Zertifizierungsreport

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0309-2006

zu

Smart Terminal ST-2xxx
Firmware Version 5.08

der

Cherry 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-0309-2006

Chipkartenterminal der Familie

Smart Terminal ST-2xxx Firmware Version 5.08

der

Cherry GmbH

Common Criteria Arrangement für Komponenten bis EAL4

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 sowie Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL4 evaluiert.

Prüfergebnis:

Funktionalität:	**Produktspezifische Sicherheitsvorgaben** **Common Criteria Teil 2 konform**
Vertrauenswürdigkeit:	**Common Criteria Teil 3 konform** **EAL3 mit Zusatz von** ADO_DEL.2 – Erkennung von Modifizierungen ADV_IMP.1 – Teilmenge der Implementierung der TSF ADV_LLD.1 – Beschreibender Entwurf auf niedriger Ebene ALC_TAT.1 – Klar festgelegte Entwicklungswerkzeuge AVA_MSU.3 – Analysieren und Testen auf unsichere Zustände AVA_VLA.4 – Hohe Widerstandsfähigkeit

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 09. Februar 2006

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

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

Die Bewertung der Stärke der Funktionen erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten Kryptoalgorithmen (vgl. §4 Abs. 3 Nr. 2 BSIG).

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)
- Informationen von der Zertifizierungsstelle zur Methodologie für Vertrauenswürdigkeitskomponenten oberhalb von EAL 4 (AIS 34)

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.

Diese Evaluierung beinhaltet die Komponenten AVA_MSU.3 und AVA_VLA.4, die nicht unter der Common Criteria Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten anerkannt werden. Für die gegenseitige Anerkennung sind die in der Vertrauenswürdigkeitsstufe EAL4 enthaltenen Komponenten dieser Vertrauenswürdigkeitsfamilien relevant.

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 Smart Terminal ST-2xxx, Firmware Version 5.08 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts Smart Terminal ST-2xxx, Firmware Version 5.08 wurde von der TÜV Informationstechnik GmbH durchgeführt. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Antragsteller, Hersteller und Vertreiber ist

Cherry GmbH
Cherrystraße
D-91275 Auerbach.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 09. Februar 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 Smart Terminal ST-2xxx, Firmware Version 5.08 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.

[7] Cherry GmbH
Cherrystraße
D-91275 Auerbach

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

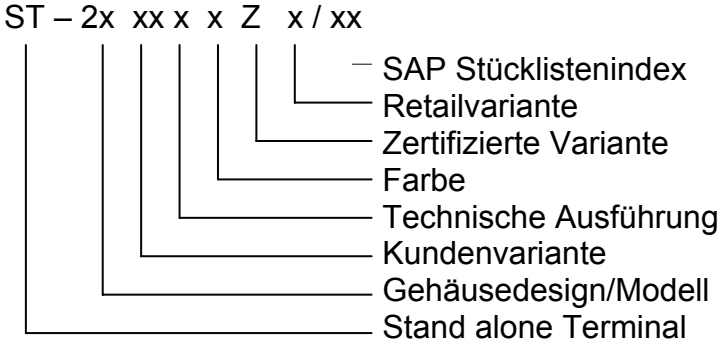
- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

Gliederung des Zertifizierungsberichtes

1 Zusammenfassung

Der Evaluationsgegenstand (EVG) ist der universelle Chipkartenleser mit Keypad der Famile SmartTerminal ST-2xxx mit der Firmware-Version 5.08 des Herstellers Cherry GmbH.

Der Evaluationsgegenstand gliedert sich dabei in verschiedene Produktvarianten mit der gleichen evaluiertn Firmware, welche die folgenden Bezeichnungen besitzen:



Die Anfangsbezeichnung ST deklariert das Produkt als Stand alone Terminal und der Buchstabe Z zeigt an, dass es sich um einen zertifizierten Chipkartenleser handelt.

Der EVG besitzt die Möglichkeit, mit kontaktbehaftete Speicher- und Prozessorchipkarten zu kommunizieren. Bei synchronen Chipkarten (Speicherchipkarten) werden Übertragungsproto-kolle nach herstellerspezifischen Spezifikationen unterstützt. Für Prozessorkarten werden die Übertragungsprotokolle T=0 und T=1 angeboten. Prozessorkarten müssen die Spezifikationen [13] bzw. [14] erfüllen.

Propagiertes Ziel des EVG ist es, das Kartenterminal für Anwendungen zur Erzeugung von qualifizierten elektronischen Signaturen nach dem deutschen Signaturgesetz [8] einzusetzen. Dazu wird für Prozessorchipkarten die Funktion der sicheren PIN-Eingabe über das Keypad vom EVG unterstützt. Für Speicherchipkarten steht eine solche Funktion der sicheren PIN-Eingabe nicht zur Verfügung.

Der EVG ist für den Einsatz im nichtöffentlichen Bereich, d.h. den privaten Bereich oder die normale Büroumgebung mit geregelten Zugriffsmöglichkeiten vorgesehen. Er bietet Schutz gegen Angreifer mit hohem Angriffspotential. Die Unversehrtheit des EVG kann der Benutzer anhand seiner Versiegelung überprüfen.

Der EVG bietet prinzipiell die Möglichkeit, die Firmware mit einer neuen Version zu aktualisieren und somit dem Endkunden einen größeren Investitionsschutz für sein Gerät zu gewähren[8]. Die Sicherheitsfunktionalität des EVG erzwingt, dass ausschließlich von der Firma Cherry bereitgestellte und signierte Firmware aufgespielt werden kann. Der Benutzer wird somit vor dem unzulässigen Aufladen kompromittierter Firmware geschützt.

Momentan stellt der Hersteller keine Firmware für das Chipkartenterminal ST-2xxx separat vom Gerät zur Verfügung. Von daher ist die Auslieferung von Firmware für das

[8] Das Aufspielen einer anderen Firmware-Version ist nicht Bestandteil dieses Zertifikats. Um weiterhin mit einem zertifizierten Produkt zu arbeiten, muss die neue Firmware-Version sowie der zugehörige Auslieferungsweg in einem weiteren Verfahren evaluiert und zertifiziert werden (s. auch Kapitel 10).

Chipkartenterminal ST-2xxx allein (z.B. über das Internet) nicht Bestandteil des Zertifikats. Innerhalb der Evaluierung und Zertifizierung wurde lediglich die Auslieferung des gesamten Gerätes inklusive der im Rahmen der Produktion aufgebrachten Firmware betrachtet.

Sollte zukünftig der Hersteller zertifizierte und bestätigte Versionen der Firmware für das Gerät bereitstellen, so muss dieser Auslieferungsweg in einem Verfahren zur Re-Zertifizierung des Produktes geprüft werden. Außerdem darf der Benutzer für die Verwendung des Gerätes im Bereich der qualifizierten elektronischen Signatur nur solche Firmware aufspielen, die vom Hersteller als bestätigt und zertifiziert gekennzeichnet ist.

Die Sicherheitsfunktionen des EVG wurden so gewählt, dass den Sicherheitszielen des deutschen Signaturgesetzes [8] bzw. der Signaturverordnung [9]

- Keine Preisgabe oder Speicherung der Identifikationsdaten (§15 Abs. 2 Nr. 1a [9])
- Erkennbarkeit sicherheitstechnischer Veränderungen (§15 Abs. 4 [9])

entsprochen wird.

Die Evaluation des Produkts Smart Terminal ST-2xxx, Firmware Version 5.08 wurde von TÜV Informationstechnik GmbH durchgeführt und am 23. Januar 2006 abgeschlossen. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[9].

Antragsteller, Hersteller und Vertreiber ist

Cherry GmbH
Cherrystraße
D-91275 Auerbach

1.1 Vertrauenswürdigkeitspaket

Die Vertrauenswürdigkeitskomponenten des EVG sind konform zum Teil 3 der CC [1]. Der EVG wurde erfolgreich mit der Prüfstufe EAL3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4 evaluiert. In der folgenden Tabelle sind die gewählten Vertrauenswürdigkeitskomponenten detailliert aufgeführt.

Klasse	Familie	Komponente
Evaluation der Sicherheitsvor-gaben	ASE_DES.1	Beschreibung des EVG
	ASE_ENV.1	Sicherheitsumgebung
	ASE_INT.1	ST Einführung
	ASE_OBJ.1	Sicherheitsziele
	ASE_PPC.1	PP-Postulate
	ASE_REQ.1	IT– Sicherheitsanforderungen
	ASE_SRE.1	Explizit dargelegte IT– Sicherheitsanforderungen

[9] Information Technology Security Evaluation Facility

Klasse	Familie	Komponente
	ASE_TSS.1	EVG– Übersichtsspezifikation
Konfigurations-management	ACM_CAP.3	Autorisierungskontrolle
	ACM_SCP.1	EVG– CM– Umfang
Auslieferung und Betrieb	ADO_DEL.2	Erkennung von Modifizierungen
	ADO_IGS.1	Installations-, Generierungs-, und Anlaufprozeduren
Entwicklung	ADV_FSP.1	Informell funktionale Spezifikation
	ADV_HLD.2	Sicherheitsspezifischer Entwurf auf hoher Ebene
	ADV_IMP.1	Teilmenge der Implementierung der TSF
	ADV_LLD.1	Beschreibender Entwurf auf niedriger Ebene
	ADV_RCR.1	Informeller Nachweis der Übereinstimmung
Handbücher	AGD_ADM.1	Systemverwalterhandbuch
	AGD_USR.1	Benutzerhandbuch
Lebenszyklus – Unterstützung	ALC_DVS.1	Identifikation der Sicherheitsmaßnahmen
	ALC_TAT.1	Klar festgelegte Entwicklungswerkzeuge
Testen	ATE_COV.2	Analyse der Testabdeckung
	ATE_DPT.1	Testen – Entwurf auf hoher Ebene
	ATE_FUN.1	Funktionales Testen
	ATE_IND.2	Unabhängiges Testen – Stichprobenartig
Schwachstellen-bewertung	AVA_MSU.3	Analysieren und Testen auf unsichere Zustände
	AVA_SOF.1	Stärke der EVG-Sicherheitsfunktionen
	AVA_VLA.4	Hohe Widerstandsfähigkeit

Tabelle 1: Vertrauenswürdigkeitskomponenten und EAL-Zusätze

1.2 Funktionalität

Zum Einsatz des EVG als Signaturanwendungskomponente nach dem deutschen Signaturgesetz [8] in einer nicht-öffentlichen Umgebung stehen drei Sicherheitsfunktionen und eine Sicherheitsmaßnahme zur Verfügung. Diese sind in der folgenden Tabelle aufgeführt:

Sicherheitsfunktion	Beschreibung
Schutz der PIN (SF.1)	Das Umschalten des Kartenterminals in den sicheren PIN-Eingabemodus wird durch ein explizites CT-Kommando nach CCID-Standard [12] durchgeführt. Dieses CT-Kommando enthält die PIN-Handlingsvereinbarungen und das Chipkar-tenkommando, in welches die PIN an die spezifizierte Stelle integriert wird. Anhand des Instructionbytes des Chipkartenkommandos wird überprüft,

Sicherheitsfunktion	Beschreibung
	ob es sich um ein PIN-Kommando handelt, welches explizit eine PIN-Eingabe erwartet. Die Eingabe der persönlichen Identifikationsdaten wird im RAM zwischengespeichert, um sie nach Beendigung der Eingabe direkt mit dem PIN-Kommando zur Chipkarte zu senden. Der PIN-Eingabemodus wird optisch durch die orange blinkende PIN-LED angezeigt, bis die Vollständigkeit der PIN erreicht beziehungsweise der Vorgang abgebrochen wird. Zum Abbruch des Vorgangs zählen das Ziehen der Karte, das Betätigen der Abbruchtaste und das Überschreiten der vorgegebenen Eingabezeit. Der Eingabefortschritt wird mittels der Übertragung von Dummycodes dem System mitgeteilt.
Speicherwiederaufbereitung (SF.2)	Die Kommunikation zwischen PC-System und Chipkarte basiert gemäß CCID-Standard [12] auf den sogenannten APDUs. Wird eine APDU über die USB-Schnittstelle im Kartenterminal empfangen, so wird sie zuerst zwischengespeichert, um anschließend zur Chipkarte gesendet zu werden. Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos bzw. dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet, um sicherzustellen, dass keine persönlichen Identifikationsdaten bzw. Datenfragmente im Kartenterminal erhalten bleiben. Außerdem wird die LED zur Anzeige der sicheren PIN-Eingabe ausgeschaltet.
Sicherer Firmware-download (SF.3)	Die Verifikation einer Signatur der Firmware mit dem asymmetrischen RSA-Algorithmus und einer Bitlänge von 1024 garantiert die Integrität und Authentizität der Firmware beim Laden einer neuen Firmware in den Chipkartenleser. Der Hash-Wert über die neu zu ladende Firmware wird basierend auf dem Algorithmus SHA-1 mit einer Länge von 160 Bit ermittelt. Die Verifikation der Integrität und Authentizität erfolgt im TOE durch Vergleich des ermittelten Hash-Wertes und des Hash-Wertes als Bestandteil der entschlüsselten Signatur. Der öffentliche Schlüssel ist hierfür im TOE gespeichert.

Tabelle 2: Sicherheitsfunktionen des EVG

Sicherheitsmaßnahme	Beschreibung
Versiegelung (SM.1)	Anhand authentischer und fälschungssicherer Sicherheitssiegel, welche über die Trennkante zwischen Gehäuseunter- und Oberteil geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden. Dies wird dadurch sichergestellt, dass ein Öffnen nicht ohne Beschädigung des Siegels möglich ist. Die Beschaffenheit (Zerstöreigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann. Das eingesetzte Siegel ist fälschungssicher und weist Authentizitätsmerkmale auf.

Tabelle 3: Sicherheitsmaßnahme des EVG

1.3 Stärke der Funktionen

Der EVG bietet Schutz gegen hohes Angriffspotential. Die geforderte Mindeststärke des EVG ist SOF-hoch.

Die Bewertung der Stärke der Funktionen erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten Kryptoalgorithmen (vgl. §4 Abs. 3 Nr. 2 BSIG).

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

Alle Bedrohungen gehen von einem Angreifer mit einem hohen Angriffpotential aus.

Die zu schützenden Objekte sind die PIN als Identifikationsmerkmal des Karteninhabers sowie die Firmware und die Hardware des EVG.

Folgende Bedrohungen für die zu schützenden Objekte wurden identifiziert:

Bedrohungen	Beschreibung
T.1	Ein Angreifer könnte versuchen, durch Einsatz von Sniffertools (Hardware oder Software) die über den EVG eingegebene PIN auszuspähen.
T.2	Ein Angreifer könnte versuchen, eine PIN-Eingabe zu provozieren und damit die PIN zu erlangen.
T.3a	Ein Angreifer könnte versuchen, den EVG in seinen Bestandteilen (Hardware und Firmware) zu manipulieren, um die PIN zu ermitteln.
T.3b	Ein Angreifer könnte versuchen, die im EVG zwischengespeicherte PIN auszulesen.
T.4	Ein Angreifer könnte versuchen, die PIN in einen ungeschützten Bereich der Chipkarte zu schreiben, um sie anschließend daraus auszulesen

Bedrohungen	Beschreibung
T.5	Ein Angreifer könnte versuchen, durch Manipulation des Sicherheitssiegels sicherheitstechnische Veränderungen am TOE vorzunehmen.
T.6	Ein Angreifer könnte versuchen, durch Manipulation beim Download eine modifizierte oder fremde Firmware in den Leser zu laden, die Funktionalitäten zum Ausspähen der PIN beinhalten können.

Tabelle 4: Bedrohungen

Organisatorische Sicherheitspolitiken sind nicht vorgesehen.

1.5 Spezielle Konfigurationsanforderungen

Die Ergebnisse der Evaluierung gelten für die evaluierte und getestete Ausprägung des EVG:

> Chipkartenterminal ST-2xxx mit der Firmware-Version 5.08 des Herstellers Cherry GmbH.

Die Installation und Inbetriebnahme des EVG ist in den der Lieferung in Papierform beiliegenden Betriebsdokumentationen beschrieben. Der Kunde wird darauf hingewiesen, dass das Siegel unbeschädigt und authentisch sein muss, wenn er den EVG in Betrieb nimmt.

Eine Konfiguration des EVG und eine damit verbundene Beeinflussung der Sicherheitsfunktionen durch den Nutzer ist nicht möglich. Das Aufladen neuer Firmware stellt in diesem Zusammenhang keine Konfiguration sondern eine Veränderung des EVG dar, die nicht Bestandteil des Zertifikats ist.

1.6 Annahmen über die Einsatzumgebung

Der Einsatz des Kartenterminal ist für nichtöffentliche Umgebungen wie Single- und MultiUser-PC im privaten Bereich und in der Büroumgebung zugelassen.

Der Endanwender wird über seine Verantwortung während der Nutzung des EVGs in Zusammenhang mit einer Chipkarte informiert. Die Regeln zur sicheren Aufbewahrung und Nichtweitergabe der PIN der Chipkarte werden dem Anwender vom Herausgeber der Chipkarte mitgeteilt.

Für den EVG werden folgende Annahmen an die Einsatzumgebung gestellt:

Annahmen	Beschreibung
AE.1	Es wird angenommen, dass der EVG für die nicht öffentliche Umgebung eingesetzt wird.
AE.2	Es wird angenommen, dass der Benutzer ausschließlich Prozessorkarten benutzt, die den Spezifikationen ISO 7816 [13] bzw. EMV 2000 [14] genügen.
AE.3	Es wird angenommen, dass sich der Nutzer vor der Inbetriebnahme und regelmäßig vor Benutzung des Gerätes durch die Kontrolle der Unversehrtheit der Siegel überzeugt, ob keine sicherheitstechnischen Veränderungen am Kartenterminal vorgenommen wurden.

Annahmen	Beschreibung
AE.4	Es wird angenommen, dass der Benutzer eine unbeobachtete Eingabe der Identifikationsdaten (PIN) gewährleistet.
AE.5	Es wird angenommen, dass der Benutzer während der PIN-Eingabe über das Keypad den Status der LED dahingehend überprüft, ob der Modus der sicheren PIN-Eingabe aktiv ist.
AE.6	Es wird angenommen, dass der Benutzer die PIN über das Keypad eingibt.
AE.7	Es wird angenommen, dass der Benutzer mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor Benutzung des Geräts verifiziert, ob die Versionsnummer des TOEs mit der bestätigten Version übereinstimmt. Applikationen gemäß §2 Nummer 11 SigG sollten automatisch verifizieren, dass nur bestätigte Versionen des TOEs verwendet werden, um diese Aufgabe dem Endanwender abzunehmen.
AE.8	Es wird angenommen, dass der Benutzer bei einem späteren Firmware-Upgrade darauf achtet, dass die zum Download bereitgestellte Firmware explizit als zertifizierte und bestätigte Version gekennzeichnet ist.

Tabelle 5: Annahmen

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 Smart Terminal ST-2xxx, Firmware Version 5.08. Er stellt ein universelles Chipkartenlesegerät dar, das Prozessorchipkarten nach ISO7816 und EMV über verschiedene Applikationsschnittstellen (CT-API [15], PC/SC [16] u.a.) verarbeiten kann. Die Geräte arbeiten mit allen Chipkarten-Datenübertragungsprotokollen gemäß ISO 7816 [13] (T=0, T=1), Datenübertragungsprotokolle für Speicherchipkarten (I^2C-, 2-Wire-, 3-Wire-Protokoll) werden ebenfalls unterstützt.

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Bezeichnung	Version	Form der Auslieferung
1	HW	SmartTerminal ST-2xxx mit Firmware	5.08	Einzelverpackung
2	DOK	Quick-Start Instructions SmartTerminal ST-2000U	03, Dezember 2005	Papier

Nr	Typ	Bezeichnung	Version	Form der Auslieferung
3	DOK	Betriebsdokumentation „AGD“ 644-0417-01 DE	009, Dezember 2005	Papier
4	SW	Treibersoftware[10]		CD-ROM

Tabelle 6: Auslieferungsumfang des TOE

3 Sicherheitspolitik

Es ist ein erklärtes Ziel, den EVG für die Applikation „digitale Signatur“ nach dem deutschen Signaturgesetz [8] einzusetzen. Um ein elektronisches Dokument digital zu signieren, muss sich ein Benutzer durch Besitz (Signaturkarte) und Wissen (PIN) gegenüber seiner Signaturkarte authentifizieren.

Im Vordergrund der Sicherheitspolitik des EVG steht deshalb der Schutz der Firmware und der persönlichen Identifikationsdaten (PIN) als Identifikationsmerkmal des Chipkarteninhabers sowie die Unversehrtheit der Hardware des EVG.

Die Sicherheitsziele des EVG sehen vor, die Identifikationsdaten des Benutzers nicht zu speichern und/oder preiszugeben. Sicherheitstechnische Veränderungen am EVG müssen erkennbar sein.

4 Annahmen und Klärung des Einsatzbereiches

4.1 Annahmen über den Einsatz

Der TOE ist für einen universellen Einsatz in chipkartenbasierenden Applikationen ohne vorherige Authentisierung geeignet. Mögliche Anwendungen sind:

- Digitale Signatur
- Homebanking (HBCI)
- Access Control (PC-Systeme)
- Internet Shopping

Bei der Anwendung „qualifizierte elektronische Signatur“ dürfen ausschließlich im Sinne des SigG und SigV bestätigte Chipkarten und bestätigte Signaturanwendungsprogramme bzw. herstellererklärte Signuaturanwendungsprogramme verwendet werden. Zugelassene Komponenten sind auf der Internetseite der Bundesnetzagentur (www.bundesnetzagentur.de) zu finden.

Die Sicherheitsfunktionalität des EVG ist unabhängig vom ansteuernden Anwendungsprogramm immer wirksam. Um die sichere PIN-Eingabe zu nutzen, ist lediglich das entsprechende CT-Kommando nach [12] zu verwenden. Dabei müssen die Chipkarten die Voraussetzungen nach AE.2 (s. u.) erfüllen.

[10] Die CD-ROM ist optional. Sie ist somit nicht Bestandteil der Evaluierung und damit nicht im Zertifikat enthalten.

Der Einsatz des Kartenterminal ist für folgende nichtöffentliche Umgebungen zugelassen:

- Single- und MultiUser-PC im privaten Bereich und in der Büroumgebung.

Der Endanwender wird über seine Verantwortung während der Nutzung des EVGs in der zugehörigen Benutzerdokumentation informiert. Dazu gehört auch, dass die Regeln zur sicheren Aufbewahrung und Nichtweitergabe der PIN der Chipkarte dem Anwender vom Herausgeber der Chipkarte mitgeteilt werden.

4.2 Angenommene Einsatzumgebung

Folgende Annahmen werden in den Sicherheitsvorgaben [6] zur Einsatzumgebung formuliert:

Annahmen	Beschreibung
AE.1	Es wird angenommen, dass der EVG für die nicht öffentliche Umgebung eingesetzt wird.
AE.2	Es wird angenommen, dass der Benutzer ausschließlich Prozessorkarten benutzt, die den Spezifikationen ISO 7816 [13] bzw. EMV 2000 [14] genügen.
AE.3	Es wird angenommen, dass sich der Nutzer vor der Inbetriebnahme und regelmäßig vor Benutzung des Gerätes durch die Kontrolle der Unversehrtheit der Siegel überzeugt, ob keine sicherheitstechnischen Veränderungen am Kartenterminal vorgenommen wurden.
AE.4	Es wird angenommen, dass der Benutzer eine unbeobachtete Eingabe der Identifikationsdaten (PIN) gewährleistet.
AE.5	Es wird angenommen, dass der Benutzer während der PIN-Eingabe über das Keypad den Status der LED dahingehend überprüft, ob der Modus der sicheren PIN-Eingabe aktiv ist.
AE.6	Es wird angenommen, dass der Benutzer die PIN über das Keypad eingibt.
AE.7	Es wird angenommen, dass der Benutzer mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor Benutzung des Geräts verifiziert, ob die Versionsnummer des TOEs mit der bestätigten Version übereinstimmt. Applikationen gemäß §2 Nummer 11 SigG sollten automatisch verifizieren, dass nur bestätigte Versionen des TOEs verwendet werden, um diese Aufgabe dem Endanwender abzunehmen.
AE.8[11]	Es wird angenommen, dass der Benutzer bei einem späteren Firmware-Upgrade darauf achtet, dass die zum Download bereitgestellte Firmware explizit als zertifizierte und bestätigte Version gekennzeichnet ist.

Tabelle 7: Annahmen an die Einsatzumgebung

[11] Die Auslieferung neuer Firmware über das Internet gehört nicht zum Umfang der Evaluierung und ist somit nicht in diesem Zertifikat enthalten. Diese Annahme muss zukünftig erfüllt werden, damit der Benutzer für qualifizierte Signaturen nur bestätigte und zertifizierte Firmware einsetzt.

4.3 Klärung des Einsatzbereiches

Es wurden keine Bedrohungen identifiziert, die nicht durch die Sicherheitsfunktionen des EVG, sondern ausschließlich durch dessen Einsatzumgebung abgewehrt werden. Die Annahmen an die Einsatzumgebung unterstützen den EVG jedoch, die in Kapitel 1.4 beschriebenen Bedrohungen abzuwehren.

Nähere Informationen zu den Sicherheitsfunktionen des EVG befinden sich in Kapitel 1.2 dieses Reportes oder in den Sicherheitsvorgaben [6], Kapitel 6.1 und 6.2.

5 Informationen zur Architektur

Der EVG besteht aus Hardware und Firmware. Die Hardware-Komponenten werden im Sinne von Teilsystemen wie folgt aufgegliedert:

- 8051 Mikrocontroller mit internem Datenspeicher (EEPROM), Programmspeicher (SRAM), USB-Controller, Smart Card Controller
- USB-Interface (mit Kabel und Stecker)
- Anzeigeeinheit (Leuchtdioden)
- Keypad
- Chipkarteninterface (Kontaktiereinheit)

Die in Firmware realisierten Teilsysteme des EVG sind auf dem Mikrocontroller implementiert. Es werden fünf Teilsysteme identifiziert, welche die logische Struktur im Aufbau der Firmware wiedergeben:

- *TSS1 USB*: Das Subsystem TSS1 verwaltet und implementiert alle Funktionen, die sich auf die Verarbeitung der Standard USB Kommandos und der Host-spezifischen Kommandos beziehen. Von diesem Subsystem werden die über den USB-Bus empfangenen Host-Kommandos zu den Subsystemen „TSS6 SecureDownload“ und „TSS3 CCID" weitergeleitet.
- *TSS3 CCID*: Das Subsystem TSS3 verarbeitet die vom USB Subsystem erhaltenen CCID Kommandos. Das Subsystem TSS3 leitet die Kommandos entsprechend weiter zu den Subsystemen „TSS4 SmartOS“ oder „TSS6 Secure Download“. Erhaltene Rückgabewerte (Daten, Fehler, Status) von diesen Subsystemen werden vom Subsystem TSS3 an den Host zurückgemeldet.
- *TSS4 SmartOS*: Das Subsystem TSS4 hat alle Funktionen implementiert, die zur Verwaltung von Smart Cards notwendig sind. Es umfasst Funktionen, die Methoden liefern zu Card Power Control, Card Reset und zur Verarbeitung der APDU-Kommandos. Ebenso werden direkt gesendete oder empfangene Datenströme verarbeitet, um unterschiedliche Karten zu unterstützen. Das Subsystem TSS4 stellt die Verbindung her zwischen den Subsystemen „TSS5 Secure Pinpad“ und „TSS3 CCID“.
- *TSS5 SecurePinpad*: Das Subsystem TSS5 hat die Sicherheitsfunktionen SF.1 (PINCOMMAND) und SF.2 (Speicherwiederaufbereitung) implementiert. Es verarbeitet die CCID PIN Eingangsdaten (PIN Verify und PIN Modify). Es behandelt die PIN-Eingabe durch den Benutzer und schickt die APDU-Kommandos zum Subsystem

„TSS4 SmartOS". Die erhaltene Antwort vom Subsystem „TSS4 SmartOS" wird an das Subsystem „TSS3 CCID" zurückgemeldet.

- *TSS6 SecureDownload*: Das Subsystem TSS6 hat die Sicherheitsfunktion SF3. (Sicherer Firmwaredownload) implementiert.

6 Dokumentation

Die folgende Dokumentation wird vom Hersteller an den Kunden ausgeliefert und wurde bei der Evaluation geprüft:

- Quick-Start Instructions SmartTerminal ST-2000U, Version 03 vom Dezember 2005, herausgegeben von der Cherry GmbH.
- Betriebsdokumentation „AGD“ 644-0417-01 DE, Version 009 vom 23.12.2005, herausgegeben von der Cherry GmbH

Wie in Kapitel 2 erwähnt, liegt diese Dokumentation dem Produkt in Papierform bei.

7 Testverfahren

Gemäß der gewählten Prüftiefe EAL3 mit Zusatz wurden umfangreiche Tests sowohl durch Hersteller als auch durch die Prüfstelle durchgeführt. Die jeweiligen Testansätze sind Inhalt der folgenden Kapitel.

7.1 Testverfahren des Herstellers

7.1.1 Getestete EVG Konfiguration

- Die Herstellertests wurden am EVG ST-2000UCZ/01 durchgeführt. Er steht stellvertretend für die EVG-Familie ST-2x xx x x Z -x / xx und besitzt wie in den Sicherheitsvorga-ben [6] definiert die Firmware-Version 5.08.
- Für die Tests wird der EVG an einem IBM-kompatiblen PC-System mit 32-Bit Windows Betriebssystem betrieben. Mit einem Testprogramm des Herstellers werden die Kommandos per Szenario-Files zum EVG gesendet. Die Rückgaben vom EVG werden in Log-Dateien protokolliert.

7.1.2 Testansatz des Herstellers

Gemäß der Teststrategie des Herstellers sollen die vorgesehenen funktionalen Tests am EVG die Übereinstimmung mit den in der funktionalen Spezifikation beschriebenen Sicherheitsfunktionen prüfen und zeigen.

Die Tests werden getrennt nach den Sicherheitsfunktionen durchgeführt und dokumentiert. Für jeden Test werden ein Testplan einschließlich Testziel erstellt, die Prozeduren zur Testdurchführung beschrieben, die erwarteten Testergebnisse definiert und die tatsächlich erzielten Ergebnisse dargestellt. Aufgeteilt auf die einzelnen Sicherheitsfunktionen bedeutet dies:

- Die Sicherheitsfunktion SF.1 (Schutz der PIN) wird vollständig mit der oben angeführten Testumgebung überprüft.

- Die Sicherheitsfunktion SF.2 (Speicherwiederaufbereitung) kann auf diese Weise nicht überprüft werden, da sie nicht über die Schnittstellen des EVG getestet werden kann. Daher wurde für die Sicherheitsfunktion SF.2 der Ansatz gewählt, sie am Entwicklungs-system des Herstellers zu testen.
- Die Sicherheitsfunktion SF.3 (Sicherer Firmwaredownload) wird vollständig mit der oben angeführten Testumgebung überprüft.

7.1.3 Umfang der durchgeführten Herstellertests

Der Hersteller hat die drei Sicherheitsfunktionen des EVG mit 48 Tests getestet. Diese Tests unterteilen sich in 39 Tests für SF.1 Schutz der PIN, 1 Test für SF.2 Speicherwiederaufbereitung und 8 Tests für SF.3 Sicherer Firmwaredownload.

Wie durch die Testabdeckungsanalyse nachgewiesen ist, hat der Hersteller den EVG systematisch auf dem Niveau der Sicherheitsfunktionalitäten aus der funktionalen Spezifikation getestet. Die Testtiefenanalyse weist außerdem nach, dass der Hersteller den EVG systematisch auf dem Niveau der Teilsysteme aus dem Entwurf auf hoher Ebene getestet hat.

7.1.4 Gesamtergebnis der Herstellertests

Der Hersteller spezifiziert zu jeder Sicherheitsfunktion funktionale Tests. Deren Ergebnisse wurden in der Testdokumentation dokumentiert. Die Testergebnisse stellten sich für alle durchgeführten Tests wie erwartet ein.

Es wurden keine Fehler entdeckt und es traten keine Abweichungen bzgl. der beschriebenen Sicherheitsfunktionalität auf. Infolgedessen konnten alle Sicherheitsfunktionen erfolgreich getestet werden.

7.2 Unabhängiges Testen durch die Prüfstelle

7.2.1 Getestete EVG Konfiguration

Vom Hersteller wurde der EVG mit der Bezeichnung ST-2000UCZ/01 geliefert und für die unabhängigen Tests der Prüfstelle einschließlich der stichprobenhaften Wiederholung von Herstellertests verwendet.

Bei dem Prüfobjekt handelt es sich um den EVG SmartTerminal ST-2xxx, der auch als solcher gekennzeichnet ist (Model St-2000, Part-No. ST-2000UCZ/01). Er steht stellvertretend für die EVG-Familie ST-2x xx x x Z -x / xx und besitzt wie in den Sicherheitsvorgaben [6] festgelegt die Firmware-Version 5.08.

Für die Tests wird der EVG an einem IBM-kompatiblen Laptop mit 32-Bit Windows Betriebssystem betrieben. Der Hersteller hat für die Tests zwei Testprogramme sowie spezielle Treibersoftware zu Testzwecken zur Verfügung gestellt. Der Evaluator verwendet außerdem ein weiteres Testprogramm, um den EVG anzusteuern. Darüber hinaus werden die Kommandos und Antworten des EVG an der USB-Schnittstellen mit einer dafür vorgesehenen Software aufgezeichnet. Die Rückgaben vom EVG werden mittels des Standardeditors NotePad kontrolliert.

Als Chipkarten werden verschiedene Prozessorchipkarten verwendet. Es handelt sich dabei um Testchipkarten mit unterschiedlichen Chipkarten-Betriebssystem und Anwendungsstrukturen, die den Signaturchipkarten der Zertifizierungsdiensteanbieter Telesec, Signtrust, Datev, D-Trust und TC-Trustcenter entsprechen sowie weitere Chipkarten nach der GSM- bzw. der Geldkarten-Spezifikation.

7.2.2 Testansatz der unabhängigen Evaluatortests

Gemäß der Teststrategie des Evaluators sollen die vorgesehenen unabhängigen Tests am EVG die Erfüllung der funktionalen Sicherheitsanforderung durch die Sicherheitsfunktionen gemäß den Sicherheitsvorgaben [6] sowie die Übereinstimmung mit den in der funktionalen Spezifikation beschriebenen Sicherheitsfunktionalitäten zeigen. Darüber hinaus sollen alle Teilsysteme und ihre Schnittstellen gemäß des Entwurfs auf hoher Ebene durch die Tests erfasst werden.

Dazu werden die Tests getrennt nach den Sicherheitsfunktionen durchgeführt und dokumentiert. Für jeden Test werden ein Testplan mit Testziel erstellt, die verwendete Testkonfiguration aufgeführt, das Testverfahren beschrieben, die erwarteten Testergebnisse definiert und die tatsächlich erzielten Ergebnisse dargestellt.

7.2.3 Umfang der durchgeführten Evaluatortests

Der Evaluator hat aus den Herstellertests der Sicherheitsfunktionen des EVG eine Stichprobe ausgewählt und getestet. Sie erfasst etwa 40 % der Herstellertests, die als 19 Testfälle formuliert wurden. Die Stichprobe des Evaluator deckt alle Sicherheitsfunktionen des EVG ab und berücksichtigt deren Charakteristika laut funktionaler Spezifikation.

Der Evaluator hat die drei Sicherheitsfunktionen des EVG mit insgesamt 40 unabhängigen Tests getestet. Davon sind 27 Tests auf SF.1 (Schutz der PIN) bezogen, 4 Tests entfallen auf SF.2 (Speicherwiederaufbereitung) sowie 9 Tests zu SF.3 (Sicherer Firmwaredownload). Diese Testfälle betreffen sowohl den normalen Ablauf der sicheren PIN-Eingabe als auch verschiedene Arten von Fehlersituationen.

Zusätzlich hat der Evaluator 30 Penetrationstests am EVG durchgeführt, die sich auf die Schwachstellenanalyse und den Missbrauch beziehen.

7.2.3 Gesamtergebnis der unabhängigen Evaluatortests

Der Evaluator spezifiziert zu jeder Sicherheitsfunktion unabhängige Tests sowie Penetrationstests zu den Prüfaspekten Schwachstellenanalyse und Missbrauch.

Die Ergebnisse dieser Tests hat der Evaluator dokumentiert und mit den erwarteten Ergebnissen verglichen. Die tatsächlichen Ergebnisse stimmten mit den erwarteten Ergebnissen überein.

Außerdem wurden Tests des Herstellers stichprobenhaft durch den Evaluator wiederholt. Auch hierbei stellten sich die erhaltenen Testergebnisse für alle durchgeführten Tests wie erwartet ein.

Fazit: Es wurden keine Fehler entdeckt und es traten keine Abweichungen bzgl. der beschriebenen Sicherheitsfunktionalität auf. Infolgedessen konnten alle Sicherheitsfunktionen erfolgreich getestet werden.

7.3 Penetrationstests

Für Penetrationstests hat der Evaluator den EVG in derselben Konfiguration verwendet, die beim unabhängige Testen zum Einsatz kam. Als Basis für die Penetrationstests dienten:

- Die Schwachstellensuche in Herstellerdokumenten und Prüfberichten
- Die Schwachstellensuche gemäß [2] und [4, (AIS 34)].

Der Evaluator hat im Rahmen der Penetrationstests des EVG die Sicherheitsfunktion SF.1 (Schutz der PIN) und die Sicherheitsfunktion SF.3 (Sicherer Firmwaredownload) auf Schwachstellen untersucht. Die Sicherheitsfunktion SF.2 (Speicherwiederaufbereitung) kann auf diese Weise nicht überprüft werden, da sie nicht über die Schnittstellen des EVG getestet werden kann.

Weiterhin hat der Evaluator die Sicherheitsmaßnahme Versiegelung des EVG auf Schwachstellen hinsichtlich der Anbringung und Positionierung der Siegel untersucht. Zusätzlich wurde vom BSI eine Kurzprüfung der Siegelmuster (Ergänzungsprüfung) durchgeführt, die gesondert dokumentiert ist. Das Siegel kann aus Sicht des BSI für die Versiegelung verwendet werden.

Mit den Penetrationstests zur Widerstandsfähigkeit des EVG gegenüber Angriffen mit hohem Angriffspotential hat der Evaluator nicht nur die vollständige und korrekte Implementierung der Sicherheitsfunktion überprüft, sondern auch nach versteckten Funktionen oder weiteren Kommandos gesucht.

7.3.1 Urteil der Testaktivitäten

Der Sicherheitsfunktionen des EVG haben sich während der Penetrationstests wie spezifiziert verhalten.

Der Sicherheitsmaßnahme zur Versiegelung des EVG hat sich während der Penetrationstests den Anforderungen entsprechend verhalten.

Die Schwachstellen sind in der beabsichtigten Einsatzumgebung des EVG nicht ausnutzbar.

Der EVG widersteht Angreifern mit hohem Angriffspotential.

8 Evaluierte Konfiguration

Die Hersteller- und Evaluatortests wurden an einem Seriengerät des EVG mit der Firmware-Version 5.08 durchgeführt. Bei den Tests wurde das Chipkartenterminal an einem IBM-kompatiblen PC-System mit 32-Bit Windows Betriebssystem betrieben.

Der Ergebnisse der Evaluierung gelten nur für die evaluierte und getestete Version des EVG:

Smart Terminal ST-2xxx, Firmware Version 5.08 des Herstellers Cherry GmbH.

Eine Übertragung der Ergebnisse der Evaluierung auf andere Versionen ist nicht möglich, sondern erfordert eine Re-Evaluierung.

9 Ergebnisse der Evaluierung

Der Evaluation Technical Report (ETR), [7] wurde von der Prüfstelle gemäß den Common Criteria [1], der Methodology [2], den Anforderungen des Schemas [3] und allen Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind, von der Prüfstelle TÜV Informationstechnik GmbH erstellt.

Die Evaluationsmethodology CEM [2] wurde für die Komponente aus dem Vertrauenswürdigkeitsstufe EAL3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4 verwendet. Für Komponenten oberhalb von EAL4

wurde die Methodology in Zusammenarbeit mit der Zertifizierungsstelle festgelegt [4, AIS 34]).

Die funktionalen Anforderungen des EVG erfüllen die in [1], Teil 2 spezifizierten funktionalen Anforderungen (CC, Part 2 conformant) .

Die Vertrauenswürdigkeitsanforderungen des EVG erfüllen die in [1], Teil 3 spezifizierten Vertrauenswürdigkeitsanforderungen (CC, Part 3 conformant).

Die Anforderungen der gewählten EVG Vertrauenswürdigkeitsklassen, d.h. alle Komponenten der Klasse ASE and alle Komponenten, die durch die Komponenten der Vertrauenswürdigkeitsstufe EAL3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 und AVA_VLA.4 definiert sind, werden erfüllt und gemäß [1] mit „PASS“ beurteilt.

Der EVG besitzt in der angenommenen Einsatzumgebung keine ausnutzbaren Schwachstellen für Angreifer mit hohem Angriffspotenzial.

Die Bewertung der Stärke der Funktionen erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten Kryptoalgorithmen (vgl. §4 Abs. 3 Nr. 2 BSIG). Dies gilt für Die EVG Sicherheitsfunktion SF3 (Sicherer Firmwaredownload)

Die Resultate der Evaluierung sind nur anwendbar auf den EVG

Smart Terminal ST-2xxx, Firmware Version 5.08 des Herstellers Cherry GmbH.

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

10 Kommentare und Auflagen

Die Dokumente [11] und [10] enthalten die notwendigen Informationen über die Verwendung des EVG. Alle Sicherheitshinweise sind darin enthalten.

Die Sicherheitsfunktion SF.3 (Sicherer Firmwaredownload) ist im EVG implementiert und getestet worden. Damit bietet das Gerät Schutz vor dem unzulässigen Aufladen von schadhafter Firmware. Da der Hersteller allerdings die Firmware separat von der Hardware nicht zur Verfügung stellt, konnte der Auslieferungsprozess von Firmware allein nicht evaluiert werden. Daher ist der Auslieferungsprozess von Firmware allein **nicht Bestandteil des Zertifikats**. Soll es dem Benutzer möglich sein, zertifizierte Firmware separat vom Gerät vom Hersteller zu erhalten und auf das Chipterminal aufzuspielen, so ist dafür eine Re-Zertifizierung notwendig.

Die Sicherheitsfunktion SF.3 (Sicherer Firmwaredownload) stützt sich im wesentlichen auf die Algorithmen RSA-1024 und SHA-1 ab. Gemäß der von der Bundesnetzagentur veröffentlichten Übersicht über geeignete Algorithmen [17] ist der RSA-Algorithmus mit einer Länge von 1024 Bit nur bis Ende 2007 zur Erfüllung der Anforderungen nach §17, Abs. 1-3 des SigG [8] geeignet. Sind die Algorithmen gemäß der Einstufung der Bundesnetzagentur nicht mehr geeignet, ist die geforderte Funktionsstärke SOF-hoch nicht mehr gewährleistet. Damit das Chipkartenterminal ST-2xxx auch nach diesem Zeitpunkt für qualifizierte elektronische Signaturen eingesetzt werden kann, ist eine entsprechende Verstärkung der gewählten Mechanismen im Rahmen einer Re-Evaluierung vor Ablauf der Gültigkeit der Algorithmen notwendig.

11 Anhänge

Keine.

12 Sicherheitsvorgaben

Die Sicherheitsvorgaben [6] sind Bestandteil dieses Zertifizierungsreports. Zum Zwecke der Veröffentlichung werden sie in einem separaten Dokument bereitgestellt.

13 Definitionen

13.1 Abkürzungen

APDU Application Programming Data Unit

BSI Bundesamt für Sicherheit in der Informationstechnik, Bonn, Deutschland

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

CCID Chip Card Interface Devices

CT Card Terminal

EAL Evaluation Assurance Level – Vertrauenswürdigkeitsstufe

EVG Evaluationsgegenstand

HBCI Homebanking Computer Interface

ICC Integrated Chipcard – integrierte Chipkarte

ISO International Organization for Standardization

IT Informationstechnik

LED Light Emitting Diode – Leuchtdiode

PC Personal Computer

PC/SC Personal Computer/ SmartCard

PIN Persönliche Identifikationsnummer

PP Protection Profile - Schutzprofil

SF Sicherheitsfunktion

SigG Signaturgesetz

SigV Signaturverordnung

SOF Strength of Function - Stärke der Funktionen

ST Security Target - Sicherheitsvorgaben

SM Sicherheitsmaßnahme

TSC TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle

TSF TOE Security Functions - EVG-Sicherheitsfunktionen

TSP TOE security policy - EVG-Sicherheitspolitik

USB Universeller serieller Bus

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-0309-2006, Version 1.07, 23.12.2005 , Common-Criteria-Dokument Sicherheitsvorgaben EAL3+ SmartTerminal ST-2xxx, Cherry GmbH

[7] Evaluierungsbericht, Version 1.8, 18.01.2006, Technischer Evaluierungsbericht (ETR) CC Evaluierung des SmartTerminal ST-2xxx (vertrauliches Dokument)

[8] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) in der Fassung vom 16.05.2001 (BGBl. Jahrgang 2001 Teil I Nr. 22 S. 876)

[9] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) in der Fassung vom 16.11.2001 (BGBl. Jahrgang 2001 Teil I Nr. 59 S. 3074)

[10] Quick-Start Instructions SmartTerminal ST-2000U, Version 03 vom Dezember 2005, herausgegeben von der Cherry GmbH

[11] Betriebsdokumentation „AGD“ 644-0417-01 DE, Version 009 vom 23.12.2005, herausgegeben von der Cherry GmbH

[12] Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00, March 20, 2001

[13] DIN ISO 7816 - 1 Identification cards - Integrated circuit(s) cards with contacts – Physical Characteristics

DIN ISO 7816 - 2 Identification cards - Integrated circuit(s) cards with contacts - Dimensions and locations of the contacts

DIN ISO 7816 - 3 Identification cards - Integrated circuit(s) cards with contacts - electrical characteristics and transmission protocols

DIN ISO 7816 - 4 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Inter - industry commands for interchange

DIN ISO 7816 – 8 Identification cards – Integrated circuit(s) cards with contacts – Security related interindustry commands

[14] EMV 2000 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.0, December 2000

[15] Anwendungsunabhängiges CardTerminal Application Programming Interface (CT-API) für Chipkartenanwendungen, Revision 1.1, 14. 10. 1998

[16] Interoperability Specification for ICCs and Personal Computer Systems, PC/SCWorkgroup, Version 1.0, Dezember 1997

[17] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 02. Januar 2005, veröffentlicht am 30. März 2005 im Bundesanzeiger Nr. 59, S. 4695-4696

Dies ist eine eingefügte Leerseite.

C Auszüge aus den technischen Regelwerken

CC Teil 1:

Kennzeichnung der Evaluationsergebnisse (Kapitel 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 2.1 -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 6.1 - 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.“

Dies ist eine eingefügte Leerseite.