Firmware oder Software implementiert ist.

ADV_HLD.1.6C Der Entwurf auf hoher Ebene muss alle Schnittstellen zu den Teilsystemen der TSF identifizieren.

ADV_HLD.1.7C Der Entwurf auf hoher Ebene muss angeben, welche der Schnittstellen zu den Teilsystemen der TSF von außerhalb sichtbar sind.

Elemente zu Evaluatoraufgaben:

ADV_HLD.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ADV_HLD.1.2E Der Evaluator muss feststellen, dass der Entwurf auf hoher Ebene eine getreue und vollständige Umsetzung der funktionalen EVG-Sicherheitsanforderungen ist.

ADV_RCR.1 Informeller Nachweis der Übereinstimmung

Elemente zu Entwickleraufgaben:

ADV_RCR.1.1D Der Entwickler muss eine Analyse der Übereinstimmung aller benachbarten Paare der bereitgestellten TSF-Darstellungen bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ADV_RCR.1.1C Die Analyse muss für jedes Paar benachbarter TSF-Darstellungen nachweisen, dass die gesamte relevante Sicherheitsfunktionalität der abstrakteren TSF-Darstellung in der weniger abstrakten TSF-Darstellung korrekt und vollständig verfeinert wurde.

Elemente zu Evaluatoraufgaben:

ADV_RCR.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

AGD_ADM.1 Systemverwalterhandbuch

Elemente zu Entwickleraufgaben:

AGD_ADM.1.1D Der Entwickler muss ein Systemverwalterhandbuch bereitstellen, das an das für Systemverwaltung zuständige Personal gerichtet ist.

Elemente zu Inhalt und Form des Nachweises:

AGD_ADM.1.1C Das Systemverwalterhandbuch muss die Systemverwaltungsfunktionen und Schnittstellen beschreiben, die dem Systemverwalter des TOE (EVG) zur Verfügung stehen.

AGD_ADM.1.2C Das Systemverwalterhandbuch muss beschreiben, wie der TOE (EVG) auf sichere Art und Weise zu verwalten ist.

AGD_ADM.1.3C Das Systemverwalterhandbuch muss Warnungen bezüglich Funktionen und Privilegien enthalten, die in einer sicheren Verarbeitungsumgebung kontrolliert werden sollen.

AGD_ADM.1.4C Das Systemverwalterhandbuch muss alle Annahmen zum Benutzerverhalten beschreiben, die für den sicheren Betrieb des TOE (EVG) relevant sind.

AGD_ADM.1.5C Das Systemverwalterhandbuch muss alle vom Systemverwalter kontrollierten Sicherheitsparameter beschreiben und dabei, wie jeweils angemessen, sichere Werte angeben.

AGD_ADM.1.6C Das Systemverwalterhandbuch muss jede Art von sicherheitsrelevanten Ereignissen bezüglich der auszuführenden Systemverwaltungsfunktionen beschreiben, einschließlich der Änderungen der Sicherheitseigenschaften von Einheiten, die unter Kontrolle der TSF stehen.

AGD_ADM.1.7C Das Systemverwalterhandbuch muss konsistent mit allen anderen für die Prüfung und Bewertung gelieferten Dokumentationen sein.

AGD_ADM.1.8C Das Systemverwalterhandbuch muss alle Sicherheitsanforderungen an die IT-Umgebung beschreiben, die für den Systemverwalter relevant sind.

Elemente zu Evaluatoraufgaben:

AGD_ADM.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

AGD_USR.1 Benutzerhandbuch

Elemente zu Entwickleraufgaben:

AGD_USR.1.1D Der Entwickler muss ein Benutzerhandbuch bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

AGD_USR.1.1C Das Benutzerhandbuch muss die Funktionen und Schnittstellen beschreiben, die den Benutzern des TOE (EVG) zur Verfügung stehen, die nicht für Systemverwaltung zuständig sind.

AGD_USR.1.2C Das Benutzerhandbuch muss den Gebrauch der vom TOE (EVG) bereitgestellten Sicherheitsfunktionen, die für den Benutzer zugänglich sind, beschreiben.

AGD_USR.1.3C Das Benutzerhandbuch muss Warnungen bezüglich den Benutzern zugänglichen Funktionen und Privilegien enthalten, die in einer sicheren Verarbeitungsumgebung kontrolliert werden sollen.

AGD_USR.1.4C Das Benutzerhandbuch muss alle Verantwortlichkeiten des Benutzers klar darstellen, die für den sicheren Betrieb des TOE (EVG) notwendig sind, einschließlich derjenigen, die mit den in der Darlegung der EVG-Sicherheitsumgebung enthaltenen Annahmen zum Benutzerverhalten zusammenhängen.

AGD_USR.1.5C Das Benutzerhandbuch muss konsistent mit allen anderen für die Prüfung und Bewertung gelieferten Dokumentationen sein.

AGD_USR.1.6C Das Benutzerhandbuch muss alle Sicherheitsanforderungen an die IT-Umgebung beschreiben, die für den Benutzer relevant sind.

Elemente zu Evaluatoraufgaben:

AGD_USR.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ATE_COV.1 Nachweis der Testabdeckung

Elemente zu Entwickleraufgaben:

ATE_COV.1.1D Der Entwickler muss den Nachweis der Testabdeckung erbringen.

Elemente zu Inhalt und Form des Nachweises:

ATE_COV.1.1C Der Nachweis der Testabdeckung muss die Übereinstimmung zwischen den in der Testdokumentation identifizierten Tests und den TSF, die in der funktionalen Spezifikation beschrieben sind, zeigen.

Elemente zu Evaluatoraufgaben:

ATE_COV.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ATE_FUN.1 Funktionales Testen

Elemente zu Entwickleraufgaben:

ATE_FUN.1.1D Der Entwickler muss die TSF testen und die Ergebnisse dokumentieren.

ATE_FUN.1.2D Der Entwickler muss die Testdokumentation bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ATE_FUN.1.1C Die Testdokumentation muss die Testpläne, die Beschreibungen der Testprozeduren, die erwarteten Testergebnisse und die tatsächlichen Testergebnisse enthalten.

ATE_FUN.1.2C Die Testpläne müssen die zu testenden Sicherheitsfunktionen identifizieren und das Ziel der durchzuführenden Tests beschreiben.

ATE_FUN.1.3C Die Beschreibungen der Testprozeduren müssen die durchzuführenden Tests identifizieren und die Testszenarien für jede Sicherheitsfunktion beschreiben. Diese Szenarien müssen alle Ordnungsabhängigkeiten von den Ergebnissen anderer Tests enthalten.

ATE_FUN.1.4C Die erwarteten Testergebnisse müssen die bei einem erfolgreichen Testverlauf zu erwartenden Ergebnisse aufzeigen.

ATE_FUN.1.5C Die Testergebnisse der durch den Entwickler durchgeführten Tests müssen nachweisen, dass sich jede getestete Sicherheitsfunktion (SF) wie spezifiziert verhielt.

Elemente zu Evaluatoraufgaben:

ATE_FUN.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ATE_IND.2 Unabhängiges Testen - stichprobenartig

Elemente zu Entwickleraufgaben:

ATE_IND.2.1D Der Entwickler muss den TOE (EVG) zum Testen bereitstellen.

Elemente zu Inhalt und Form des Nachweises:

ATE_IND.2.1C Der TOE (EVG) muss sich zum Testen eignen.

ATE_IND.2.2C Der Entwickler muss eine Menge von Betriebsmitteln bereitstellen, die denen entsprechen, die beim funktionalen Testen der TSF durch den Entwickler verwendet wurden.

Elemente zu Evaluatoraufgaben:

ATE_IND.2.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

ATE_IND.2.2E Der Evaluator muss eine Teilmenge der TSF angemessen testen, so dass bestätigt werden kann, dass der TOE (EVG) entsprechend seiner Spezifikation wirkt.

ATE_IND.2.3E Der Evaluator muss zur Verifizierung der Entwicklertestergebnisse eine Stichprobe der in der Testdokumentation enthaltenen Tests durchführen.

AVA_SOF.1 Stärke der EVG-Sicherheitsfunktionen

Elemente zu Entwickleraufgaben:

AVA_SOF.1.1D Der Entwickler muss eine Analyse der Stärke der EVG-Sicherheitsfunktionen für jeden Mechanismus durchführen, der nach den Angaben in den ST ein Postulat der Stärke der EVG-Sicherheitsfunktionen aufweist.

Elemente zu Inhalt und Form des Nachweises:

AVA_SOF.1.1C Für jeden Mechanismus mit einem Postulat zur Stärke der EVG-Sicherheitsfunktionen muss die Analyse der EVG-Sicherheitsfunktionsstärke nachweisen, dass er die im PP / in den ST definierte Mindeststärkestufe erreicht oder übertrifft.

AVA_SOF.1.2C Für jeden Mechanismus mit einem konkreten Postulat der Stärke der EVG-Sicherheitsfunktion soll die Analyse der Stärke der EVG-Sicherheitsfunktionen nachweisen, dass er die im PP / in den ST definierte spezielle Metrik der Stärke der Funktion erreicht oder übertrifft.

Elemente zu Evaluatoraufgaben:

AVA_SOF.1.1E Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.

AVA_SOF.1.2E Der Evaluator muss bestätigen, dass die Stärkepostulate korrekt sind.

AVA_VLA.1 Schwachstellenanalyse des Entwicklers

Elemente zu Entwickleraufgaben:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Elemente zu Inhalt und Form des Nachweises:

AVA_VLA.1.1C Die Dokumentation muss für alle identifizierten Schwachstellen zeigen, dass die Schwachstelle in der vorgesehenen Einsatzumgebung des TOE (EVG) nicht ausgenutzt werden kann.[5]

---

[5] Interpretation 051: In der englischen Fassung der CC wurde das Element zu Inhalt und Form des Nachweises geändert in:

"The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE."

Elemente zu Evaluatoraufgaben:

AVA_VLA.1.1E	Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Form des Nachweises erfüllen.
AVA_VLA.1.2E	Der Evaluator muss Penetrationstests durchführen, die auf der Schwachstellenanalyse des Entwicklers aufbauen, um sicherzustellen, dass offensichtliche Schwachstellen berücksichtigt wurden.

5.2 Sicherheitsanforderungen an die IT-Umgebung

Alle aufgeführten Anforderungen sind bis auf die explizit dargelegten Anforderungen FIA_UAU.EX.EXT.1 und FIA_UID.EX.EXT.1 dem Teil 2 der CC entnommen.

Der EVG hat folgende Anforderungen an die IT-Umgebung:

Familie FCO_NRO Nichtabstreitbarkeit der Urheberschaft

FCO_NRO.1 Selektiver Urheberschaftsbeweis

FCO_NRO.1.1 **Das Betriebssystem muss** auf Anforderung des *Urhebers, Empfänger*s für übertragene [Nutzdaten] Urheberschaftsnachweise generieren können.

FCO_NRO.1.2 **Das Betriebssystem muss** die [Identität] des Informationsurhebers den [Nutzdaten] der Informationen, auf die sich der Nachweis bezieht, zuordnen können.

FCO_NRO.1.3 **Das Betriebssystem muss** dem *Urheber, Empfänger* die Fähigkeit zum Verifizieren des Urheberschaftsnachweises von Informationen unter der Vorgabe von [Zertifikaten] bereitstellen.

Familie FCO_NRR Nichtabstreitbarkeit des Empfangs

FCO_NRR.1 Selektiver Empfangsbeweis

FCO_NRR.1.1 **Das Betriebssystem muss** auf Anforderung des *Urhebers, Empfängers* für empfangene [Nutzdaten] Empfangsnachweise generieren können.

FCO_NRR.1.2 **Das Betriebssystem muss** die [Identität] des Informationsempfängers den [Nutzdaten] der Informationen, auf die sich der Nachweis bezieht, zuordnen können.

FCO_NRR.1.3 **Das Betriebssystem muss** dem *Urheber, Empfänger* die Fähigkeit zum Verifizieren des Empfangsnachweises von Informationen unter der Vorgabe von [Zertifikaten] bereitstellen.

Familie FDP_UIT Schutz der Benutzerdatenintegrität bei Inter-TSF-Transfer

FDP_UIT.1 Einfache Integrität des Datenaustausches

FDP_UIT.1.1 **Das Betriebssystem muss** die [Sicherheitsrichtlinien zum Aufbau einer VPN-Verbindung] durchsetzen, um in der Lage zu sein, Benutzerdaten vor *Modifizieren, Löschen, Einfügen, Wiedereinspielen* geschützt zu *übertragen, empfangen*.

FDP_UIT.1.2 **Das Betriebssystem muss** in der Lage sein, beim Empfang der Benutzerdaten festzustellen, ob ein *Modifizieren, Löschen, Einfügen, Wiedereinspielen* stattgefunden hat.

Familie FDP_UCT Schutz der Benutzerdatenvertraulichkeit bei Inter-TSF-Transfer

FDP_UCT.1 Einfache Vertraulichkeit des Datenaustausches

FDP_UCT.1.1 **Das Betriebssystem muss** die [Sicherheitsrichtlinien zum Aufbau einer VPN-Verbindung] durchsetzen, um in der Lage zu sein, Objekte vor nichtautorisierter Preisgabe geschützt zu *übertragen, empfangen*.

Explizit dargelegte Sicherheitsanforderungen an die IT-Umgebung

FIA_UAU.EX.EXT.1 Serverseitige Authentisierung

Ist hierarchisch zu: Keinen anderen Komponenten

FIA_UAU.EX.EXT.1.1 Bei Interneteinwahlverbindungen werden Benutzer zunächst online gegenüber einem RADIUS-Server mittels CHAP authentisiert.

Abhängigkeiten: FIA_UID.EX.EXT.1 Serverseitige Identifikation

FIA_UAU.EX.1 Externe Authentisierung der Benutzer bei Start des EVG

FIA_UID.EX.EXT.1 Serverseitige Identifikation

Ist hierarchisch zu: Keinen anderen Komponenten

FIA_UID.EX.EXT.1.1 Bei Interneteinwahlverbindungen werden Benutzer zunächst online gegenüber einem RADIUS-Server mittels CHAP identifiziert.

Abhängigkeiten: FIA_UID.EX.1 Externe Identifikation der Benutzer bei Start des EVG

6 EVG Übersichtsspezifikation

Dieses Kapitel beschreibt die vom EVG bereitgestellten Sicherheitsfunktionen und die durch die Entwicklungsumgebung des EVG bereitgestellten Maßnahmen zur Vertrauenswürdigkeit.

6.1 EVG-Sicherheitsfunktionen

VPNConnect bietet dem Anwender die Sicherheitsfunktionen Identifikation (Familie FIA_UID und Komponente FIA_UID.EX.1), Spezifikation von Geheimnissen (Familie FIA_SOS), Authentisierung (Familie FIA_UAU und Komponente FIA_UAU.EX.1), Zugriffskontrolle (Familie FDP_ACF), Kryptografisches Schlüsselmanagement (Familie FCS_CKM), Schutz von Konfigurationsdateien (Komponente FPT_ITT.EX.1) sowie Funktionen zur IP-Sicherheitsrichtlinienverwaltung (Komponente FDP_IFF.EX.1).

6.1.1 Identifikation und Authentisierung

IA.1 Bevor ein Benutzer VPNConnect nutzen kann, muss er sich gegenüber VPNConnect mit seinem eindeutigen Benutzerkennzeichen identifizieren und sich über sein Passwort authentisieren. Nur wenn eine korrekte Kombination von Benutzerkennzeichen und Passwort eingegeben wurde, erhält der Benutzer Zugriff auf die ihm zugewiesenen Funktionen.[6]

IA.2 Die Identifikation und Authentisierung erfolgt bei Interneteinwahlverbindungen online gegenüber einem RADIUS-Server.[7]

IA.3 Die Identifikation und Authentisierung erfolgt bei allen Verbindungsarten nach Aufbau des Authentifizierungstunnels.[8]

IA.4 Wurde eine falsche Kombination von Benutzerkennzeichen und Passwort eingegeben, erhält der Benutzer einen Hinweis, dass Benutzerkennzeichen oder Passwort falsch waren. Aus dieser Fehlermeldung geht nicht hervor, ob Benutzerkennzeichen oder Passwort falsch waren.[9]

---

[6] Bei Start der Applikation muss der Benutzer Username und Passwort eingeben. Die eingegebenen Daten werden online mit einem RADIUS-Server (bei Interneteinwahlen) abgeglichen. Zum Abgleich der Daten mit einem Authentifizierungsserver, wird mittels einer Funktion zur Generierung von Challenges eine Challenge generiert, mit der der Benutzername verschlüsselt and den Authentifizierungsserver übertragen wird. Nur wenn ein Benutzerkonto auf dem Authentifizierungsserver vorhanden ist, wird mittels eines Challenge-Responsemechanismus eine Steuerdatei verschlüsselt zum EVG zurück übertragen. Der EVG entschlüsselt diese Konfigurationsdatei und identifiziert und authentisiert den Benutzer.

Nur wenn der Benutzer erfolgreich vom EVG identifiziert und authentisiert wurde, kann ein Produktivtunnel aufgebaut werden.

[7] Die RADIUS-Authentifizierung erfolgt durch die Windows-RAS, die vom EVG mit den vordefinierten Einstellungen (z.B. CHAP) konfiguriert wurde. Der EVG nimmt Callbacks der Windows-RAS entgegen, d.h. die gesamte RAS-Verbindung wird vom EVG konfiguriert und über Callbacks überwacht.

[8] Der EVG übergibt den mit einer Challenge verschlüsselten Username und diese Challenge im durch das Betriebssystem aufgebauten Authentifizierungstunnel geschützt an den Authentifizierungsserver und nimmt die serverseitig mittels eines Challenge-Responsemechanismus verschlüsselte Konfigurationsdatei für den Produktivtunnel vom Authentifizierungsserver entgegen. Die Identifikation und Authentisierung erfolgt clientseitig durch Entschlüsselung und Auswertung der Steuerdatei. Für den Download der Konfiguration werden Funktionen der Winsock und auf IP-Ebene der IP-Helper-API benutzt.

IA.5 Die Installation von VPNConnect darf nur von Administratoren des Betriebssystems durchgeführt werden.[10]

Die Eigenschaften der Sicherheitsfunktion „Identifikation und Authentisierung“, die zur Erfüllung der funktionalen Anforderungen beitragen sind:

Nr.	Eigenschaften	Trägt bei zu
1	Bevor ein Benutzer VPNConnect nutzen kann, muss er sich gegenüber VPNConnect mit seinem eindeutigen Benutzerkennzeichen identifizieren und sich über sein Passwort authentisieren. Nur wenn eine korrekte Kombination von Benutzerkennzeichen und Passwort eingegeben wurde, erhält der Benutzer Zugriff auf die ihm zugewiesenen Funktionen.	FIA_UAU.1 FIA_UID.1 FIA_UAU.EX.1 FIA_UID.EX.1 FMT_MSA.3 FMT_SMR.1
2	Die Identifikation und Authentisierung erfolgt bei Internetwahlverbindungen online gegenüber einem RADIUS-Server.	FIA_UAU.EX.1 FIA_UID.EX.1
3	Die Identifikation und Authentisierung erfolgt bei allen Verbindungsarten nach Aufbau des Authentifizierungstunnels.	FIA_UAU.1 FIA_UID.1 FIA_SOS.2 FDP_IFF.EX.1 FMT_SMR.1
4	Wurde eine falsche Kombination von Benutzerkennzeichen und Passwort eingegeben, erhält der Benutzer einen Hinweis, dass Benutzerkennzeichen oder Passwort falsch waren. Aus dieser Fehlermeldung geht nicht hervor, ob Benutzerkennzeichen oder Passwort falsch waren.	FIA_UAU.7
5	Die Installation von VPNConnect darf nur von Administratoren des Betriebssystems durchgeführt werden.	FMT_SMF.1 FMT_SMR.1

Tabelle 6.1 – Identifikation und Authentisierung

---

[9] Der EVG erhält bei Interneteinwahlen von der Windows-RAS Information darüber, dass Username oder Passwort falsch waren. Der Authentifizierungsserver übergibt direkt über den vom Betriebssystem aufgebauten Authentifizierungstunnel geschützt zurück, dass ein Benutzer nicht vorhanden ist. Fehlerhafte Passwörter resultieren in einem nicht erwarteten Ergebnis bei der Entschlüsselung der vom Authentifizierungsserver empfangenen Konfigurationsdatei.

In allen Fällen übernimmt der EVG die Ablaufkontrolle, die Auswertung der Rückgaben und die Darstellung der Fehlermeldungen an den Benutzer, ohne dass aus dieser hervorgeht, welche Daten inkorrekt waren.

Für den Download der Konfigurationsdatei werden Funktionen der Winsock und auf IP-Ebene der IP-Helper-API benutzt.

[10] Der EVG überprüft über mehrere, vom Betriebssystem und der MFC und das Filesystem bereitgestellte Funktionen, ob der angemeldete Benutzer ein Administrator des Betriebssystems ist.

6.1.2 Zugriffskontrolle

AC.1 VPNConnect kontrolliert den Zugriff von Benutzern auf die hinter einem VPN-Gateway befindlichen Netze durch Anlegen, Modifizieren und Aktivieren von entsprechenden IP-Sicherheitsrichtlinien.[11]

AC.2 VPNConnect beschränkt den Zugriff auf von dem Authentifizierungsserver zugewiesene Server hinter dem VPN-Gateway durch Anlegen, Modifizieren und Aktivieren von entsprechenden IP-Sicherheitsrichtlinien.[12]

AC.3 Brandings vom Produkt VPNConnect können aufgrund der verschlüsselten Konfigurationsdateien nur vom Hersteller oder von herstellerautorisierten Administratoren durchgeführt werden.[13]

AC.4 Ist ein Zielserver nicht mehr erreichbar, ist ein bestehender Tunnel von VPNConnect sofort abzubauen.[14]

---

[11] Der EVG übernimmt das Anlegen, Modifizieren, Löschen, Aktivieren und Deaktivieren von IP-Sicherheitsrichtlinien. Diese IP-Sicherheitsrichtlinien sind essentiell durch die Definition der Netze bestimmt, die durch den EVG bestimmt werden. Der physikalische IP-Sicherheitsrichtlinienspeicher und deren Verwaltung und In-Kraft-Setzen wird durch Funktionen des Betriebssystems bereitgestellt, die vom EVG aufgerufen werden.

[12] Der EVG übernimmt das Anlegen, Modifizieren, Löschen, Aktivieren und Deaktivieren von IP-Sicherheitsrichtlinien. Diese IP-Sicherheitsrichtlinien sind essentiell durch die Definition der Netze bestimmt, die durch den EVG bestimmt und durch die vom Authentifizierungsserver übertragene Konfigurationsdatei definiert werden. Der physikalische IP-Sicherheitsrichtlinienspeicher und deren Verwaltung und In-Kraft-Setzen wird durch Funktionen des Betriebssystems bereitgestellt, die vom EVG aufgerufen werden.

[13] Die Konfigurationsdateien werden vom EVG entschlüsselt. Zur Verschlüsselung werden Funktionen des EVGs benutzt, die über ein separates, vom Hersteller des EVG entwickeltes Tool angesprochen werden, das nur dem Hersteller oder herstellerautorisierten Administratoren zur Verfügung steht.

[14] Der EVG überprüft timergesteuert, ob ein im vom Authentifizierungsserver übermittelten Konfigurationsfile definierter Server erreichbar ist. Hierzu wird SNMP oder ICMP benutzt, deren Protokolle unter Zuhilfenahme von Funktionen der Winsock und auf IP-Ebene der IP-Helper-API implementiert sind. Ist der definierte Zielserver über diese Funktionalität nicht erreichbar, wird der bestehende Tunnel vom EVG initiiert abgebaut.

Die Eigenschaften der Sicherheitsfunktion „Zugriffskontrolle“, die zur Erfüllung der funktionalen Anforderungen beitragen sind:

Nr.	Eigenschaften	Trägt bei zu
1	VPNConnect kontrolliert den Zugriff von Benutzern auf die hinter einem VPN-Gateway befindlichen Netze durch Anlegen, Modifizieren und Aktivieren von entsprechenden IP-Sicherheitsrichtlinien.	FDP_ACC.2 FDP_ACF.1 FDP_IFF.EX.1
2	VPNConnect beschränkt den Zugriff auf von dem Authentifizierungsserver zugewiesene Server hinter dem VPN-Gateway durch Anlegen, Modifizieren und Aktivieren von entsprechenden IP-Sicherheitsrichtlinien.	FDP_ACC.2 FDP_ACF.1 FDP_IFF.EX.1
3	Brandings vom Produkt VPNConnect können aufgrund der verschlüsselten Konfigurationsdateien nur vom Hersteller oder von herstellerautorisierten Administratoren durchgeführt werden.	FMT_MSA.1 FMT_MSA.3 FDP_ACF.1 FMT_SMR.1 FMT_SMF.1
4	Ist ein Zielserver nicht mehr erreichbar, ist ein bestehender Tunnel von VPNConnect sofort abzubauen	FCS_CKM.4 FDP_IFF.EX.1

Tabelle 6.2 - Zugriffskontrolle

6.1.3 Kryptografisches Schlüsselmanagement

KM.1 Das generische Zertifikat zum Aufbau des Authentifizierungstunnels wird vor jedem Verbindungsaufbau in den Benutzerzertifikatsspeicher importiert und dient der sicheren Authentifizierung des Benutzers am Authentifizierungsserver.[15]

KM.2 Bei vorhandenem Benutzerkonto am Authentifizierungsserver lädt VPNConnect im vorher aufgebauten Authentifizierungstunnel eine mittels eines Challenge-Responsemechanismus verschlüsselte Konfigurationsdatei herunter, die der Autorisierung und Identifikation des Benutzers dient und u.a. den Ort der Benutzerzertifikate enthält, die im nächsten Schritt gesichert auf den Rechner heruntergeladen werden und physikalisch auf dem Datenträger gespeichert. Die Zertifikate werden automatisch in den Windows-Zertifikatsspeicher importiert.[16]

KM.3 Die privaten Zertifikate, die während der Laufzeit von VPNConnect heruntergeladen worden sind, sind passwortgeschützt. Die Passwörter werden durch die Konfigurationsdatei VPNConnect übergeben und sind dem Benutzer nicht bekannt.

KM.4 Bei Tunnelabbau werden die privaten Zertifikate von VPNConnect aus dem Windows-Zertifikatsspeicher entfernt und bei Beendigung der Applikation physikalisch vom Datenträger gelöscht.[17]

---

[15] Zum Importieren von Zertifikaten werden Funktionen aus Funktionsbibliotheken des Betriebssystems verwendet. Die Zeitpunkte und der Ablauf sowie die Kontrollmechanismen werden vom EVG bereitgestellt.

[16] Zum Herunterladen des Konfigurationsfiles werden Funktionen der Winsock auf IP-Ebene als Helper-API benutzt, dito für das Herunterladen der Zertifikate. Zum Importieren von Zertifikaten werden Funktionen aus Funktionsbibliotheken des Betriebssystems verwendet. Die Zeitpunkte dieser Vorgänge, deren Ablauf sowie Kontrollmechanismen werden vom EVG bereitgestellt.

Die Funktionalität zur Identifikation und Autorisierung stellt der EVG bereit.

[17] Zum Löschen von Zertifikaten werden Funktionen aus Funktionsbibliotheken des Betriebssystems verwendet. Die Zeitpunkte dieser Vorgänge, deren Ablauf sowie Kontrollmechanismen werden vom EVG bereitgestellt.

Die Eigenschaften der Sicherheitsfunktion „Kryptografisches Schlüsselmanagement“, die zur Erfüllung der funktionalen Anforderungen beitragen sind:

Nr.	Eigenschaften	Trägt bei zu
1	Das generische Zertifikat zum Aufbau des Authentifizierungstunnels wird vor jedem Verbindungsaufbau in den Benutzerzertifikatsspeicher importiert und dient der sicheren Authentifizierung des Benutzers am Authentifizierungsserver.	FCS_CKM.2 FDP_IFF.EX.1 FDP_ACF.1 FMT_MSA.3 FIA_UAU.1 FIA_UID.1
2	Bei vorhandenem Benutzerkonto am Authentifizierungsserver lädt VPNConnect im vorher aufgebauten Authentifizierungstunnel eine mittels eines Challenge-Responsemechanismus verschlüsselte Konfigurationsdatei herunter, die der Autorisierung und Identifikation des Benutzers dient und u.a. den Ort der Benutzerzertifikate enthält, die im nächsten Schritt gesichert auf den Rechner heruntergeladen werden und physikalisch auf dem Datenträger gespeichert. Die Zertifikate werden automatisch in den Windows-Zertifikatsspeicher importiert.	FCS_CKM.2 FCS_CKM.3 FDP_IFF.EX.1 FIA_UAU.1 FIA_UID.1 FIA_SOS.2
3	Die privaten Zertifikate, die während der Laufzeit von VPNConnect heruntergeladen worden sind, sind passwortgeschützt. Die Passwörter werden durch die Konfigurationsdatei VPNConnect übergeben und sind dem Benutzer nicht bekannt.	FCS_CKM.3 FDP_IFF.EX.1
4	Bei Tunnelabbau werden die privaten Zertifikate von VPNConnect aus dem Windows-Zertifikatsspeicher entfernt und bei Beendigung der Applikation physikalisch vom Datenträger gelöscht.	FCS_CKM.4 FDP_IFF.EX.1

Tabelle 6.3 – Kryptografisches Schlüsselmanagement

6.1.4 Schutz von Konfigurationsdateien

SK.1 Die von VPNConnect verwendeten Konfigurationsdateien werden verschlüsselt gespeichert.

SK.2 Die vom Authentifizierungsserver zu generierenden Konfigurationsdateien werden mittels eines Challenge-Responsemechanismus verschlüsselt übertragen und von VPNConnect entschlüsselt.

Die Eigenschaften der Sicherheitsfunktion „Schutz von Konfigurationsdateien“, die zur Erfüllung der funktionalen Anforderungen beitragen sind:

Nr.	Eigenschaften	Trägt bei zu
1	Alle Konfigurationsdateien die VPNConnect verwendet, werden verschlüsselt auf den Datenträger gespeichert.	FMT_MSA.3 FPT_ITT.EX.1 FCS_CKM.3
2	Die vom Authentifizierungsserver zu generierenden Konfigurationsdateien werden mittels eines Challenge-Responsemechanismus verschlüsselt übertragen und von VPNConnect entschlüsselt.	FIA_UAU.1 FIA_UID.1 FIA_SOS.2

Tabelle 6.4 – Schutz von Konfigurationsdateien

6.1.5 IP-Sicherheitsrichtlinienverwaltung

IPS.1 Während der Laufzeit werden dynamisch IP-Sicherheitsrichtlinien angelegt, die es erlauben, Verbindungen zu spezifizierten Netzen mit einem geeigneten Algorithmus zu verschlüsseln.[18]

IPS.2 Der in einer IP-Sicherheitsrichtlinie zum Aufbau einer VPN-Verbindung zu verwendende Verschlüsselungsalgorithmus und die zu verwendende Hashing-Funktion sind dynamisch setzbar.

IPS.3 Bei der Anlage von IP-Sicherheitsrichtlinien werden Zugriffe auf andere Netze als das vertraute Netz blockiert.

IPS.4 Benutzerdaten werden nur dann übermittelt, wenn ein Produktivtunnel unter Verwendung von Zertifikaten erfolgreich aufgebaut wurde, serverseitig eine Regel für das private Benutzerzertifikat vorhanden ist und die Verbindung zu einem Zielserver im vertrauten Netz steht.[19]

IPS.5 Die IP-Sicherheitsrichtlinienverwaltung ist unabhängig von der Windows-eigenen Benutzerverwaltung in der Lage, Sicherheitsrichtlinien zu erstellen, zu ändern, zu aktivieren, zu deaktivieren und zu löschen.[20]

---

[18] Der EVG übernimmt das Anlegen, Modifizieren, Löschen, Aktivieren und Deaktivieren von IP-Sicherheitsrichtlinien. Diese IP-Sicherheitsrichtlinien sind essentiell durch die Definition der Netze bestimmt, die durch den EVG bestimmt und durch die vom Authentifizierungsserver übertragene Konfigurationsdatei definiert werden. Der physikalische IP-Sicherheitsrichtlinien-Speicher und deren Verwaltung und In-Kraft-Setzen wird durch Funktionen des Betriebssystems bereitgestellt, die vom EVG aufgerufen werden.
Die Verwaltung des zu verwendenden Verschlüsselungsalgorithmus wird vom EVG übernommen.

[19] Der EVG erlaubt nur dann die Übermittlung von Daten, wenn die o.a. Bedingungen erfüllt sind. Ansonsten gilt die VPN-Verbindung als nicht aufgebaut und der EVG verweigert die Übertragung von Benutzerdaten.

[20] Der EVG ist auch dann in der Lage, Funktionalitäten zur IP-Sicherheitsrichtlinienverwaltung des Betriebssystems aufzurufen und auszuführen, wenn der angemeldete Benutzer des Betriebssystems über keine Administrationsrechte verfügt. Um dies zu ermöglichen werden diverse Funktionen der MFC und Funktionalitäten des Betriebssystems verwendet. Die Zeitpunkte und der Ablauf sowie die Kontrollmechanismen werden vom EVG bereitgestellt.

Die Eigenschaften der Sicherheitsfunktion „IP-Sicherheitsrichtlinienverwaltung“, die zur Erfüllung der funktionalen Anforderungen beitragen sind:

Nr.	Eigenschaften	Trägt bei zu
1	Während der Laufzeit werden dynamisch IP-Sicherheitsrichtlinien angelegt, die es erlauben, Verbindungen zu spezifizierten Netzen mit einem geeigneten Algorithmus zu verschlüsseln.	FDP_IFF.EX.1
2	Der in einer IP-Sicherheitsrichtlinie zum Aufbau einer VPN-Verbindung zu verwendende Verschlüsselungsalgorithmus und die zu verwendende Hashing-Funktion sind dynamisch setzbar.	FDP_IFF.EX.1
3	Bei der Anlage von IP-Sicherheitsrichtlinien werden Zugriffe auf andere Netze als das vertraute Netz blockiert.	FDP_IFF.EX.1
4	Benutzerdaten werden nur dann übermittelt, wenn ein Produktivtunnel unter Verwendung von Zertifikaten erfolgreich aufgebaut wurde, serverseitig eine Regel für das private Benutzerzertifikat vorhanden ist und die Verbindung zu einem Zielserver im vertrauten Netz steht.	FDP_IFF.EX.1 FDP_ACF.1
5	Die IP-Sicherheitsrichtlinienverwaltung ist unabhängig von der Windows-eigenen Benutzerverwaltung in der Lage, Sicherheitsrichtlinien zu erstellen, zu ändern, zu aktivieren, zu deaktivieren und zu löschen.	FDP_IFF.EX.1

Tabelle 6.5 – IP-Sicherheitsrichtlinienverwaltung

6.1.6 Spezifikation der Geheimnisse

SG.1 VPNConnect generiert für die Authentifizierung am Authentifizierungsserver sog. Challenges, die laufzeitgeneriert und eindeutig sind.

Die Eigenschaften der Sicherheitsfunktion „Spezifikation der Geheimnisse“, die zur Erfüllung der funktionalen Anforderungen beitragen sind:

Nr.	Eigenschaften	Trägt bei zu
1	VPNConnect generiert für die Authentifizierung am Authentifizierungsserver sog. Challenges, die laufzeitgeneriert und eindeutig sind.	FIA_SOS.2

Tabelle 6.6 – Spezifikation der Geheimnisse

6.2 Maßnahmen zur Vertrauenswürdigkeit

In der nachfolgenden Tabelle wird aufgezeigt, welche Maßnahmen zur Sicherung der Vertrauenswürdigkeit in der Entwicklung getroffen wurden, um die in EAL2 spezifizierten Anforderungen an die Vertrauenswürdigkeit zu erfüllen.

Anforderungen EAL2	**Maßnahmen des Entwicklers**
Konfigurationsmanagement	Ein projektorientierter KM-Plan im Rahmen eines Konfigurationsmanagements wird erstellt. Der Entwickler betreibt ein Konfigurationsmanagement, das alle Versionen für alle Konfigurationsteile verwaltet und die Sicherheitsfunktionen des Betriebssystems nutzt, um sicherzustellen, dass keine unerlaubten Modifikationen am EVG vorgenommen werden. (SourceSafe) Das eingesetzte Konfigurationskontrollsystem verfolgt die Darstellung der Implementierung, Design, Tests und Dokumentation.
ACM_CAP.2 Konfigurationsteile	
Auslieferung und Betrieb	Entsprechende Verfahren befinden sich im Einsatz. Auslieferungsprozeduren sind klar definiert und strukturiert. Diese Aspekte werden im Systemverwalterhandbuch erläutert.
ADO_DEL.1 Auslieferungsprozeduren	
ADO_IGS.1 Installations-, Generierungs- und Anlaufprozeduren	
Entwicklung	
ADV_FSP.1 Informelle funktionale Spezifikation	Es wird eine informelle Spezifikation bereitgestellt, die die externen Schnittstellen beschreibt.
ADV_HLD.1 Beschreibender Entwurf auf hoher Ebene	Eine funktionale Spezifikation wird bereitgestellt, die den Zweck und die Methode des Gebrauchs beschreibt. Die Methodik der Schnittstellen, die Details der Wirkungen, Ausnahmen und Fehlermeldungen sind daraus ersichtlich.
ADV_RCR.1 Informeller Nachweis der Übereinstimmung	Der Entwickler stellt eine Analyse bereit, die die Übereinstimmung aller benachbarten Paare mit den bereitgestellten TSF-Darstellungen darstellen.
AVA_SOF.1 Stärke der EVG-Sicherheitsfunktionen	Da kein Postulat zur Stärke der Funktionen abgegeben wurde, wird kein entsprechendes Dokument bereitgestellt.
Handbücher	Handbücher sind verfügbar und werden in elektronischer Form mit dem EVG ausgeliefert.

Anforderungen EAL2	**Maßnahmen des Entwicklers**
AGD_ADM.1 Systemverwalterhandbuch	Das Handbuch für Systemverwalter und Benutzer gibt Hinweise zur Installation und zum sicheren Betrieb des EVG. Das Benutzerhandbuch gibt Hinweise zur sicheren Verwendung des EVG. Für herstellerautorisierte Administratoren ist ein eigenständiges Handbuch vorhanden.
AGD_USR.1 Benutzerhandbuch	
Testen	Der Entwickler setzt dokumentierte Testverfahren ein: - Tests der funktionalen Spezifikationen - Tests aller Sicherheitsfunktionen Eigenständige Test sind vom Evaluator durchzuführen.
ATE_COV.1 Nachweis der Testabdeckung	
ATE_FUN.1 Funktionales Testen	
ATE_IND.2 Unabhängiges Testen – Stichprobenartig	Der Entwickler stellt einen EVG und alle von ihm genutzten Testhilfsmittel bereit.
Schwachstellenbewertung	Der Entwickler führt verschiedene Analysen durch. Insbesondere wird eine Analyse zur Identifikation von Schwachstellen durchgeführt und deren Ergebnis dokumentiert.
AVA_VLA.1 Schwachstellenanalyse des Entwicklers	

Tabelle 6.7 – Maßnahmen zur Vertrauenswürdigkeit

6.3 Stärke der Funktionen

Alle EVG-Sicherheitsfunktionen beruhen auf einem Wahrscheinlichkeits- oder Permutationsmechanismus und nutzen kryptographische Algorithmen. In Übereinstimmung mit den Anforderungen des nationalen Zertifizierungsschemas wird hierfür kein Postulat zur Stärke dieser Funktionen abgegeben.

7 PP Postulate

Diese Sicherheitsvorgaben postulieren keine Konformanz zu einem Schutzprofil.

8 Erklärungen

8.1 Erklärung der Sicherheitsziele

Die folgende Tabelle zeigt auf, durch welche Sicherheitsziele die identifizierten Bedrohungen, Annahmen und Policies abgedeckt werden.

Bedrohungen – Annahmen – Policies / Sicherheitsziele	**O.AUTH**	**O.AUTOR**	**O.CERT**	**O.POLICY**	**O.CHGCONFIG**	**O.READCONFIG**	**O.INSTALL**	**OE.1**	**OE.2**	**OE.3**	**OE.4**	**OE.5**	**OE.6**	**OE.7**	**OE.8**	**OE.9**	**OE.10**	**OE.11**
T.1	x																	
T.2		x		x	x	x												
T.3						x												
T.4					x													
T.5			x	x					x									
T.6			x	x					x									
T.7			x	x					x									
P.1							x											
P.2					x													
A.LOCKEDCOMPUTER								x										
A.RADIUS										x								
A.VISP											x							
A.VPNGATE												x						
A.AUTH													x					
A.CREATECERT														x				
A.ACCESSCERT															x			
A.CREATEGENCERT																x		
A.TRUSTEDADMIN																	x	
A.TRUSTEDUSER																		x

Tabelle 8.1 - Abbildung der EVG-Sicherheitsumgebung auf die Sicherheitsziele

Die Policy **P.1** (Administratorenbestimmte Zugriffskontrolle) legt fest, dass die Installation des EVG nur durch Administratoren erfolgen darf.

Dies entspricht genau dem Sicherheitsziel O.INSTALL. Dieses Sicherheitsziel ist also hinreichend für P.1.

Die Policy **P.2** (Administratorbestimmte Aktionen) legt fest, dass die Aktionen autorisierter Benutzer des EVG nur durch herstellerautorisierte Administratoren definiert werden.

Dies entspricht dem Sicherheitsziel O.CHGCONFIG. Dieses Sicherheitsziel ist also hinreichend für P.2.

Die Bedrohung **T.1** (nicht authentifizierter Benutzer) behandelt Angriffe, bei denen angenommen wird, dass Zugriffe auf Funktionen des EVG durch Personen erfolgen, die nicht zur Benutzung berechtigt sind.

Nach O.AUTH wird definiert dass der Zugriff auf autorisierte Benutzer beschränkt wird. Damit wird diese Bedrohung durch das Ziel O.AUTH adressiert.

Die Bedrohung **T.2** (nicht autorisierter Zugriff) behandelt Angriffe, bei denen angenommen wird, dass nicht autorisierte Zugriffe auf Funktionen des EVG durch Personen erfolgen, die zur Benutzung berechtigt sind.

Nach O.AUTOR wird definiert dass Zugriffe auf IP-Adressbereiche auf autorisierte Benutzer begrenzt werden.

Nach O.CHGCONFIG wird definiert dass, unautorisierte Änderungen an Konfigurationsdateien erkannt werden.

Nach O.READCONFIG wird definiert, dass Konfigurationsdateien nur von herstellerautorisierten Personen gelesen werden können. Die Authentifizierung kann nur gegenüber einem in der Konfigurationsdatei verschlüsselt gespeichertem Authentifizierungsserver erfolgen.

Nach O.POLICY wird definiert, dass die Funktionalität der benötigten Sicherheitsrichtlinien-Verwaltung (erstellen, modifizieren, aktivieren, deaktivieren und löschen von Sicherheitsrichtlinien) bereitgestellt wird. Durch die Managementfunktionalität der IP-Sicherheitsrichtlinienverwaltung, durch die im Durchgriff explizit VPN-Verbindungen aufgebaut werden, wird sichergestellt, dass nur autorisierte Personen die entsprechenden VPN-Verbindungen aufbauen können.

Damit wird diese Bedrohung gemeinsam durch die Ziele O.AUTH, O.POLICY, O.CHGCONFIG und O.READCONFIG adressiert.

Die Bedrohung **T.3** (Lesender Zugriff auf von VPNConnect verwaltete Konfigurationsdaten unter Umgehung der Anwendung VPNConnect.) behandelt Angriffe, bei denen angenommen wird, dass ein Angreifer versucht Zugriff auf Daten des EVG, z.B. über andere Anwendungen, zu erhalten.

Nach O.READCONFIG wird definiert, dass Konfigurationsdateien nur von herstellerautorisierten Personen gelesen werden können.

Damit wird diese Bedrohung durch das Ziel O.READCONFIG adressiert.

Die Bedrohung **T.4** (Manipulation auf von VPNConnect verwaltete Konfigurationsdaten unter Umgehung der Anwendung VPNConnect) behandelt Angriffe, bei denen davon ausgegangen wird, dass ein Angreifer unautorisiert und unerkannt versucht, Konfigurationsdateien zu modifizieren.

Nach O.CHGCONFIG wird definiert dass, unautorisierte Änderungen an Konfigurationsdateien erkannt werden. Damit wird diese Bedrohung durch das Ziel O.CHGCONFIG adressiert.

Die Bedrohung **T.5** (Unbefugte Kenntnisnahme von Benutzerdaten auf dem Übertragungsweg) behandelt Angriffe bei denen angenommen wird, dass ein Angreifer unautorisiert und unerkannt versucht, Informationen auf dem Übertragungsweg abzuhören.

Nach O.CERT wird definiert, dass die Funktionalität des benötigten Zertifikatsmanagement (importieren und löschen von Zertifikaten) bereitgestellt wird.

Nach O.POLICY wird definiert, dass die Funktionalität der benötigten Sicherheitsrichtlinien-Verwaltung (erstellen, modifizieren, aktivieren, deaktivieren und löschen von Sicherheitsrichtlinien) bereitgestellt wird.

Nach OE.2 wird definiert, dass die Herkunft von Datenpaketen, die von autorisierten Benutzern in geschützte Netzwerke versandt werden, vom Empfänger verifiziert werden können. Ebenso wird definiert, dass Datenpakete die von autorisierten Benutzern in geschützte Netzwerke geschickt und empfangen werden, von keiner Seite wiederholt gesendet werden können. Es wird ebenfalls definiert, dass Datenpakete, die von autorisierten Benutzern in geschützte Netzwerke gesendet und empfangen werden, verschlüsselt werden.

Damit wird diese Bedrohung durch die Ziele O.CERT, O.POLICY und OE.2 in ihrer Gesamtheit adressiert.

Die Bedrohung **T.6** (Versuch, Benutzerdaten auf dem Übertragungsweg zu modifizieren) behandelt Angriffe bei denen angenommen wird, dass ein Angreifer unautorisiert und unerkannt versucht, Benutzerdaten auf dem Übertragungsweg zu modifizieren, einzufügen, umzuordnen, zu löschen oder zu wiederholen.

Nach O.CERT wird definiert, dass die Funktionalität des benötigten Zertifikatsmanagement (importieren und löschen von Zertifikaten) bereitgestellt wird.

Nach O.POLICY wird definiert, dass die Funktionalität der benötigten Sicherheitsrichtlinien-Verwaltung (erstellen, modifizieren, aktivieren, deaktivieren und löschen von Sicherheitsrichtlinien) bereitgestellt wird.

Nach OE.2 wird definiert, dass die Herkunft von Datenpaketen, die von autorisierten Benutzern in geschützte Netzwerke versandt werden, vom Empfänger verifiziert werden können. Ebenso wird definiert, dass Datenpakete die von autorisierten Benutzern in geschützte Netzwerke geschickt und empfangen werden, von keiner Seite wiederholt gesendet werden können. Es wird ebenfalls definiert, dass Datenpakete, die von autorisierten Benutzern in geschützte Netzwerke gesendet und empfangen werden, verschlüsselt werden. Als Protokolle können z.B. IPSEC, L2TP/IPSEC oder vergleichbare Protokolle verwendet werden. Diese Protokolle haben die Eigenschaft, dass sie das Einfügen, Modifizieren und Löschen von Datenpaketen verhindern.

Damit wird diese Bedrohung durch die Ziele O.CERT, O.POLICY und OE.2 in ihrer Gesamtheit adressiert.

Die Bedrohung **T.7** (Vortäuschung einer Identität durch Eingriff auf dem Übertragungsweg) behandelt Angriffe bei denen angenommen wird, dass ein Angreifer unautorisiert und unerkannt versucht, die Identität eines Benutzers auf dem Übertragungsweg anzunehmen, um dadurch eine unzulässige Kommunikationsverbindung aufzubauen.

Nach O.CERT wird definiert, dass die Funktionalität des benötigten Zertifikatsmanagement (importieren und löschen von Zertifikaten) bereitgestellt wird.

Nach O.POLICY wird definiert, dass die Funktionalität der benötigten Sicherheitsrichtlinien-Verwaltung (erstellen, modifizieren, aktivieren, deaktivieren und löschen von Sicherheitsrichtlinien) bereitgestellt wird. Durch die Managementfunktionalität der IP-Sicherheitsrichtlinienverwaltung, durch die im Durchgriff explizit VPN-Verbindungen aufgebaut werden, wird sichergestellt, dass nur autorisierte Personen die entsprechenden VPN-Verbindungen aufbauen können.

Nach OE.2 wird definiert, dass die Herkunft von Datenpaketen, die von autorisierten Benutzern in geschützte Netzwerke versandt werden, vom Empfänger verifiziert werden können. Ebenso wird definiert, dass Datenpakete die von autorisierten Benutzern in geschützte Netzwerke geschickt und empfangen werden, von keiner Seite wiederholt gesendet werden können. Es wird ebenfalls definiert, dass Datenpakete, die von autorisierten Benutzern in geschützte Netzwerke gesendet und empfangen werden, verschlüsselt werden.

Damit wird diese Bedrohung gemeinsam durch die Ziele O.CERT, O.POLICY und OE.2 adressiert.

Die Annahme **A.RADIUS** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass netzseitig ein RADIUS - Server zur Verfügung gestellt wird, an dem sich Clients mittels CHAP authentifizieren müssen.

Dies entspricht exakt dem Ziel OE.3.

Die Annahme **A.VISP** behandelt eine Vorgabe, bei der zugrunde gelegt wird, Clients die sich mittels einer DSL – Einwahlverbindung in das Internet einwählen müssen, netzseitig durch VISP oder ein analoges System verifiziert und authentifiziert werden.

Das Ziel OE.4 fordert den Zugriff auf die VISP-Struktur der DTAG bzw. ein analoges System. Damit wird diese Annahme durch das Ziel OE.4 adressiert.

Die Annahme **A.VPNGATE** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass NAT-T fähige IPSEC VPN-Gateways serverseitig verwendet werden, um eine eindeutige Rückverfolgung verschlüsselter IP-Adressen zu gewährleisten.

Dies entspricht exakt dem Ziel OE.5.

Die Annahme **A.AUTH** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass serverseitig ein geeigneter Authentifizierungsserver eingesetzt wird, der sich in einem eigenen Subnetz befinden muss, in dem sich kein weiterer Rechner findet.

Damit wird diese Annahme durch das Ziel OE.6 adressiert.

Die Annahme **A.CREATECERT** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass für jeden Benutzer des EVG eindeutige X.509 Benutzer-Zertifikate erstellt werden. OE.7 fordert den Aufbau oder die Verwendung eines TrustCenters zur Erstellung von Zertifikaten.

Damit wird diese Annahme durch das Ziel OE.7 adressiert.

Die Annahme **A.ACCESSCERT** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass Benutzer-Zertifikate auf einen Authentifizierungsserver bereitgestellt werden, der ausschließlich über einen aufgebauten VPN Tunnel erreicht werden kann.

Dies entspricht exakt dem Ziel OE.8.

Die Annahme **A.CREATEGENCERT** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass pro Branding ein generisches Zertifikat zum Zugriff auf den Authentifizierungsserver und die verwendeten Gateways benutzt wird.

Dies entspricht exakt dem Ziel OE.9.

Die Annahme **A.TRUSTEDADMIN** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass nur kompetente, vertrauenswürdige und ausgebildete Personen mit der Administration des EVG vertraut werden.

Dies entspricht exakt dem Ziel OE.10.

Die Annahme **A.TRUSTEDUSER** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass vertrauliche Informationen nicht zur Kenntnis Anderer gelangen.

Dies entspricht exakt dem Ziel OE.11.

Die Annahme **A.LOCKEDCOMPUTER** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass verwendete Hardwarekomponenten vor Entwendung geschützt sind und Unberechtigte keinen Zugriff auf physikalischen Speicherort des EVG erhalten.

Dies entspricht exakt dem Ziel OE.1.

8.2 Erklärung der Sicherheitsanforderungen

8.2.1 Erklärung der funktionalen Sicherheitsanforderungen des EVG

Die folgende Tabelle zeigt auf, durch welche EVG-Sicherheitsfunktionen die Funktionalen Sicherheitsanforderungen an den EVG abgedeckt werden.

EVG-Sicherheitsfunktionen / Funktionale Sicherheitsanforderungen an den EVG	**O.AUTH**	**O.AUTOR**	**O.CERT**	**O.POLICY**	**O.CHGCONFIG**	**O.READCONFIG**	**O.INSTALL**
FCS_CKM.2		x					
FCS_CKM.3			x	x			
FCS_CKM.4			x				
FDP_ACC.2		x		x			
FDP_ACF.1		x		x			
FIA_UAU.1	x						
FIA_UAU.7	x						
FIA_UID.1	x						
FIA_UAU.EX.1	x						
FIA_UID.EX.1	x						
FIA_SOS.2	x						
FDP_IFF.EX.1				x			
FPT_ITT.EX.1					x	x	
FMT_MSA.1					x	x	x
FMT_MSA.3					x	x	x
FMT_SMF.1					x		x
FMT_SMR.1					x	x	x

Tabelle 8.2 - Abbildung der EVG-Sicherheitsziele auf Funktionale Sicherheitsanforderungen an den EVG

Das **Sicherheitsziel O.AUTH** legt fest, dass der Zugriff auf die im EVG bereitgestellten Funktionen auf diejenigen Personen beschränkt wird, die authentisiert sind.

FIA_UAU.1 fordert, dass nur der Aufruf der Konfiguration der Verbindungsart erlaubt ist bevor sich der Benutzer authentisieren muss.

FIA_UAU.7 fordert, dass während der Authentisierung nur Rückmeldungen ohne Rückgriff auf Benutzernamen und Passwort sowie Fehler bei Eingabe dieser Attribute an den Benutzer bereitgestellt werden.

FIA_UID.1 fordert, nur den Aufruf der Konfiguration der Verbindungsart zu erlauben, bevor der Benutzer identifiziert wird.

FIA_UAU.EX.1 fordert, dass nur der Aufruf der Konfiguration der Verbindungsart erlaubt ist bevor sich der Benutzer bei Interneteinwahlverbindungen online gegenüber einem RADIUS-Server authentisieren muss.

FIA_UID.EX.1 fordert, nur den Aufruf der Konfiguration der Verbindungsart zu erlauben, bevor der Benutzer bei Interneteinwahlverbindungen online gegenüber einem RADIUS-Server identifiziert wird.

FIA_SOS.2 fordert, dass die TSF in der Lage sein müssen, den Gebrauch der TSF-generierten Geheimnisse für die Identifikation und Autorisierung von Benutzern durchzusetzen.

Diese sechs Anforderungen sind in Ihrer Gesamtheit geeignet, das Ziel O.AUTH zu erreichen.

Das **Sicherheitsziel O.AUTOR** legt fest, dass Zugriffe auf IP-Adressbereiche (geschütztes Netz) auf die jeweils autorisierten Benutzer begrenzt werden.

FCS_CKM.2 definiert, wie die kryptographischen Schlüssel zu verteilen sind, nämlich

- nach erfolgreicher Authentisierung am Authentifizierungsserver
- von einem Pfad, der dem Client als Ergebnis der Authentisierung übermittelt wurde
- gesichert durch den Authentifizierungstunnel

FDP_ACC.2 verlangt die vollständige Zugriffskontrolle für alle Operationen zwischen dem lokalen Client und dem geschützten Netz über das Durchsetzen einer Zugriffskontrollpolitik.

FDP_ACF.1 verlangt, die Zugriffskontrollpolitik auf Basis von IP-Adressbereichen und Zertifikaten durchzusetzen. Die Autorisierung muss durch einen zertifikatsbasierten Tunnel erfolgen, wobei folgende Anforderungen gestellt werden:

- Gültigkeit der benutzten Zertifikate für den Aufbau des Authentifizierungstunnels
- Import der benötigten Zertifikate möglich
- Korrespondenz zwischen lokalem Zertifikat und Zertifikaten auf dem VPN-Gateway
- Der lokale Client baut nur VPN-Verbindungen zu der in der Konfigurationsdatei gespeicherten IP-Adressbereichen (Authentifizierungstunnel) oder zur Laufzeit vom Authentifizierungsserver übermittelten IP-Adressbereichen (Produktivtunnel) auf.
- Ein Verbindungsaufbau zum VPN-Gateway ist nur möglich, wenn das lokale private Zertifikat und die aufzubauende Verbindung (IP-Adressbereich) mit den am VPN-Gateway eingerichteten Richtlinien korrespondieren.

- Ein Zugriff auf die in der Konfigurationsdatei gespeicherten oder zur Laufzeit vom Authentifizierungsserver übermittelten IP-Adressbereiche ist nur möglich, wenn die VPN-Verbindung erfolgreich aufgebaut wurde.

Diese drei Anforderungen sind in Ihrer Gesamtheit geeignet, das Ziel O.AUTOR zu erreichen.

Das **Sicherheitsziel O.CERT** legt fest, dass die Funktionalität, des zum Aufbau eines VPN-Tunnels benötigten Zertifikats-Management (Import und Löschen der Zertifikate) sichergestellt wird.

FCS_CKM.3 erfordert

- den Schutz privater Zertifikate vor Import durch Passwörter
- die Speicherung dieser Passwörter für den Aufbau des Authentifizierungstunnels verschlüsselt in Konfigurationsdateien und
- die geschützte Übermittlung von Passwörtern für den Aufbau des Authentifizierungstunnels als Ergebnis der Authentisierung.

FCS_CKM.4 fordert, nach jedem VPN-Tunnelabbau die Zertifikate aus dem Windows-Zertifikatsspeicher und bei Beenden der Applikation physikalisch vom Datenträger zu löschen. Ebenso muss bei Verbindungsunterbrechung zu den angegebenen Produktivservern der VPN-Tunnel sofort abgebaut werden.

Diese zwei Anforderungen sind in Ihrer Gesamtheit geeignet, das Ziel O.CERT zu erreichen.

Das **Sicherheitsziel O.POLICY** legt fest, dass die Funktionalität, des zum Aufbau eines VPN-Tunnels benötigten Sicherheitsrichtlinien-Management (Erstellung, Modifikation, Aktivierung, Deaktivierung und Löschen von Sicherheitsrichtlinien) sichergestellt wird.

FCS_CKM.3 erfordert

- den Schutz privater Zertifikate vor Import durch Passwörter
- die Speicherung dieser Passwörter für den Aufbau des Authentifizierungstunnels verschlüsselt in Konfigurationsdateien und
- die geschützte Übermittlung von Passwörtern für den Aufbau des Authentifizierungstunnels als Ergebnis der Authentisierung.

FDP_ACC.2 verlangt die vollständige Zugriffskontrolle für alle Operationen zwischen dem lokalen Client und dem geschützten Netz über das Durchsetzen einer Zugriffskontrollpolitik.

FDP_ACF.1 verlangt, die Zugriffskontrollpolitik auf Basis von IP-Adressbereichen und Zertifikaten durchzusetzen. Die Autorisierung muss durch einen zertifikatsbasierten Tunnel erfolgen, wobei folgende Anforderungen gestellt werden:

- Gültigkeit der benutzten Zertifikate für den Aufbau des Authentifizierungstunnels
- Import der benötigten Zertifikate möglich
- Korrespondenz zwischen lokalem Zertifikat und Zertifikaten auf dem VPN-Gateway

FDP_IFF.EX.1 fordert

- dynamisch IP-Sicherheitsrichtlinien anzulegen, die Verbindungen zu spezifizierten Netzen mittels z.B. IPSEC verschlüsseln

- den für die Verschlüsselung der Daten zu verwendenden Algorithmus (z.B. 3DES) und die zu verwendende Hashing-Funktion (z.B. MD5) zu setzen
- dynamisch Tunnelendpunkte zu setzen
- aufgrund erfolgter Autorisierung Zugriffsrechte zu setzen
- private Zertifikate zum Aufbau der VPN-Verbindungen zu setzen
- Zugriffe auf andere Netze als das geschützte Netz zu verweigern
- Serverseitig die Nichtabstreitbarkeit der Urheberschaft von übermittelten Daten auswerten zu können
- Benutzerdaten nur nach erfolgtem VPN-Aufbau übermitteln zu lassen
- die Sicherheitsrichtlinienverwaltung unabhängig vergebener Benutzerrechte lauffähig zu halten

Diese vier Anforderungen sind in Ihrer Gesamtheit geeignet, das Ziel O.POLICY zu erreichen.

Das **Sicherheitsziel O.CHGCONFIG** legt fest, dass unautorisiert durchgeführte Änderungen an Konfigurationsdateien erkannt werden.

FPT_ITT.EX.1 fordert, die Konfigurationsdateien gegen unerkannte Modifizierung zu schützen.

FMT_MSA.1 fordert, sichere Standardvorgaben nur durch Administratoren mit Herstellerautorisierung durchführen zu lassen.

FMT_MSA.3 fordert, Zugriffskontrollpolitiken zur Bereitstellung von vorgegebenen Standardwerten mit einschränkenden Eigenschaften durchzusetzen und alternative Standardwerte nur Administratoren mit Herstellerautorisierung zu gestatten.

FMT_SMF.1 fordert, dass alternative Anfangswerte, die die vorgegebenen Standardwerte ersetzen, dürfen nur von Administratoren mit Herstellerautorisierung gesetzt werden.

FMT_SMR.1 fordert, dass die TSF die Rollen Benutzer, Betriebssystemadministratoren, Administratoren mit Herstellerautorisierung erhalten und die TSF Benutzer mit Rollen verknüpfen können müssen.

Diese fünf Anforderungen sind in Ihrer Gesamtheit geeignet, das Ziel O.CHGCONFIG zu erreichen.

Das **Sicherheitsziel O.READCONFIG** legt fest, dass Konfigurationsdateien nur von herstellerautorisierten Personen gelesen werden können.

FPT_ITT.EX.1 fordert, die Konfigurationsdateien gegen unerkannte Modifizierung zu schützen.

FMT_MSA.1 fordert, sichere Standardvorgaben nur durch Administratoren mit Herstellerautorisierung durchführen zu lassen.

FMT_MSA.3 fordert, Zugriffskontrollpolitiken zur Bereitstellung von vorgegebenen Standardwerten mit einschränkenden Eigenschaften durchzusetzen und alternative Standardwerte nur Administratoren mit Herstellerautorisierung zu gestatten.

FMT_SMR.1 fordert, dass die TSF die Rollen Benutzer, Betriebssystemadministratoren, Administratoren mit Herstellerautorisierung erhalten und die TSF Benutzer mit Rollen verknüpfen können müssen.

Diese vier Anforderungen sind in Ihrer Gesamtheit geeignet, das Ziel O.READCONFIG zu erreichen.

Das **Sicherheitsziel O.INSTALL** legt fest, dass Installation(en) auf ein Zielsystem nur durch Administratoren des Betriebssystems erfolgen.

FMT_MSA.1 fordert, sichere Standardvorgaben nur durch Administratoren mit Herstellerautorisierung durchführen zu lassen.

FMT_MSA.3 fordert, Zugriffskontrollpolitiken zur Bereitstellung von vorgegebenen Standardwerten mit einschränkenden Eigenschaften durchzusetzen und alternative Standardwerte nur Administratoren mit Herstellerautorisierung zu gestatten.

FMT_SMF.1 fordert, dass die Installation nur durch Administratoren des Betriebssystems durchgeführt werden darf.

FMT_SMR.1 fordert, dass die TSF die Rollen Benutzer, Betriebssystemadministratoren, Administratoren mit Herstellerautorisierung erhalten und die TSF Benutzer mit Rollen verknüpfen können müssen.

Diese vier Anforderungen sind in Ihrer Gesamtheit geeignet, das Ziel O.INSTALL zu erreichen.

8.2.2 Erklärung der Anforderungen an die Vertrauenswürdigkeit des EVG

Die Vertrauenswürdigkeitsstufe EAL2 wurde ausgewählt, um einem Anwender ein Grundvertrauen zu vermitteln, dass eine unabhängige Evaluierung durch vertrauenswürdige Dritte nach international anerkannten Sicherheitskriterien durchgeführt wurde.

Die Analyse wird unterstützt durch unabhängiges Testen der EVG-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation, durch selektive, unabhängige Bestätigung der Entwicklertestergebnisse und durch einen Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen (zum Beispiel solchen, die allgemein bekannt sind).

Dies wird als sinnvoll erachtet, weil bei einem nur Angreifer begrenzte technische und zeitliche Möglichkeiten und allgemein verfügbare Kenntnisse der Informationstechnik, des Betriebssystems und des EVG angenommen werden.

8.2.3 Erklärung der explizit formulierten Anforderungen

O.POLICY verlangt, Funktionalität für die Sicherheitsrichtlinienverwaltung bereitzustellen. Diese Anforderungen sind zwar sehr spezifisch, lassen sich jedoch in der Basis von der Familie FDP_IFF ableiten. Aus diesem Grund wurde die explizit formulierte Anforderung **FDP_IFF.EX.1** eingeführt.

FPT_ITT.EX.1 stellt besondere Anforderungen an den Schutz der Konfigurationsdaten, die sich mit anderen Komponenten aus dem Teil 2 der CC nur schlecht modellieren lassen. Diese Anforderung wurde in Anlehnung an FPT_ITT.1 formuliert. Gegenüber dieser Anforderung bezieht sie sich nur auf Speicherung von Konfigurationsdaten.

O.AUTH verlangt, dass der EVG den Zugriff auf die im EVG bereitgestellten Funktionen auf diejenigen Personen beschränken muss, die authentisiert sind.

Realisiert wurde die Identifikation und Autorisierung über einen Client/Server-basierte Architektur. Die Identifikation und Authentisierung erfolgt im EVG aufgrund von Rückgaben des Authentifizierungsservers.

Da der EVG auch den Aufbau von Internetverbindungen zur Verfügung stellt, wurde die rein serverseitig vorhandene Identifikations- und Authentisierungsfunktionalität am RADIUS-Servern als Kombination von Anforderungen an den EVG und die Umgebung abgebildet.

Die Anforderungen aus Teil 2 der CC (FIA_UAU.1 und FIA_UID.1) wurden als Basis für die Abbildung der-RADIUS-Authentifizierung herangezogen, die im EVG in der Definition der Anforderungen **FIA_UAU.EX.1** und **FIA_UID.EX.1** resultiert sowie als Anforderung an die IT-Umgebung **FIA_UAU.EX.EXT.1** und **FIA_UID.EX.EXT.1** jeweils in Anlehnung an FIA_UAU.1 und FIA_UID.1 formuliert.

8.2.4 Erklärung der Anforderungen an die Stärke der EVG-Sicherheitsfunktionen

Es wurde kein Postulat zur Stärke der Funktionen abgegeben.

8.2.5 Erklärung der gegenseitigen Unterstützung der funktionalen Anforderungen und der Anforderungen an die Vertrauenswürdigkeit des EVGs

Die folgende Tabelle zeigt die Abhängigkeiten zwischen den verschiedenen funktionalen Sicherheitsanforderungen auf und zeigt auf, ob die Abhängigkeiten aufgelöst sind. Die angeführten Hinweise geben hierzu weitere Erläuterungen und Begründungen.

SFR	**Abhängigkeiten**	**aufgelöst**
FCS_CKM.2	(FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FCS_CKM.1 Kryptographische Schlüsselgenerierung) FCS_CKM.4 Zerstörung des kryptographischen Schlüssels FMT_MSA.2 Sichere Sicherheitsattribute	**nein**, siehe Hinweis 1
FCS_CKM.3	(FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FCS_CKM.1 Kryptographische Schlüsselgenerierung) FCS_CKM.4 Zerstörung des kryptographischen Schlüssels FMT_MSA.2 Sichere Sicherheitsattribute	**nein**, siehe Hinweis 1
FCS_CKM.4	(FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute oder FCS_CKM.1 Kryptographische Schlüsselgenerierung) FMT_MSA.2 Sichere Sicherheitsattribute	**nein**, siehe Hinweis 1
FDP_ACC.2	FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen	**ja**
FDP_ACF.1	FDP_ACC.1 Teilweise Zugriffkontrolle FMT_MSA.3 Initialisierung statischer Attribute	**ja**, siehe Hinweis 2
FIA_UAU.1	FIA_UID.1 Zeitpunkt der Identifikation	**ja**
FIA_UAU.EX.1	FIA_UID.EX.1 Externe Identifikation der Benutzer bei Start des EVG FIA_UAU.EX.EXT.1 Serverseitige Authentisierung	**nein,** siehe Hinweis 3
FIA_UAU.7	FIA_UAU.1 Zeitpunkt der Authentisierung	**ja**
FIA_UID.1	(keine Abhängigkeiten)	**ja**, implizit
FIA_UID.EX.1	FIA_UID.EX.EXT.1 Serverseitige Identifizierung	**nein,** siehe Hinweis 4
FIA_SOS.2	(keine Abhängigkeiten)	**ja**, implizit
FDP_IFF.EX.1	FCS_CKM.2 Verteilung des kryptographischen Schlüssels FCS_CKM.3 Zugriff auf einen kryptographischen Schlüssel FCS_CKM.4 Zerstörung des kryptographischen Schlüssels	**ja**
FMT_MSA.1	(FDP_ACC.1 Teilweise Zugriffkontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle) FMT_SMR.1 Sicherheitsrollen	**ja**, siehe Hinweis 2

SFR	Abhängigkeiten	aufgelöst
FMT_MSA.3	FMT_MSA.1 Management der Sicherheitsattribute FMT_SMR.1 Sicherheitsrollen	**ja**
FMT_SMF.1	(keine Abhängigkeiten)	**ja**, implizit
FMT_SMR.1	FIA_UID.1 Zeitpunkt der Identifikation	**ja**
FPT_ITT.EX.1	FCS_CKM.2 Verteilung des kryptographischen Schlüssels FCS_CKM.3 Zugriff auf einen kryptographischen Schlüssel FCS_CKM.4 Zerstörung eines kryptographischen Schlüssels	**ja**

Tabelle 8.3 - Erfüllung der Abhängigkeiten zwischen Funktionalen Sicherheitsanforderungen

Hinweis 1: Die Abhängigkeit zu FCS_CKM.4 ist aufgelöst. Die Abhängigkeiten zu FCS_CKM.1, FMT_MSA.2 bzw. FDP_ITC.1 sind nicht aufgelöst, weil Schlüssel und Schlüsselzertifikate außerhalb des EVG erzeugt (siehe Annahme A.CREATECERT für Benutzer-Zertifikate und Annahme A.CREATEGENCERT für generisches Zertifikat) und bereitgestellt (siehe Annahme A.ACCESSCERT für Benutzer-Zertifikate und Annahme A.CREATEGENCERT für generisches Zertifikat) werden. Die Komponenten FCS_CKM.1, FMT_MSA.2 bzw. FDP_ITC.1 sind daher für den EVG nicht anwendbar.

Hinweis 2: Statt der Komponente FDP_ACC.1 wurde die Komponente FDP_ACC.2 ausgewählt, die hierarchisch zur Komponente FDP_ACC.1 ist.

Hinweis 3: Die Abhängigkeit zu FIA_UID.EX.1 ist aufgelöst. Die Abhängigkeit zu FIA_UAU.EX.EXT.1 ist nicht aufgelöst weil die RADIUS-Authentisierung außerhalb des EVG erfolgt, aber durch eine Annahme an die Umgebung abgebildet wird.

Hinweis 4: Die Abhängigkeit zu FIA_UID.EX.EXT.1 ist nicht aufgelöst weil die RADIUS-Identifizierung außerhalb des EVG erfolgt, aber durch eine Annahme an die Umgebung abgebildet wird.

Die Vertrauenswürdigkeitskomponenten wurden der Vertrauenswürdigkeitsstufe EAL2 entnommen.

EAL2 bildet ein in sich geschlossenes Ganzes.

8.2.6 Erklärung der Sicherheitsanforderungen an die IT-Umgebung

Die folgende Tabelle zeigt auf, durch welche Sicherheitsziele die in Kapitel 5.2 identifizierten Sicherheitsanforderungen an die Umgebung abgedeckt werden.

Sicherheitsanforderungen an die IT-Umgebung / Sicherheitsziele	**OE.2**	**OE.3**
FCO_NRO.1	x	
FCO_NRR.1	x	
FDP_UIT.1	x	
FDP_UCT.1	x	
FIA_UAU.EX.EXT.1		x
FIA_UID.EX.EXT.1		x

Tabelle 8.4 - Abbildung der Sicherheitsanforderungen an die IT-Umgebung auf die Sicherheitsziele

Die Einsatzumgebung ist so zu wählen, dass sie die Sicherheitsanforderungen **FCO_NRO.1**, **FCO_NRR.1**, **FDP_UIT.1** und **FDP_UCT.1** erfüllen.

Nach OE.2 ist definiert, dass das auf dem Zielsystem installierte Betriebsystem in der Lage sein muss, zertifikatsbasierte VPN-Verbindungen zu durch den EVG definierten geschützten Netzen aufzubauen. Als VPN-Verbindungsarten können z.B. IPSEC, L2TP oder IPSEC/L2TP verwendet werden.

Weiterhin müssen lt. OE.2 folgende Anforderungen erfüllt werden:

- Es muss sichergestellt sein, dass die Herkunft von Datenpaketen, die von autorisierten Benutzern in geschützte Netzwerke geschickt werden, vom Empfänger verifiziert werden kann.

- Es muss sichergestellt sein, dass Datenpakete, die von autorisierten Benutzern in geschützte Netzwerke geschickt und empfangen werden, von keiner Seite wiederholt gesendet werden.

- Es muss sichergestellt sein, dass Datenpakete, die von autorisierten Benutzern in geschützte Netzwerke geschickt und empfangen werden, verschlüsselt sind.

FCO_NRO.1 verlangt, dass das Betriebssystem:

- auf Anforderung des Urhebers und/oder Empfängers für übertragene Daten Urheberschaftsnachweise generieren können
- die Identität des Informationsurhebers den Informationen, auf die sich der Nachweis bezieht, zuordnen können und
- dem Urheber und/oder, Empfänger die Fähigkeit zum Verifizieren des Urheberschaftsnachweises von Informationen bereitstellen

muss.

FCO_NRR.1 verlangt, dass das Betriebssystem:

- auf Anforderung des Urhebers und/oder Empfängers für empfangene Daten Empfangsnachweise generieren können
- die Identität des Informationsempfängers den Informationen, auf die sich der Nachweis bezieht, zuordnen können und
- dem Urheber und/oder Empfänger die Fähigkeit zum Verifizieren des Empfangsnachweises von Informationen bereitstellen

muss.

FDP_UIT.1 verlangt, dass das Betriebssystem:

- die SFPs für Zugriffskontrolle und/oder SFPs für Informationsflußkontrolle durchsetzen muss, um in der Lage zu sein, Benutzerdaten vor Modifizieren, Löschen, Einfügen, Wiedereinspielen geschützt zu übertragen und/oder zu empfangen.
- in der Lage sein muss, beim Empfang der Benutzerdaten festzustellen, ob ein Modifizieren, Löschen, Einfügen, Wiedereinspielen stattgefunden hat.

FDP_UCT.1 verlangt, dass das Betriebssystem SFPs für Zugriffskontrolle und/oder SFPs für Informationsflußkontrolle durchsetzen muss, um in der Lage zu sein, Objekte vor nichtautorisierter Preisgabe geschützt zu übertragen, empfangen.

Microsoft Windows 2000 und Windows XP als Einsatzumgebung erfüllen diese Anforderungen.

FCO_NRO.1, FCO_NRR.1, FDP_UIT.1 und FDP_UCT.1 tragen somit in Ihrer Gesamtheit zur Erreichung von OE.2 bei.

Die IT-Umgebung ist so zu wählen, dass sie den Sicherheitsanforderungen **FIA_UAU.EX.EXT.1** und **FIA_UID.EX.EXT.1** erfüllen.

In OE.3 ist hierbei definiert, dass zur Authentifizierung der Clients muss netzseitig ein RFC 2865 konformer RADIUS-Server bereitgestellt werden muss. Dieser Radius-Server muss eingehende RADIUS-Anfragen mittels CHAP authentifizieren.

FIA_UAU.EX.EXT.1 fordert, dass bei Interneteinwahlverbindungen Benutzer online gegenüber einem RADIUS-Server mittels CHAP authentisiert werden müssen.

FIA_UID.EX.EXT.1 fordert, dass bei Interneteinwahlverbindungen Benutzer online gegenüber einem RADIUS-Server mittels CHAP identifiziert werden müssen.

FIA_UAU.EX.EXT.1 und FIA_UID.EX.EXT.1 tragen somit in Ihrer Gesamtheit zur Erreichung von OE.3 bei.

8.3 Erklärung der EVG-Übersichtsspezifikation

8.3.1 Erklärung der EVG-Sicherheitsfunktionen

Die folgende Tabelle zeigt auf, durch welche EVG-Sicherheitsfunktionen die Funktionalen Sicherheitsanforderungen an den EVG abgedeckt werden.

Funktionale Sicherheitsanforderungen an den EVG / EVG-Sicherheitsfunktionen	**FCS_CKM.2**	**FCS_CKM.3**	**FCS_CKM.4**	**FDP_ACC.2**	**FDP_ACF.1**	**FIA_UAU.1**	**FIA_UAU.EX.1**	**FIA_UAU.7**	**FIA_UID.1**	**FIA_UID.EX.1**	**FIA_SOS.2**	**FDP_IFF.EX.1**	**FMT_MSA.1**	**FMT_MSA.3**	**FPT_ITT.EX.1**	**FMT_SMF.1**	**FMT_SMR.1**
IA.1						x	x		x	x				x			x
IA.2							x			x							
IA.3						x			x		x	x					x
IA.4								x									
IA.5																x	x
AC.1				x	x							x					
AC.2				x	x							x					
AC.3					x								x	x		x	x
AC.4			x									x					
KM.1	x				x	x			x			x		x			
KM.2	x	x				x			x		x	x					
KM.3		x										x					
KM.4			x									x					
SG.1											x						
SK.1		x												x	x		
SK.2						x			x		x						
IPS.1												x					
IPS.2												x					
IPS.3												x					
IPS.4					x							x					
IPS.5												x					

Tabelle 8.5 - Abbildung der Funktionalen Sicherheitsanforderungen an den EVG auf EVG-Sicherheitsfunktionen.

Die Sicherheitsanforderung **FCS_CKM.2** fordert, wie die kryptographischen Schlüssel zu verteilen sind, nämlich

- nach erfolgreicher Authentisierung am Authentifizierungsserver
- von einem Pfad, der dem Client als Ergebnis der Authentisierung übermittelt wurde
- gesichert durch den Authentifizierungstunnel

Nach KM.1 wird das generische Zertifikat zum Aufbau des Authentifizierungstunnels vor jedem Verbindungsaufbau in den Benutzerzertifikatsspeicher importiert, und dient der sicheren Authentifizierung des Benutzers am Authentifizierungsserver.

KM.2 stellt sicher, dass bei vorhandenem Benutzerkonto am Authentifizierungsserver im vorher aufgebauten Authentifizierungstunnel eine mittels eines Challenge-Responsemechanismus verschlüsselte Konfigurationsdatei heruntergeladen wird, die u.a. den Ort der Benutzerzertifikate enthält, die im nächsten Schritt gesichert auf den Rechner heruntergeladen werden und physikalisch auf dem Datenträger gespeichert werden. Die Zertifikate werden im Anschluss automatisch in den Windows-Zertifikatsspeicher importiert.

Diese beiden Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FCS_CKM.2 um.

Die Sicherheitsanforderung **FCS_CKM.3** fordert

- den Schutz privater Zertifikate vor Import durch Passwörter
- die Speicherung dieser Passwörter für den Aufbau des Authentifizierungstunnels verschlüsselt in Konfigurationsdateien und
- die geschützte Übermittlung von Passwörtern für den Aufbau des Produktivtunnels als Ergebnis der Authentisierung.

KM.2 stellt sicher, dass bei vorhandenem Benutzerkonto am Authentifizierungsserver im vorher aufgebauten Authentifizierungstunnel eine mittels eines Challenge-Responsemechanismus verschlüsselte Konfigurationsdatei heruntergeladen wird.

KM.3 stellt sicher, dass die privaten Zertifikate, die während der Laufzeit von VPNConnect heruntergeladen werden, passwortgeschützt sind. Die Passwörter werden durch die Konfigurationsdatei VPNConnect übergeben und sind dem Benutzer nicht bekannt.

Nach SK.1 werden die von VPNConnect verwendeten Konfigurationsdateien verschlüsselt gespeichert.

Diese drei Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FCS_CKM.3 um.

Die Sicherheitsanforderung **FCS_CKM.4** fordert, nach jedem VPN-Tunnelabbau die Zertifikate aus dem Windows-Zertifikatsspeicher und bei Beenden der Applikation physikalisch vom Datenträger zu löschen. Ebenso muss bei Verbindungsunterbrechung zu den angegebenen Produktivservern der VPN-Tunnel sofort abgebaut werden.

KM.4 stellt sicher, dass bei Tunnelabbau die privaten Zertifikate von VPNConnect aus dem Windows-Zertifikatsspeicher entfernt und bei Beendigung der Applikation physikalisch vom Datenträger gelöscht werden.

Nach AC.4 wird ein bestehender Tunnel von VPNConnect sofort abgebaut, wenn ein Zielserver nicht mehr erreichbar.

Diese beiden Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FCS_CKM.4 um.

Die Sicherheitsanforderung **FDP_ACC.2** verlangt die vollständige Zugriffskontrolle für alle Operationen zwischen dem lokalen Client und dem geschützten Netz über das Durchsetzen einer Zugriffskontrollpolitik.

Nach AC.1 kontrolliert VPNConnect den Zugriff von Benutzern auf die hinter einem VPN-Gateway befindlichen Netze.

Nach AC.2 beschränkt VPNConnect den Zugriff auf von dem Authentifizierungsserver zugewiesene Server hinter dem VPN-Gateway.

Diese beiden Sicherheitsfunktionen gemeinsam setzen die Sicherheitsanforderung FDP_ACC.2 um.

Die Sicherheitsanforderung **FDP_ACF.1** verlangt, die Zugriffskontrollpolitik auf Basis von IP-Adressbereichen und Zertifikaten durchzusetzen. Die Autorisierung muss durch einen zertifikatsbasierten Tunnel erfolgen, wobei folgende Anforderungen gestellt werden:

- Gültigkeit der benutzten Zertifikate für den Aufbau des Authentifizierungstunnels
- Import der benötigten Zertifikate möglich
- Korrespondenz zwischen lokalem Zertifikat und Zertifikaten auf dem VPN-Gateway

Nach AC.1 kontrolliert VPNConnect den Zugriff von Benutzern auf die hinter einem VPN-Gateway befindlichen Netze.

Nach AC.2 beschränkt VPNConnect den Zugriff auf von dem Authentifizierungsserver zugewiesene Server hinter dem VPN-Gateway.

Brandings vom Produkt VPNConnect können nach AC.3 aufgrund der verschlüsselten Konfigurationsdateien nur vom Hersteller oder von herstellerautorisierten Administratoren durchgeführt werden.

Durch KM.1 ist sichergestellt, dass das generische Zertifikat zum Aufbau des Authentifizierungstunnels vor jedem Verbindungsaufbau in den Benutzerzertifikatsspeicher importiert wird, und dient der sicheren Authentifizierung des Benutzers am Authentifizierungsserver.

IPS.4 legt fest, dass Benutzerdaten nur dann übermittelt werden, wenn ein Produktivtunnel unter Verwendung von Zertifikaten erfolgreich aufgebaut wurde, serverseitig eine Regel für das private Benutzerzertifikat vorhanden ist und die Verbindung zu einem Zielserver im vertrauten Netz

steht. Hiermit ist ebenfalls die Nichtabstreitbarkeit der Urheberschaft durch die Verwendung von Zertifikaten gegeben.

Diese fünf Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FDP_ACF.1 um.

Die Sicherheitsanforderung **FIA_UAU.1** fordert, dass nur der Aufruf der Konfiguration der Verbindungsart erlaubt ist bevor sich der Benutzer authentisieren muss.

Nach IA.1 muss sich ein Benutzer gegenüber VPNConnect mit seinem eindeutigen Benutzerkennzeichen identifizieren und sich über sein Passwort authentisieren VPNConnect nutzen kann. Nur wenn eine korrekte Kombination von Benutzerkennzeichen und Passwort eingegeben wurde, erhält der Benutzer Zugriff auf die ihm zugewiesenen Funktionen.

Nach IA.3 erfolgt die Authentisierung bei allen Verbindungsarten nach Aufbau des Authentifizierungstunnels.

Nach KM.1 wird das generische Zertifikat zum Aufbau des Authentifizierungstunnels vor jedem Verbindungsaufbau in den Benutzerzertifikatsspeicher importiert, und dient der sicheren Authentifizierung des Benutzers am Authentifizierungsserver.

Nach KM.2 muss der EVG bei vorhandenem Benutzerkonto am Authentifizierungsserver eine im vorher aufgebauten Authentifizierungstunnel mittels eines Challenge-Responsemechanismus verschlüsselte Konfigurationsdatei herunterladen, die der Autorisierung und Identifikation des Benutzers dient und u.a. den Ort der Benutzerzertifikate enthält, die im nächsten Schritt gesichert auf den Rechner heruntergeladen und physikalisch auf dem Datenträger gespeichert werden.

Nach SK.2 werden die vom Authentifizierungsserver zu generierenden Konfigurationsdateien mittels eines Challenge-Responsemechanismus verschlüsselt übertragen und von VPNConnect entschlüsselt.

Diese fünf Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FIA_UAU.1 um.

Die Sicherheitsanforderung **FIA_UAU.7** erfordert, dass während der Authentisierung Rückmeldungen ohne Rückgriff auf Benutzernamen und Passwort sowie Fehler bei Eingabe dieser Attribute an den Benutzer bereitgestellt werden.

Wurde nach IA.4 eine falsche Kombination von Benutzerkennzeichen und Passwort eingegeben, erhält der Benutzer einen Hinweis, dass Benutzerkennzeichen oder Passwort falsch waren. Aus dieser Fehlermeldung geht nicht hervor, ob Benutzerkennzeichen oder Passwort falsch waren.

Diese Sicherheitsfunktion setzt exakt die Anforderung um.

Die Sicherheitsanforderung **FIA_UAU.EX.1** fordert, dass nur der Aufruf der Konfiguration der Verbindungsart erlaubt ist bevor sich der Benutzer bei Interneteinwahlverbindungen online gegenüber einem RADIUS-Server authentisieren muss.

Nach IA.1 muss sich ein Benutzer gegenüber VPNConnect mit seinem eindeutigen Benutzerkennzeichen identifizieren und sich über sein Passwort authentisieren VPNConnect nutzen kann. Nur wenn eine korrekte Kombination von Benutzerkennzeichen und Passwort eingegeben wurde, erhält der Benutzer Zugriff auf die ihm zugewiesenen Funktionen.

IA.2 legt fest, dass die Authentisierung bei Interneteinwahlverbindungen online gegenüber einem RADIUS-Server erfolgt.

Diese zwei Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FIA_UAU.EX.1 um.

Die Sicherheitsanforderung **FIA_UID.1** fordert, nur den Aufruf der Konfiguration der Verbindungsart zu erlauben, bevor der Benutzer identifiziert wird.

Nach IA.1 muss sich ein Benutzer gegenüber VPNConnect mit seinem eindeutigen Benutzerkennzeichen identifizieren und sich über sein Passwort authentisieren VPNConnect nutzen kann. Nur wenn eine korrekte Kombination von Benutzerkennzeichen und Passwort eingegeben wurde, erhält der Benutzer Zugriff auf die ihm zugewiesenen Funktionen.

Nach IA.3 erfolgt die Authentisierung bei allen Verbindungsarten nach Aufbau des Authentifizierungstunnels.

Nach KM.1 wird das generische Zertifikat zum Aufbau des Authentifizierungstunnels vor jedem Verbindungsaufbau in den Benutzerzertifikatsspeicher importiert, und dient der sicheren Authentifizierung des Benutzers am Authentifizierungsserver.

Nach KM.2 muss der EVG bei vorhandenem Benutzerkonto am Authentifizierungsserver eine im vorher aufgebauten Authentifizierungstunnel mittels eines Challenge-Responsemechanismus verschlüsselte Konfigurationsdatei herunterladen, die der Autorisierung und Identifikation des Benutzers dient und u.a. den Ort der Benutzerzertifikate enthält, die im nächsten Schritt gesichert auf den Rechner heruntergeladen und physikalisch auf dem Datenträger gespeichert werden.

Nach SK.2 werden die vom Authentifizierungsserver zu generierenden Konfigurationsdateien mittels eines Challenge-Responsemechanismus verschlüsselt übertragen und von VPNConnect entschlüsselt.

Diese fünf Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FIA_UID.1 um.

Die Sicherheitsanforderung **FIA_UID.EX.1** fordert, nur den Aufruf der Konfiguration der Verbindungsart zu erlauben, bevor der Benutzer online gegenüber einem Authentifizierungsserver, bei Interneteinwahlverbindungen zuvor online gegenüber einem RADIUS-Server, identifiziert wird.

Nach IA.1 muss sich ein Benutzer gegenüber VPNConnect mit seinem eindeutigen Benutzerkennzeichen identifizieren und sich über sein Passwort authentisieren VPNConnect nutzen kann. Nur wenn eine korrekte Kombination von Benutzerkennzeichen und Passwort eingegeben wurde, erhält der Benutzer Zugriff auf die ihm zugewiesenen Funktionen.

IA.2 legt fest, dass die Identifizierung bei Interneteinwahlverbindungen online gegenüber einem RADIUS-Server erfolgt.

Diese zwei Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FIA_UID.EX.1 um.

Die Sicherheitsfunktion **FIA_SOS.2** fordert, dass die TSF einen Mechanismus bereitstellen müssen, um Geheimnisse zu generieren, die der Metrik für die Generierung von Challenges entsprechen und in der Lage sein müssen, den Gebrauch der TSF-generierten Geheimnisse für die Identifikation und Autorisierung von Benutzern durchzusetzen.

Nach SG.1 werden für die Authentifizierung am Authentifizierungsserver sog. Challenges generiert, die laufzeitgeneriert und eindeutig sind.

Nach SK.2 werden die vom Authentifizierungsserver zu generierenden Konfigurationsdateien werden mit einer Challenge verschlüsselt übertragen und von VPNConnect entschlüsselt.

KM.2 stellt sicher, dass bei vorhandenem Benutzerkonto am Authentifizierungsserver im vorher aufgebauten Authentifizierungstunnel eine mittels eines Challenge-Responsemechanismus verschlüsselte Konfigurationsdatei heruntergeladen wird.

Nach IA.3 erfolgt die Authentisierung bei allen Verbindungsarten nach Aufbau des Authentifizierungstunnels.

Diese vier Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FIA_SOS.2 um.

Die Sicherheitsanforderung **FDP_IFF.EX.1** fordert

- dynamisch IP-Sicherheitsrichtlinien anzulegen, die Verbindungen zu spezifizierten Netzen mittels z.B. IPSEC verschlüsseln
- den für die Verschlüsselung der Daten zu verwendenden Algorithmus (z.B. 3DES) und die zu verwendende Hashing-Funktion (z.B. MD5) zu setzen
- dynamisch Tunnelendpunkte zu setzen
- aufgrund erfolgter Autorisierung Zugriffsrechte auf ganze Netze oder einzelne Server zu setzen
- private Zertifikate zum Aufbau der VPN-Verbindungen zu setzen
- Zugriffe auf andere Netze als das geschützte Netz zu verweigern
- Serverseitig die Nichtabstreitbarkeit der Urheberschaft von übermittelten Daten auswerten zu können
- Benutzerdaten nur nach erfolgtem VPN-Aufbau übermitteln zu lassen, wenn ein Verbindungsaufbau zum definierten Netz hinter dem VPN-Gateway möglich ist und die Verbindung zum definierten Netz hinter dem VPN-Gateway besteht
- bei fehlgeschlagenem Verbindungsversuch zum VPN-Gateway die IP-Sicherheitsrichtlinien entfernen, was zum sofortigen Tunnelabbau führt
- die Sicherheitsrichtlinienverwaltung unabhängig vergebener Benutzerrechte lauffähig zu halten

Nach IPS.1 werden während der Laufzeit dynamisch IP-Sicherheitsrichtlinien angelegt, die es erlauben, Verbindungen zu spezifizierten Netzen mit einem geeigneten Algorithmus zu verschlüsseln. Hiermit werden ebenfalls dynamisch Tunnelendpunkte gesetzt.

IPS.2 setzt die in einer IP-Sicherheitsrichtlinie zum Aufbau einer VPN-Verbindung zu verwendende Verschlüsselungsalgorithmus und die zu verwendende Hashing-Funktion dynamisch.

Nach AC.2 beschränkt VPNConnect den Zugriff auf von dem Authentifizierungsserver zugewiesene Server hinter dem VPN-Gateway.

Nach IA.3 erfolgt die Authentisierung bei allen Verbindungsarten nach Aufbau des Authentifizierungstunnels.

Durch KM.1 ist sichergestellt, dass das generische Zertifikat zum Aufbau des Authentifizierungstunnels vor jedem Verbindungsaufbau in den Benutzerzertifikatsspeicher importiert wird, und dient der sicheren Authentifizierung des Benutzers am Authentifizierungsserver.

KM.2 stellt sicher, dass bei vorhandenem Benutzerkonto am Authentifizierungsserver im vorher aufgebauten Authentifizierungstunnel eine mittels eines Challenge-Responsemechanismus verschlüsselte Konfigurationsdatei heruntergeladen wird, die u.a. den Ort der Benutzerzertifikate enthält, die im nächsten Schritt gesichert auf den Rechner heruntergeladen werden und physikalisch auf dem Datenträger gespeichert werden. Die Zertifikate werden im Anschluss automatisch in den Windows-Zertifikatsspeicher importiert.

Nach IPS.3 wird bei der Anlage von IP-Sicherheitsrichtlinien ein Zugriff auf andere Netze als das vertraute Netz blockiert.

IPS.4 legt fest, dass Benutzerdaten nur dann übermittelt werden, wenn ein Produktivtunnel unter Verwendung von Zertifikaten erfolgreich aufgebaut wurde, serverseitig eine Regel für das private Benutzerzertifikat vorhanden ist und die Verbindung zu einem Zielserver im vertrauten Netz steht. Hiermit ist ebenfalls die Nichtabstreitbarkeit der Urheberschaft durch die Verwendung von Zertifikaten gegeben.

Nach AC.1 kontrolliert VPNConnect den Zugriff von Benutzern auf die hinter einem VPN-Gateway befindlichen Netze.

Nach AC.4 wird ein bestehender Tunnel von VPNConnect sofort abgebaut, wenn ein Zielserver nicht mehr erreichbar.

KM.3 stellt sicher, dass die privaten Zertifikate, die während der Laufzeit von VPNConnect heruntergeladen werden, passwortgeschützt sind. Die Passwörter werden durch die Konfigurationsdatei VPNConnect übergeben und sind dem Benutzer nicht bekannt.

KM.4 stellt sicher, dass bei Tunnelabbau die privaten Zertifikate von VPNConnect aus dem Windows-Zertifikatsspeicher entfernt und bei Beendigung der Applikation physikalisch vom Datenträger gelöscht werden.

Nach IPS.5 ist die IP-Sicherheitsrichtlinienverwaltung unabhängig von der Windows-eigenen Benutzerverwaltung in der Lage, IP-Sicherheitsrichtlinien zu erstellen, zu ändern, zu aktivieren, zu deaktivieren und zu löschen.

Diese 13 Sicherheitsfunktionen setzen in Ihrer Gesamtheit die Anforderung FDP_IFF.EX.1 um.

Die Sicherheitsanforderung **FMT_MSA.1** fordert, sichere Standardvorgaben nur durch Administratoren mit Herstellerautorisierung durchführen zu lassen.

Nach AC.3 können Brandings vom Produkt VPNConnect aufgrund der verschlüsselten Konfigurationsdateien nur vom Hersteller oder von herstellerautorisierten Administratoren durchgeführt werden.

Diese Sicherheitsfunktion setzt exakt die Anforderung um.

Die Sicherheitsanforderung **FMT_MSA.3** fordert, Zugriffskontrollpolitiken zur Bereitstellung von vorgegebenen Standardwerten mit einschränkenden Eigenschaften durchzusetzen und alternative Standardwerte nur Administratoren mit Herstellerautorisierung zu gestatten.

Nach IA.1 muss sich ein Benutzer gegenüber VPNConnect mit seinem eindeutigen Benutzerkennzeichen identifizieren und sich über sein Passwort authentisieren VPNConnect nutzen kann. Nur wenn eine korrekte Kombination von Benutzerkennzeichen und Passwort eingegeben wurde, erhält der Benutzer Zugriff auf die ihm zugewiesenen Funktionen.

Nach KM.1 wird das generische Zertifikat zum Aufbau des Authentifizierungstunnels vor jedem Verbindungsaufbau in den Benutzerzertifikatsspeicher importiert, und dient der sicheren Authentifizierung des Benutzers am Authentifizierungsserver.

Nach AC.3 können Brandings vom Produkt VPNConnect aufgrund der verschlüsselten Konfigurationsdateien nur vom Hersteller oder von herstellerautorisierten Administratoren durchgeführt werden.

Nach SK.1 werden die von VPNConnect verwendeten Konfigurationsdateien verschlüsselt gespeichert.

Diese vier Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FMT_MSA.3 um.

Die Sicherheitsanforderung **FMT_SMF.1** fordert, dass die folgenden Sicherheitsmanagement-funktionen umgesetzt werden müssen:

- alternative Anfangswerte, die die vorgegebenen Standardwerte ersetzen, dürfen nur von Administratoren mit Herstellerautorisierung gesetzt werden.

- die Installation des TSF darf nur von Administratoren des Betriebssystems durchgeführt werden.

Nach AC.3 können Brandings vom Produkt VPNConnect aufgrund der verschlüsselten Konfigurationsdateien nur vom Hersteller oder von herstellerautorisierten Administratoren durchgeführt werden.

Nach IA.5 kann die Installation von VPNConnect nur durch Administratoren des Betriebssystems erfolgen.

Diese zwei Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FMT_SMF.1 um.

Die Sicherheitsanforderung **FMT_SMR.1** fordert, dass die TSF müssen die Rollen Benutzer, Betriebssystemadministratoren oder Administratoren mit Herstellerautorisierung erhalten und die Benutzer mit Rollen verknüpfen können.

Nach AC.3 können Brandings vom Produkt VPNConnect aufgrund der verschlüsselten Konfigurationsdateien nur vom Hersteller oder von herstellerautorisierten Administratoren durchgeführt werden.

Nach IA.1 muss sich ein Benutzer gegenüber VPNConnect mit seinem eindeutigen Benutzerkennzeichen identifizieren und sich über sein Passwort authentisieren VPNConnect nutzen kann. Nur wenn eine korrekte Kombination von Benutzerkennzeichen und Passwort eingegeben wurde, erhält der Benutzer Zugriff auf die ihm zugewiesenen Funktionen.

Nach IA.3 erfolgt die Authentisierung bei allen Verbindungsarten nach Aufbau des Authentifizierungstunnels.

Nach IA.5 kann die Installation von VPNConnect nur durch Administratoren des Betriebssystems erfolgen.

Diese vier Sicherheitsfunktionen setzen in ihrer Gesamtheit die Sicherheitsanforderung FMT_SMR.1 um.

Die Sicherheitsanforderung **FPT_ITT.EX.1** fordert, die Konfigurationsdateien zu verschlüsseln.

Nach SK.1 werden die von VPNConnect verwendeten Konfigurationsdateien verschlüsselt gespeichert.

Diese Sicherheitsfunktion setzt exakt die Anforderung um.

8.3.2 Erklärung der EVG-Sicherheitsmaßnahmen

Die Tabelle in Kapitel 6.2 zeigt auf, dass alle Anforderungen an die Vertrauenswürdigkeit durch geeignete Sicherheitsmaßnahmen abgedeckt sind.

8.4 Erklärung der PP-Postulate

Die Sicherheitsvorgaben postulieren keine Konformanz zu einem Schutzprofil (PP).

Anhang A - Einführung in VPN

Das Internet ist grundsätzlich ein offenes, ungeschütztes Netz. Es besteht keine Gewissheit, dass übertragene Informationen nicht abgehört oder gar manipuliert werden. Um für sicherheitsrelevante Datenübertragungen trotzdem die Vorteile (u.a. Verfügbarkeit, günstige Kosten, Geschwindigkeit) des Internet nutzen zu können gibt es unterschiedliche Ansätze.

Durch den Einsatz eines VPN wird über das Internet ein sicherer Kommunikationskanal, auch „Tunnel“ genannt, aufgebaut. Die Informationen sind durch Überwachung Chiffrierung der Daten abhörsicher und vor Manipulation geschützt.

Mit VPN werden Datenpakete eines beliebigen Protokolls verschlüsselt und verpackt übers Internet gesandt. Das Internetprotokoll TCP/IP dient als Transportmittel.

Eine VPN-Verbindung ermöglicht es, öffentliche Leitungen als Teil eines privaten Leitungsnetzes zu benutzen. Um dies zu ermöglichen, stellt das VPN dem Benutzer eine spezielle Internet-Verbindung zur Verfügung, Die über diese Verbindung übertragenen Datenpakete werden verschlüsselt und in ein Datenpaket eingepackt, das er über das öffentliche Netz an ein VPN-Gateway verschickt. Das VPN-Gateway entschlüsselt das Originalpaket und gibt es an das Zielsystem im geschützten Netz weiter.

Ein Digitales Zertifikat bestätigt die Echtheit (= Zuordnung Server zu Public Key) eines Servers. Ein digitales Zertifikat beinhaltet einen Public Key, Informationen über die Identität der Person oder der Firma, die das Zertifikat besitzt, Informationen über die Ausgabestelle und diverse Verwaltungsinformationen.

Die Public – Key - Verschlüsselung ist ein asymmetrisches Verschlüsselungsverfahren, bei dem sowohl der Sender als auch der Empfänger zwei Schlüssel einsetzen: einen öffentlichen zur Verschlüsselung, Public Key genannt, und einen geheimen, den Private Key, zur Entschlüsselung der Daten.

VPN ermöglicht es also, über das Internet Daten in einem Tunnel (= von äußeren Zugriffen geschützter Bereich) über das Internet geschützt zu übertragen und stellt somit eine kostengünstige Alternative zu (geschützten) Standleitungen (Leased Lines) dar.

Anhang B - Literaturverzeichnis

[3DES_1] RFC 3217, Triple-DES and RC2 Key Wrapping R. Housley, RSA Laboratories, December 2001

[AH_1] RFC 2402, IP Authentication Header , S. Kent, BBN Corp, R. Atkinson, November 1998

[CC_P1] Common Criteria, Teil 1: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik – Teil 1: Einführung und allgemeines Modell, Version 2.1, August 1999

[CC_P2] Common Criteria, Teil 2: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik – Teil 2: Funktionale Sicherheitsanforderungen, Version 2.1, August 1999

[CC_P3] Common Criteria, Teil 3: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik – Teil 3: Anforderungen an die Vertrauenswürdigkeit, Version 2.1, August 1999.

[CHAP_1] RFC 1994, PPP Challenge Handshake Authentication Protocol (CHAP), W. Simpson, DayDreamer, August 1996

[DES_1] RFC 2419, The PPP DES Encryption Protocol, Version 2 (DESE-bis), K. Sklower, University of California, G. Meyer, Shiva, September 1998

[ICMP_1] RFC 792, INTERNET CONTROL MESSAGE PROTOCOL, J. Postel, Information Sciences Institute, September 1981

[IKE_1] RFC 2409, The Internet Key Exchange (IKE), D. Harkins, D. Carrel, Cisco Systems, November 1998

[IP_1] RFC 760, INTERNET PROTOCOL, Information Sciences Institute, University of Southern California, Marina del Rey, January 1980

[IPSEC_1] RFC 2406, IP Encapsulating Security Payload (ESP), S. Kent, BBN Corporation, November 1998

[IPSEC_2] RFC 2709, Security Model with Tunnel-mode IPSEC for NAT Domains, P. Srisuresh, Lucent Technologies, October 1999

[IPSEC_3] RFC 3457, Requirements for IPSEC Remote Access Scenarios, S. Kelly, Airespace, S. Ramamoorthi, Juniper Networks, January 2003

[IPSEC_4] RFC 3585, IPSEC Configuration Policy Information Model, J. Jason, Intel Corporation, L. Rafalow, IBM, E. Vyncke, Cisco Systems, August 2003

[IPSEC_5] RFC 3715, IPSEC-Network Address Translation (NAT) Compatibility Requirements, B. Aboba, Microsoft, March 2004

[IPSEC_6] RFC 2401, Security Architecture for the Internet Protocol, S. Kent, BBN Corp, R. Atkinson, November 1998

[ISAKMP_1] RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP), D. Maughan, M. Schertler, Securify Inc., M. Schneider, National Security Agency, J. Turner, RABA Technologies, Inc., November 1998

[L2TP_1] RFC 2661, Layer Two Tunneling Protocol "L2TP", W. Townsley, A. Valencia, Cisco Systems, A. Rubens, Ascend Communications, G. Pall, G. Zorn, Microsoft Corporation, B. Palter, Redback Networks, August 1999

[L2TP_2] RFC 3193, Securing L2TP using IPSEC, B. Patel, Intel, B. Aboba, W. Dixon, Microsoft, G. Zorn, S. Booth, Cisco Systems, November 2001

[MD5_1] RFC 2403, The Use of HMAC-MD5-96 within ESP and AH , C. Madson, Cisco Systems Inc., R. Glenn, NIST, November 1998

[NAT_1] RFC 2663, IP Network Address Translator (NAT) Terminology and Considerations, P. Srisuresh, M. Holdrege, Lucent Technologies, August 1999

[NAT_2] RFC 2766, Network Address Translation - Protocol Translation (NAT-PT), G. Tsirtsis, BT, P. Srisuresh, Campio Communications, February 2000

[RADIUS_1] RFC 2865, Remote Authentication Dial In User Service (RADIUS), C. Rigney, S. Willens, Livingston, A. Rubens, Merit, W. Simpson, Daydreamer, June 2000

[SNMP_1] RFC 1157, Simple Network Management Protocol (SNMP), J. Case SNMP Research, M. Fedor, M. Schoffstall, Performance Systems International, J. Davin, MIT Laboratory for Computer Science, May 1990

[TCP_1] RFC 793, TRANSMISSION CONTROL PROTOCOL, Information Sciences Institute, University of Southern California, Marina del Rey, September 1981

[X.509_1] RFC 2510, Internet X.509 Public Key Infrastructure, Certificate Management Protocols, C. Adams, Entrust Technologies, S. Farrell, SSE, March 1999

Anhang C - Tabellenverzeichnis