# Zertifizierungsreport

**Bundesamt für Sicherheit in der Informationstechnik**

## BSI-DSZ-CC-0288-2006

zu

## VPNConnect
## Version 1.2.650

der

## I-MOTION GmbH

BSI- Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon (0228) 9582-0, Telefax (0228) 9582-455, Infoline (0228) 9582-111

# Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-0288-2006**

## VPNConnect Version 1.2.650

der

## I-MOTION GmbH

Common Criteria Arrangement

Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle nach den *Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1 (ISO/IEC 15408:1999),* unter Nutzung der *Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Teil 1 Version 0.6, Teil 2 Version 1.0*, ergänzt um Final Interpretations in Übereinstimmung mit Common Criteria Version 2.2 und Common Methodology Part 2, Version 2.2 evaluiert.

**Prüfergebnis:**

| | |
|---|---|
| Funktionalität: | **Produktspezifische Sicherheitsvorgaben**<br>**Common Criteria Teil 2 erweitert** |
| Vertrauenswürdigkeit: | **Common Criteria Teil 3 konform**<br>**EAL 2** |

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport.

Die Evaluation wurde in Übereinstimmung mit den Bestimmungen des Zertifizierungsschemas des Bundesamtes für Sicherheit in der Informationstechnik durchgeführt. Die im Evaluationsbericht enthaltenen Schlußfolgerungen der Prüfstelle sind in Einklang mit den erbrachten Nachweisen.

Die auf der Rückseite aufgeführten Anmerkungen sind Bestandteil dieses Zertifikates.

Bonn, den 21. März 2006

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht L.S.

**Bundesamt für Sicherheit in der Informationstechnik**
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

# Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik, Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers - im folgenden Antragsteller genannt - durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produktes gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produktes, die Einzelheiten der Bewertung und Hinweise für den Anwender.

[1] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

# Gliederung

# A Zertifizierung

## 1 Grundlagen des Zertifizierungsverfahrens

Die Zertifizierungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- BSIG[2]
- BSI-Zertifizierungsverordnung[3]
- BSI-Kostenverordnung[4]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN 45011
- BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1[5]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM)
  - Teil 1, Version 0.6
  - Teil 2, Version 1.0
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)

Die Verwendung der CC Version 2.1, der CEM Teil 2 Version 1 und der Final Interpretations als Teil der AIS 32 ergibt eine Übereinstimmung des Zertifizierungsergebnisses mit CC Version 2.2 und CEM Version 2.2 wie durch die Gremien im CC Anerkennungsabkommen festgelegt.

---

[2] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

[3] Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung-BSIZertV) vom 7.Juli 1992, Bundesgesetzblatt I S. 1230

[4] Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

[5] Bekanntmachung des Bundesministeriums des Innern vom 22. September 2000 im Bundesanzeiger S. 19445

# 2 Anerkennungsvereinbarungen

Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von IT-Sicherheitszertifikaten - sofern sie auf ITSEC oder Common Criteria (CC) beruhen - unter gewissen Bedingungen vereinbart. Zertifikate der Unterzeichnerstaaten werden damit in den jeweils anderen Unterzeichnerstaaten anerkannt.

## 2.1 ITSEC/CC - Zertifikate

Das SOGIS-Abkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten, auf Grundlage der ITSEC, ist am 03. März 1998 in Kraft getreten. Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Evaluationsstufe EAL7 erweitert.

## 2.2 CC - Zertifikate

Im Mai 2000 wurde eine Vereinbarung (Common Criteria-Vereinbarung) über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und Schutzprofilen auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 zwischen den nationalen Stellen in Australien, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Kanada, Neuseeland, Niederlande, Norwegen, Spanien und den USA unterzeichnet. Im November 2000 ist Israel der Vereinbarung beigetreten, Schweden im Februar 2002, Österreich im November 2002, Ungarn und Türkei im September 2003, Japan im November 2003, die Tschechische Republik im September 2004, die Republik Singapore im März 2005, Indien im April 2005.

# 3 Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Produkt VPNConnect Version 1.2.650 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts VPNConnect Version 1.2.650 wurde von der Tele-Consulting GmbH durchgeführt. Das Prüflabor Tele-Consulting GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Antragsteller und Vertreiber ist:

I-MOTION GmbH
Am Nordring 23
90765 Fürth

Entwickler ist:

AccSys GmbH
Lichtenbergstraße 8
85748 Garching

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 21. März 2006 vom BSI abgeschlossen.

Das bestätigte Vertrauenswürdigkeitspaket gilt nur unter der Voraussetzung, daß

- alle Auflagen bzgl. Generierung, Konfiguration und Betrieb, soweit sie im nachfolgenden Bericht angegeben sind, beachtet werden,
- das Produkt in der beschriebenen Umgebung - sofern im nachfolgenden Bericht angegeben - betrieben wird.

Dieser Zertifizierungssreport gilt nur für die hier angegebene Version des Produktes. Die Gültigkeit kann auf neue Versionen und Releases des Produktes ausgedehnt werden, sofern der Antragsteller eine Re-Zertifizierung des geänderten Produktes entsprechend den Vorgaben beantragt und die Prüfung keine sicherheitstechnischen Mängel ergibt.

Hinsichtlich der Bedeutung der Vertrauenswürdigkeitsstufen und der bestätigten Stärke der Funktionen vgl. die Auszüge aus den technischen Regelwerken am Ende des Zertifizierungsreports.

[6] Information Technology Security Evaluation Facility

# 4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-22.

Das Produkt VPNConnect Version 1.2.650 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller[7] des Produktes angefordert werden. Unter der o.g. Internetadresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

[7] I-MOTION GmbH
Am Nordring 23
90765 Fürth

# B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

# Gliederung des Zertifizierungsberichtes

# 1 Zusammenfassung

Der EVG, VPNConnect Version 1.2.650, ist eine Zugangssoftware für das Betriebssystem Microsoft Windows (Windows 2000 oder 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.

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

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

Bei der Umsetzung der einzelnen Funktionen bedient sich VPNConnect Standardroutinen des Betriebssystems (in den Bereichen „Kryptographisches Schlüsselmanagement“ und „IP-Sicherheitsrichtlinienverwaltung“, siehe ST [6], Kapitel 6.1).

Die Evaluation des Produkts VPNConnect Version 1.2.650 wurde von der Tele-Consulting GmbH durchgeführt und am 17. Februar 2006 abgeschlossen. Das Prüflabor Tele-Consulting GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[8].

Antragsteller und Vertreiber ist:

I-MOTION GmbH
Am Nordring 23
90765 Fürth

Entwickler ist:

AccSys GmbH
Lichtenbergstraße 8
85748 Garching

## 1.1 Vertrauenswürdigkeitspaket

Die Vertrauenswürdigkeitskomponenten des EVG sind konform zum Teil 3 der CC [1]. Der EVG wurde erfolgreich mit der Prüfstufe EAL2 (strukturell getestet) evaluiert (siehe auch Annex C oder [1], Teil 3). In Kapitel 9, Tabelle 6 dieses Reports sind die gewählten Vertrauenswürdigkeitskomponenten mit dem Evaluierungsergebnis detailliert aufgeführt.

[8] Information Technology Security Evaluation Facility

## 1.2 Funktionalität

Die in den Sicherheitsvorgaben ausgewählten funktionalen Sicherheitsanforderungen (SFR – Security Functional Requirements) sind CC [1],Teil 2 erweitert. Die Auflistung in der folgenden Tabelle zeigt die zu Teil 2 der CC konformen SFRs:

| Funktionale Sicherheitsanforderungen | Bedeutung |
|---|---|
| **FCS** | **Kryptographisches Unterstützung** |
| FCS_CKM.2 | Verteilung des kryptographischen Schlüssels |
| FCS_CKM.3 | Zugriff auf einen kryptographischen Schlüssel |
| FCS_CKM.4 | Zerstörung des kryptographischen Schlüssels |
| **FDP** | **Schutz der Benutzerdaten** |
| FDP_ACC.2 | Vollständige Zugriffskontrolle |
| FDP_ACF.1 | Zugriffskontrolle basierend auf Sicherheitsattributen |
| **FIA** | **Identifikation und Authentisierung** |
| FIA_UAU.1 | Zeitpunkt der Authentisierung |
| FIA_UAU.7 | Geschützte Authentisierungsrückmeldung |
| FIA_UID.1 | Zeitpunkt der Identifikation |
| FIA_SOS.2 | Generierung von Geheimnissen durch TSF |
| **FMT** | **Sicherheitsmanagement** |
| FMT_MSA.1 | Management der Sicherheitsattribute |
| FMT_MSA.3 | Initialisierung statischer Attribute |
| FMT_SMF.1 | Spezifikation der Managementfunktionen |
| FMT_SMR.1 | Sicherheitsrollen |

Tabelle 1: SFRs des EVG CC, Teil 2 konform

Die Auflistung in Tabelle 2 zeigt die explizit dargelegten (Teil 3 erweiterten) SFRs:

| Funktionale Sicherheitsanforderungen | Bedeutung |
|---|---|
| **FIA** | **Identifikation und Authentisierung** |
| FIA_UAU.EX.1 | Externe Authentisierung der Benutzer bei Start des EVG |
| FIA_UID.EX.1 | Externe Identifikation der Benutzer bei Start des EVG |
| **FPT** | **Schutz der TSF** |
| FPT_ITT.EX.1 | Schutz von Konfigurationsdateien |

Tabelle 2: SFRs des EVG CC, Teil 2 erweitert

Hinweis: Es werden nur die Titel der SFRs genannt. Detailiertere Informationen befinden sich in Kapitel 5.1.1 der Sicherheitsvorgaben [6].

Die funktionalen Sicherheitsanforderungen werden durch folgende Sicherheitsfunktionen umgesetzt:

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.

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

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

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.

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

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.

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.

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

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

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.

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 und physikalisch auf dem Datenträger gespeichert werden. Die Zertifikate werden automatisch in den Windows-Zertifikatsspeicher importiert.

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.

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.

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.

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.

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.

Spezifikation der Geheimnisse

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

## 1.3 Stärke der Funktionen

Es wird keine Stärke der Funktionen in Kap. 6.3 der Sicherheitsvorgaben [6], angegeben, da die Sicherheitsfunktionen, die auf Wahrscheinlichkeits- oder Permutations-mechanismen beruhen auch kryptographische Algorithmen nutzen.

## 1.4 Zusammenfassung der Bedrohungen und der organisatorischen Sicherheitspolitik, auf die das evaluierte Produkt ausgerichtet ist

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

Schutzwürdige Objekte sind Datenpakete, die über den EVG gesendet oder empfangen werden, Zertifikate und Konfigurationsdaten, die den sicheren Betrieb des EVG ermöglichen.

Subjekte im Sinne der CC sind autorisierte Personen, die den EVG nutzen, um eine VPN Verbindung aufzubauen, vertrauenswürdige Administratoren des Betriebssystems, die den EVG installieren und nicht-sicherheitsrelevante Parameter konfigurieren, sowie vertrauenswürdige Administratoren mit Herstellerautorisierung, die den EVG und sicherheitsrelevante Parameter vorkonfigurieren.

Urheber von Bedrohungen sind 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 sowie 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.

Aufgrund der obigen Definitionen wurden folgende Bedrohungen identifiziert, denen der EVG entgegenwirken muss:

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.

Desweiteren wurden folgende weitere Bedrohungen identifiziert, denen der EVG und die Umgebung entgegenwirken muss:

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.

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.

## 1.5 Spezielle Konfigurationsanforderungen

Der EVG wird lediglich in einer vor der Auslieferung festgelegten Konfiguration betrieben. Die sicherheitsrelevanten Einstellungen des EVG werden vom Hersteller vorkonfiguriert. Der Benutzer des EVG kann dann lediglich noch Art des Internetzugangs einstellen.

## 1.6 Annahmen über die Einsatzumgebung

Für den EVG werden folgende Annahmen an die Einsatzumgebung gestellt:

| Annahme | Inhalt |
|---|---|
| A.RADIUS | Radius-Server zur Interneteinwahl |
| A.VISP | VISP-Struktur für DSL-Einwahlverbindung |
| A.VPNGATE | Anforderungen an VPN-Gateways |
| A.AUTH | Verwendung eines Authentisierungsservers |
| A.CREATECERT | X.509-Zertifikate für Benutzer von VPNConnect |
| A.ACCESSCERT | Zugriff auf erstellte Benutzer-Zertifikate |
| A.CREATEGENCERT | Generisches Zertifikat für den Aufbau des Authentifizierungstunnels |
| A.TRUSTEDADMIN | Vertrauenswürdiger Administrator |
| A.TRUSTEDUSER | Vertrauenswürdige berechtigte Benutzer |
| A.LOCKEDCOMPUTER | Geschützte Umgebung des Computers |

Tabelle 3: Annahmen an die Einsatzumgebung

Hinweis: An dieser Stelle werden nur die Titel der Annahmen genannt. Detailliertere Informationen befinden sich in Kapitel 4 dieses Reports und in Kapitel 3.1 der Sicherheitsvorgaben [6].

## 1.7 Gewährleistungsausschluß

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

# 2 Identifikation des EVG

Der EVG heißt:

**VPNConnect, Version 1.2.650**

Die folgende Tabelle beschreibt den Auslieferungsumfang:

| Nr. | Typ | Bezeichnung | Auslieferungsmedium |
|---|---|---|---|
| 1 | Software | VPNConnect Version 1.2.650 | CD |
| 2 | Dokument | Handbuch für Systemverwalter und Benutzer Version 1.5, 10.02.2006 | pdf-File auf CD |
| 3 | Dokument | Benutzerhandbuch Version 1.2, 19.12.2005 | pdf-File auf CD |

Tabelle 4: Auslieferungsumfang des EVG

Der EVG wird vom Hersteller auf eine CD (CD-R) gebrannt und auf dem Postweg an den Kunden versendet. Die sicherheitsrelevanten Daten sind in einer verschlüsselten Konfigurationsdatei auf der CD gespeichert, die nur von herstellerautorisierten Administratoren geändert werden kann. Die Zugangsdaten werden getrennt an den Endkunden versendet.

Diese Verfahren sichern die Integrität des EVG und die Vertraulichkeit und Integrität der Konfigurationsdateien, so dass nur der berechtigte Kunde Zugriff auf den EVG bekommt.

Der Anwender hat folgende Möglichkeiten den EVG zu identifizieren:
Der Hersteller stellt den EVG auf einer CD bereit, die auf dem Label in großer Schrift u.a. die Angabe „VPNConnect Version 1.2.650“ enthält (nähere Erläuterungen zum CD-Label siehe Kapitel 10 dieses Reports).
Nach der Installation besteht zusätzlich die Möglichkeit über „Einstellung – Info“, die auf dem Label der CD angegebenen Informationen abzufragen.

# 3 Sicherheitspolitik

Bei VPNConnect handelt sich um eine Anwendung, die auf Basis der Betriebssysteme Microsoft Windows 2000 und Windows XP betrieben werden kann.
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 Betriebssystem zur Verfügung gestellten Zertifikatsspeicher benutzt.
Das gesamte Management der IP-Sicherheitsrichtlinien und das Zertifikatsmanagement werden von VPNConnect übernommen.

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

# 4 Annahmen und Klärung des Einsatzbereiches

## 4.1 Annahmen über den Einsatz

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.TRUSTEDADMIN).

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.TRUSTEDUSER).

## 4.2 Angenommene Einsatzumgebung beim Anwender

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 (A.LOCKEDCOMPUTER).

## 4.3 Angenommene Einsatzumgebung beim Hersteller

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.RADIUS).

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.VISP).

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

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 (A.AUTH).

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.CREATECERT).

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.ACCESSCERT).

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 (A.CREATEGENCERT).

# 5 Informationen zur Architektur

VPNConnect wird in Form einer Sammlung von Dateien auf CD-ROM ausgeliefert. Durch einen Installationsvorgang entsteht VPNConnect als betriebsbereite Anwendung auf einer Festplatte in Gestalt einer Sammlung von Dateien in einem bestimmten Verzeichnis.

Die Dateien sind unterteilt in:

- Programmdateien und
- Konfigurationsdateien

Die Programmdateien werden im laufenden Betrieb nicht modifiziert.

In der nachfolgenden Tabelle sind alle Teilsysteme mit Ihrem Namen und ihrem Zweck aufgeführt.

| Name | Zweck |
|---|---|
| acccard.dll | Komponente zur Erkennung von Netzwerkkarten |
| acccmd.ocx | Komponente zur Darstellung von vollgraphischen Buttons |
| acccrypt.dll | Komponente zur Verschlüsselung und Entschlüsselung (Blowfish-Klasse) |
| accdial.dll | Komponente zur Unterstützung von AutoDial-Aufrufen für Einwahlverbindungen |
| accdl.dll | Komponente zum Download über http |
| accipc.ocx | ActiveX-Control zum programmatisches Aufbau von VPN-Verbindungen |
| accipsec.dll | Komponente zur für IP-Sicherheitsrichtlinienverwaltung |
| accmenu.dll | Komponente zur Darstellung von kontextsensitiven Menüs |
| accmsg.dll | Komponente zur Darstellung von PopUp-Benachrichtigungsfenstern |
| accras.dll | Klasse zum Anlegen, Modifizieren und Löschen von Einwahlverbindungen, VPN-Verbindungen und IP-Sicherheitsrichtlinien |
| accupd.exe | Komponente zum Update von Konfigurationsdateien |
| cdstart.exe | CD-Startapplikation |
| dialer.exe | Hauptapplikation mit Userinterface.<br>Diese Applikation dient dem Userinterface und der Ansteuerung der Unterprogramme aus dem Userinterface sowie der Rückgabe von Meldungen aufgrund von Callbacks der Unterprogramme. |
| adduser.exe | Applikation zum Anlegen eines Benutzers |
| distart.exe | Applikation zum Start der Hauptapplikation |
| helper.exe | Applikation zum Überprüfen einer bereits laufenden Instanz |
| remover.exe | Applikation zum Löschen des Installationsverzeichnisses |
| unzip32.dll | Komponente zum Entpacken von ZIP-Archiven |
| zip32.dll | Komponente zum Packen von ZIP-Archiven |

Tabelle 5: Subsysteme des EVG

# 6 Dokumentation

Mit dem EVG wird folgende Dokumentation ausgeliefert:

- Handbuch für Systemverwalter und Benutzer, Version 1.5, 10.02.2006 [9]
- Benutzerhandbuch, Version 1.2, 19.12.2005 [10]

Diese Dokumentation enthält alle notwendigen Hinweise zur korrekten Installation und Bedienung des EVG.

Zusätzlich gehört zum EVG noch ein „Handbuch für herstellerautorisierte Administratoren, Version 1.4, 16.12.2005“ [8], dass jedoch nicht mit ausgeliefert wird, da in diesem Dokument lediglich Informationen beschrieben sind, die den Herstellungsprozess des EVGs betreffen und somit nur für den Hersteller und nicht für den Anwender relevant sind.

# 7 Testverfahren

## 7.1 Zusammenfassung der Herstellertests

Der Entwickler hat auf Basis einer von ihm erarbeiteten Testsuite getestet. Jeder dieser Tests ist sowohl für Windows 2000 als auch für Windows XP durchzuführen. Die überwiegende Anzahl dieser Tests kann durch unterschiedliche Wahl des Netzzugangs (Modem, ISDN, DSL, LAN) zum Internet bzw. zum Produktivnetz der I-MOTION GmbH variiert werden. Damit werden alle Konfigurationen abgedeckt, die in den Sicherheitsvorgaben angegeben sind.

Die Sicherheitsfunktionen wurden entsprechend ihrer Beschreibung auf Ebene der Funktionalen Spezifikation (bzw. der darin aufgeführten funktionalen Elemente) getestet.

Es wurden Installationstests und Tests zu den Sicherheitsfunktionen "Identifikation und Authentisierung", "Zugriffskontrolle", "Kryptographisches Schlüsselmanagement", "Schutz von Konfigurationsdateien" und " IP-Sicherheitsrichtlinienverwaltung" durchgeführt.

Die Testdokumentation des Entwicklers zeigt auf, dass alle Tests das erwartete Ergebnis ergaben.

## 7.2 Zusammenfassung der unabhängigen Prüfstellentests

Der Evaluator hatte sich entschlossen, die gesamte Testsuite des Entwicklers zu wiederholen und dabei beide relevanten Betriebssysteme (Windows 2000, Windows XP) einzubeziehen.

Darüber hinaus hat der Evaluator die Entwicklertests durch neue eigene Tests ergänzt, um eine vollständige Testabdeckung der Sicherheitsfunktionen zu gewährleisten.

Neben der Ergänzung der Entwicklertests hat der Evaluator auch Herstellertests abgewandelt und verfeinert, um deren Aussagekraft zu verbessern.

Für die Tests der Prüfstelle wurde die IT-Infrastruktur und die Kommunikationsinfrastruktur des Entwicklers AccSys GmbH in Garching genutzt. Diese Testumgebung wurde auch für die Tests des Entwicklers benutzt.

Die Betriebssysteme der beiden vom Hersteller für die Tests der Prüfstelle bereitgestellten Testsysteme (Windows 2000, Windows XP) waren vom Entwickler für die Tests neu installiert und lediglich an die Netzwerkumgebung der AccSys GmbH angepasst worden.

Der EVG wurde von den Evaluatoren auf beiden Testsystemen selbst installiert. Die im Zuge der Installation erzeugten Konfigurationsdateien wurden - soweit nötig - vom Entwickler entschlüsselt und von den Evaluatoren auf Plausibilität überprüft.

Die Tests wurden von den Evaluatoren selbständig durchgeführt. Entwicklerpersonal stand für Fragen und Diskussionen sowie zur technischen Unterstützung bei der Nutzung der Kommunikationsinfrastruktur, für die Abstimmung mit der I-MOTION GmbH, dem Betreiber des genutzten Produktivnetzes und für sonstige Aktivitäten (z.B. Entschlüsselung von Konfigurationsdateien) durchgehend zur Verfügung.

In die Test wurden auch Tests einbezogen, die den Charakter von Penetrationstests haben.

Entsprechend dem Charakter des EVG wurden alle Tests ausschließlich ohne Verwendung besonderer Test- und Analysetools des Evaluators durchgeführt, weil die von den Betriebssystemen bereitgestellten Hilfsmittel (insbesondere die Microsoft Management Console, MMC) sich als geeignetes Werkzeug erwiesen, um die den Tests zugeordneten Abläufe zu analysieren. Einschränkend muss angeführt werden, dass für die Nutzung von MMC Administratorberechtigungen erforderlich sind.

Der Evaluator hat ausführlich von der Möglichkeit Gebrauch gemacht, die bei jedem Start des EVG von diesem - primär für Diagnosezwecke - geschriebenen Traces auszuwerten und das Ergebnis dieser Auswertung in die Plausibilitätsprüfung und die Schwachstellenanalyse einfließen zu lassen.

Die Tests des Evaluators wurden am 15.12.2005 ausschließlich unter Windows 2000 durchgeführt, wobei eine ISDN-Einwahlverbindung genutzt wurde. Am 16.12.2005 erfolgte eine Erweiterung auf Windows XP. Hierbei wurde in der Regel eine DSL-Verbindung genutzt, im Einzelfall für beide Plattformen auch eine LAN-Verbindung, um die ansonsten verpflichtende Radius-Authentisierung zu vermeiden.

## 7.3 Penetrationstests der Prüfstelle

Der Evaluator hat bereits in frühen Phasen der Evaluierung darauf hin gearbeitet, Schwachstellen zu identifizieren und eliminieren zu lassen.

Darüber hinaus hat der Evaluator seine eigene Suche nach Schwachstellen auch bei der Vorbereitung und Durchführung seiner unabhängigen Tests fortgeführt und hat diese zum Gegenstand von Penetrationstests gemacht. Die Schwachstellenanalyse beinhaltete gemäß EAL 2 und AVA_VLA.1 die Suche nach offensichtlichen Schwachstellen.

Die für die Tests genutzte Konfiguration und die benutzten Hilfsmittel entsprechen dabei denjenigen, die auch ein Nutzer des EVG zur Verfügung hat (insbesondere Microsoft Management Console, Editor). Besonderes Augenmerk hat der Evaluator auf die Auswertung der Trace-Informationen gelegt, die bei der Ausführung des EVG automatisch erzeugt werden.

Die Penetrationstests des Evaluators haben gezeigt, dass nach Behandlung der während der unabhängigen Tests des Evaluators gefundenen Defizite des EVG durch den Entwickler keine in der angenommenen Einsatzumgebung des EVG offensichtlichen ausnutzbaren Schwachstellen (AVA_VLA.1) mehr bestehen.

## 7.4 Testkonfiguration

Workstation 1:

- Prozessor: 350 MHz Intel Pentium II Workstation
- OS-Version: Windows 2000 Service Pack 4
- Netzadapter: Realtek RTL 8139/810X 100 Mb/s Ethernet
- Memory: 128 MB
- Monitor: 17 Zoll SVGA Display

Workstation 2:

- Prozessor: 1,4 GHz AMD Thunderbird Workstation
- OS-Version: Windows XP Service Pack 1
- Netzadapter: Realtek RTL 8139/810X 100 Mb/s Ethernet
- Memory: 640 MB
- Monitor: 17 Zoll TFT Display

Der Netzzugang erfolgte bei den Tests der Prüfstelle über ISDN, DSL oder eine LAN-Verbindung. In die Tests des Entwicklers waren auch Modem-Verbindungen einbezogen.

Für die Tests wurden keine Werkzeuge verwendet, die nicht standardmäßig zum Betriebssystem (Windows 2000, Windows XP) gehören (insbesondere Microsoft Management Console, MMC) oder vom Entwickler bereitgestellt wurden (accipserver.exe)

# 8 Evaluierte Konfiguration

Der EVG wird durch die Bezeichnung „VPNConnect Version 1.2.650“ identifiziert.

Der EVG wird lediglich in einer vor der Auslieferung festgelegten Konfiguration betrieben. Die sicherheitsrelevanten Einstellungen des EVG werden vom Hersteller vorkonfiguriert. Der Benutzer des EVG kann dann lediglich noch Art des Internetzugangs einstellen.

Der EVG kann auf den Betriebssystemen Windows 2000 und Windows XP betrieben werden und wurde auch auf beiden Betriebssystemen getestet.

Der Netzzugang kann über Modem, ISDN, DSL oder eine LAN-Verbindung erfolgen. Alle Verbindungsarten wurden in die Tests einbezogen.

# 9 Ergebnisse der Evaluierung

Der Evaluierungsbericht (ETR), [7] wurde von der Prüfstelle gemäß den Common Criteria [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind.

Die Evaluationsmethodologie CEM [2] wurde für die Komponenten aus der Vertrauenswürdigkeitsstufe EAL 2 verwendet.

Das Urteil für die CC, Teil 3 Anforderungen an die Vertrauenswürdigkeit (gemäß EAL 2 und die Klasse ASE für die Sicherheitsvorgaben) ist in der folgenden Tabelle dargestellt:

| **Vertrauenswürdigkeitsklassen und Komponenten** | | **Urteil** |
|---|---|---|
| Security Target Evaluierung | CC Klasse ASE | PASS |
| EVG-Beschreibung | ASE_DES.1 | PASS |
| Sicherheitsumgebung | ASE_ENV.1 | PASS |
| ST-Einführung | ASE_INT.1 | PASS |
| Sicherheitsziele | ASE_OBJ.1 | PASS |
| PP-Postulate | ASE_PPC.1 | PASS |
| IT-Sicherheitsanforderungen | ASE_REQ.1 | PASS |
| Explizit dargelegte IT-Sicherheitsanforderungen | ASE_SRE.1 | PASS |
| EVG-Übersichtsspezifikation | ASE_TSS.1 | PASS |
| Konfigurationsmanagement | CC Klasse ACM | PASS |
| Konfigurationsteile | ACM_CAP.2 | PASS |
| Auslieferung und Betrieb | CC Klasse ADO | PASS |
| Auslieferungsprozeduren | ADO_DEL.1 | PASS |
| Installation, Generierung und Anlauf | ADO_IGS.1 | PASS |
| Entwicklung | CC Klasse ADV | PASS |
| Informelle funktionale Spezifikation | ADV_FSP.1 | PASS |
| Beschreibender Entwurf auf hoher Ebene | ADV_HLD.1 | PASS |
| Informeller Nachweis der Übereinstimmung | ADV_RCR.1 | PASS |
| Handbücher | CC Klasse AGD | PASS |
| Systemverwalterhandbuch | AGD_ADM.1 | PASS |
| Benutzerhandbuch | AGD_USR.1 | PASS |
| Testen | CC Klasse ATE | PASS |
| Nachweis der Testabdeckung | ATE_COV.1 | PASS |
| Funktionales Testen | ATE_FUN.1 | PASS |
| Unabhängiges Testen - Stichproben | ATE_IND.2 | PASS |
| Schwachstellenbewertung | CC Klasse AVA | PASS |
| Stärke der EVG-Sicherheitsfunktionen | AVA_SOF.1 | PASS |
| Schwachstellenanalyse des Entwicklers | AVA_VLA.1 | PASS |

Tabelle 6: Urteil zu den Vertrauenswürdigkeitskomponenten (EAL2)

Die Evaluierung hat gezeigt:

- die Sicherheitsanforderungen für den EVG aus den Sicherheitsvorgaben sind Common Criteria Part 2 erweitert
- die Vertrauenswürdigkeit des EVG ist Common Criteria Teil 3 konform, EAL 2

Es erfolgte keine Bewertung der Stärke der Funktionen, da die Sicherheitsfunktionen, die auf Wahrscheinlichkeits- oder Permutationsmechanismen beruhen auch kryptographische Algorithmen nutzen (vgl. §4 Abs. 3 Nr. 2 BSIG).

Die Resultate der Evaluierung sind nur anwendbar auf den EVG “VPNConnect Version 1.2.650” (siehe auch Kapitel 2 dieses Reports).

Die Gültigkeit kann auf neue Versionen bzw. Releases des Produktes erweitert werden. Voraussetzung dafür ist, dass der Antragsteller die Re-Zertifizierung oder die Assurance Continuity in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen der Sicherheitsfunktionen aufdeckt.

# 10 Hinweise und Empfehlungen

Hinweis zum Begriff Branding im Zusammenhang mit dem EVG:

VPNConnect wird in mehreren unterschiedlichen grafischen Versionen, sog. „Brandings“ vertrieben. Diese verschiedenen Ausführungen unterscheiden sich jeweils nur in der grafischen Oberfläche der Installationsroutine und der Anwendungs-Oberfläche. Des Weiteren findet pro jeweiligen Branding eine Konfiguration des Internet-Explorers in Form eines Austausches des Logos, Vorbelegung einer Startseite, sowie ein oder mehrere Einträge im Favoriten Ordner statt. Es findet zu keiner Zeit eine sicherheitsrelevante Änderung der Konfigurationsdateien statt.
Die Grundeinstellungen der Konfigurationsdateien können nur von Administratoren mit Herstellerautorisierung geändert werden.
Da der EVG in verschiedenen Brandings vertrieben wird, ist jede CD folgendermaßen beschriftet:
Die CD trägt in großer Schrift die Aufschrift „VPNConnect Version 1.2.650, durch die der EVG eindeutig identifiziert werden kann.
Zusätzlich enthält das Label noch die Information, dass es sich bei der ausgelieferten CD um ein Branding des EVG „VPNConnect Version 1.2.650 handelt, dass die sicherheitsrelevante Funktionalität gegenüber der zertifizierten Version unverändert ist und dass sich hierzu nähere Erläuterungen im Administratorenhandbuch befinden. Außerdem enthält das Label die Zertifizierungs-ID BSI-DSZ-CC-0288-2006. Des Weiteren können sich auf dem Label der CD zusätzliche branding-spezifische graphische Symbole befinden.

Die Dokumente [9] und [10] enthalten die notwendigen Informationen über die Verwendung des EVG und alle Sicherheitshinweise für den EVG.

# 11 Anhänge

Keine

# 12 Sicherheitsvorgaben

Die Sicherheitsvorgaben [6] werden zur Veröffentlichung in einem separaten Dokument bereitgestellt.

# 13 Definitionen

## 13.1 Abkürzungen

**BSI** Bundesamt für Sicherheit in der Informationstechnik, Bonn

**CC** Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

**CHAP** Challenge-Handshake Authentication Protocol

**DTAG** Deutsche Telekom AG

**EAL** Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

**EVG** Evaluationsgegenstand

**IT** Informationstechnik

**PP** Protection Profile - Schutzprofil

**SF** Sicherheitsfunktion

**SOF** Strength of Function - Stärke der Funktionen

**ST** Security Target - Sicherheitsvorgaben

**TSC** TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle

**TSF** TOE Security Functions - EVG-Sicherheitsfunktionen

**TSP** TOE security policy - EVG-Sicherheitspolitik

**VISP** Virtual Internet Service Provider

**VPN** Virtual Private Network – Virtuelles Privates Netzwerk

## 13.2 Glossar

**Zusatz** - Das Hinzufügen einer oder mehrerer Vertrauenswürdigkeitskomponenten aus Teil 3 der CC zu einer EAL oder einem Vertrauenswürdigkeitspaket.

**Erweiterung** - Das Hinzufügen von funktionalen Anforderungen, die nicht in Teil 2 enthalten sind, und/oder von Vertrauenswürdigkeitsanforderungen, die nicht in Teil 3 enthalten sind, zu den Sicherheitsvorgaben bzw. dem Schutzprofil.

**Formal** - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik, die auf bewährten mathematischen Konzepten basiert.

**Informell** - Ausgedrückt in natürlicher Sprache.

**Objekt** - Eine Einheit im TSC, die Informationen enthält oder empfängt und mit der Subjekte Operationen ausführen.

**Schutzprofil** - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG, die besondere Konsumentenbedürfnisse erfüllen.

**Sicherheitsfunktion** - Ein Teil oder Teile eines EVG, auf die zur Durchsetzung einer hierzu in enger Beziehung stehenden Teilmenge der Regeln der EVG-Sicherheitspolitik Verlaß sein muß.

**Sicherheitsvorgaben** - Eine Menge von Sicherheitsanforderungen und Sicherheitsspezifikationen, die als Grundlage für die Prüfung und Bewertung eines angegebenen EVG dienen.

**Semiformal** - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik.

**Stärke der Funktionen** - Eine Charakterisierung einer EVG-Sicherheitsfunktion, die den geringsten angenommenen Aufwand beschreibt, der notwendig ist, um deren erwartetes Sicherheitsverhalten durch einen direkten Angriff auf die zugrundeliegenden Sicherheitsmechanismen außer Kraft zu setzen.

**SOF-Niedrig** - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen angemessenen Schutz gegen zufälliges Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein geringes Angriffspotential verfügen.

**SOF-Mittel** - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen angemessenen Schutz gegen naheliegendes oder absichtliches Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein mittleres Angriffspotential verfügen.

**SOF-Hoch** - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen geeigneten Schutz gegen geplantes oder organisiertes Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein hohes Angriffspotential verfügen.

**Subjekt** - Eine Einheit innerhalb des TSC, die die Ausführung von Operationen bewirkt.

**Evaluationsgegenstand** - Ein IT-Produkt oder -System - sowie die dazugehörigen Systemverwalter- und Benutzerhandbücher - das Gegenstand einer Prüfung und Bewertung ist.

**EVG-Sicherheitsfunktionen** - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfaßt, auf die Verlaß sein muß, um die TSP korrekt zu erfüllen.

**EVG-Sicherheitspolitik** - Eine Menge von Regeln, die angibt, wie innerhalb eines EVG Werte verwaltet, geschützt und verteilt werden.

**Anwendungsbereich der TSF-Kontrolle** - Die Menge der Interaktionen, die mit oder innerhalb eines EVG vorkommen können und den Regeln der TSP unterliegen.

# 14 Literaturangaben

[1] Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind..

[5] Deutsche IT-Sicherheitszertifikate (BSI 7148, BSI 7149), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird.

[6] Sicherheitsvorgaben BSI-DSZ-0288-2006, Version 1.11, 14.02.2006, Sicherheitsvorgaben für das Produkt VPNConnect Version 1.2.650, I-MOTION GmbH

[7] Evaluierungsbericht BSI-DSZ-CC-0288-2006, Version 2, 16.02.2006, (vertrauliches Dokument)

**Handbücher**

[8] Handbuch für herstellerautorisierte Administratoren, Version 1.4, 16.12.2005, I-MOTION GmbH

[9] Handbuch für Systemverwalter und Benutzer, Version 1.5, 10.02.2006, I-MOTION GmbH

[10] Benutzer-Handbuch, Version 1.2, 19.12.2005, I-Motion GmbH.

# C Auszüge aus den technischen Regelwerken

CC Teil 1:

**Caveats on evaluation results** (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

**Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

**Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

**Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

**Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Teil 3

## **Assurance categorisation** (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

| Assurance Class | Assurance Family | Abbreviated Name |
|---|---|---|
| Class ACM: Configuration management | CM automation | ACM_AUT |
| | CM capabilities | ACM_CAP |
| | CM scope | ACM_SCP |
| Class ADO: Delivery and operation | Delivery | ADO_DEL |
| | Installation, generation and start-up | ADO_IGS |
| Class ADV: Development | Functional specification | ADV_FSP |
| | High-level design | ADV_HLD |
| | Implementation representation | ADV_IMP |
| | TSF internals | ADV_INT |
| | Low-level design | ADV_LLD |
| | Representation correspondence | ADV_RCR |
| | Security policy modeling | ADV_SPM |
| Class AGD: Guidance documents | Administrator guidance | AGD_ADM |
| | User guidance | AGD_USR |
| Class ALC: Life cycle support | Development security | ALC_DVS |
| | Flaw remediation | ALC_FLR |
| | Life cycle definition | ALC_LCD |
| | Tools and techniques | ALC_TAT |
| Class ATE: Tests | Coverage | ATE_COV |
| | Depth | ATE_DPT |
| | Functional tests | ATE_FUN |
| | Independent testing | ATE_IND |
| Class AVA: Vulnerability assessment | Covert channel analysis | AVA_CCA |
| | Misuse | AVA_MSU |
| | Strength of TOE security functions | AVA_SOF |
| | Vulnerability analysis | AVA_VLA |

**Table C-1 -Assurance family breakdown and mapping“**

## **Evaluation assurance levels** (chapter 6)

„The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

## **Evaluation assurance level (EAL) overview** (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

| Assurance Class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Configuration management | ACM_AUT | | | | 1 | 1 | 2 | 2 |
| | ACM_CAP | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ACM_SCP | | | 1 | 2 | 3 | 3 | 3 |
| Delivery and operation | ADO_DEL | | 1 | 1 | 2 | 2 | 2 | 3 |
| | ADO_IGS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Development | ADV_FSP | 1 | 1 | 1 | 2 | 3 | 3 | 4 |
| | ADV_HLD | | 1 | 2 | 2 | 3 | 4 | 5 |
| | ADV_IMP | | | | 1 | 2 | 3 | 3 |
| | ADV_INT | | | | | 1 | 2 | 3 |
| | ADV_LLD | | | | 1 | 1 | 2 | 2 |
| | ADV_RCR | 1 | 1 | 1 | 1 | 2 | 2 | 3 |
| | ADV_SPM | | | | 1 | 3 | 3 | 3 |
| Guidance documents | AGD_ADM | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_USR | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life cycle support | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | | 1 | 2 | 2 | 3 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | 2 | 2 | 3 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_CCA | | | | | 1 | 2 | 2 |
| | AVA_MSU | | | 1 | 2 | 2 | 3 | 3 |
| | AVA_SOF | | 1 | 1 | 1 | 1 | 1 | 1 |
| | AVA_VLA | | 1 | 1 | 2 | 3 | 4 | 4 |

**Table C-2 - Evaluation assurance level summary“**

## **Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 6.2.1)

„Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

## **Evaluation assurance level 2 (EAL2) - structurally tested** (chapter 6.2.2)

„Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.“

## **Evaluation assurance level 3 (EAL3) - methodically tested and checked** (chapter 6.2.3)

„Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

## **Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed** (chapter 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial

specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

**Evaluation assurance level 5 (EAL5) - semiformally designed and tested** (chapter 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

**Evaluation assurance level 6 (EAL6) - semiformally verified design and tested** (chapter 6.2.6)

„Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

**Evaluation assurance level 7 (EAL7) - formally verified design and tested** (chapter 6.2.7)

„Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

## Strength of TOE security functions (AVA_SOF) (chapter 14.3)

**AVA_SOF** Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.“

## Vulnerability analysis (AVA_VLA) (chapter 14.4)

**AVA_VLA** Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.“

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.“

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

This page is intentionally left blank.