Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0477-2007

zu

SmartTerminal ST-2xxx
Firmware Version 5.11

der

Cherry GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Hotline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0477-2007

Chipkartenterminal
SmartTerminal ST-2xxx
Firmware Version 5.11

von Cherry GmbH

Funktionalität: Produktspezifische Sicherheitsvorgaben; Common Criteria Teil 2 konform

Vertrauenswürdigkeit:
Common Criteria Teil 3 konform
EAL 3 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

Common Criteria Recognition Arrangement für Komponenten bis EAL4

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle nach der Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 und Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL 4 unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005) evaluiert.

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.

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.

Bonn, 15. Oktober 2007

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

IT Security Certified

SOGIS - MRA

Irmela Ruhrmann L.S.
Fachbereichsleiterin

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Dies ist eine eingefügte Leerseite.

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) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3[5]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)
- Hinweise der Zertifizierungsstelle zur Methodologie für Vertrauenswürdigkeitskomponenten oberhalb von EAL 4 (AIS 34)

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.

2.1 Europäische Anerkennung von ITSEC/CC - Zertifikaten

Ein Abkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten, auf deren Grundlage ITSEC-Zertifikate für IT-Produkte unter gewissen Bedingungen anerkannt werden, ist im März 1998 in Kraft getreten (SOGIS-MRA).

Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen,

---

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 Informati-onstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

5 Bekanntmachung des Bundesministeriums des Innern vom 10. Mai 2006 im Bundesanzeiger, datiert 19. Mai 2006, S. 19445

Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Evaluationsstufe EAL7 erweitert. Das BSI erkennt die Zertifikate der nationalen Zertifizierungsstellen von Frankreich und Großbritannien im Rahmen dieses Abkommens an.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens anerkannt wird.

2.2 Internationale Anerkennung von CC - Zertifikaten

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 verabschiedet (CC-MRA).

Der Vereinbarung sind bis Februar 2007 die nationalen Stellen folgender Nationen beigetreten: Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Republik Korea, Neuseeland, Niederlande, Norwegen, Österreich, Schweden, Spanien, Republik Singapur, Tschechische Republik, Türkei, Ungarn, USA.

Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite http://www.commoncriteriaportal.org eingesehen werden.

Das Common Criteria-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens anerkannt wird.

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 EAL4-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 SmartTerminal ST-2xxx Firmware Version 5.11 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-0309-2006.

Die Evaluation des Produkts SmartTerminal ST-2xxx Firmware Version 5.11 wurde von TÜV Informationstechnik GmbH durchgeführt. Die Evaluierung wurde am 31.07.2007 beendet. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Hersteller und Antragsteller ist: Cherry GmbH

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

[6] Information Technology Security Evaluation Facility

4 Gültigkeit des Zertifikats

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes.

Das Produkt ist nur unter den folgenden Bedingungen konform zu den bestätigten Vertrauenswürdigkeitskomponenten:

- alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des EVG, die in diesem Report gestellt werden, werden beachtet.
- das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben beschrieben ist.

Die Bedeutung der Vertrauenswürdigkeitsstufen und die Stärke der Funktionen werden in den Auszügen aus dem technischen Regelwerk am Ende des Zertifizierungsreports erläutert.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da Angriffe mit neuen oder weiterentwickelten Methoden in Zukunft möglich sind, besteht die Möglichkeit, die Widerstandsfähigkeit des Produktes im Rahmen des Assurance Continuity-Programms des BSI regelmäßig überprüfen zu lassen. Die Zertifizierungsstelle empfiehlt, regelmäßig eine Einschätzung der Widerstandsfähigkeit vornehmen zu lassen.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d.h. eine Re-Zertifizierung oder ein Maintenance Verfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

5 Veröffentlichung

Das Produkt SmartTerminal ST-2xxx Firmware Version 5.11 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes angefordert werden[7]. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

[7] Cherry GmbH
Cherrystraße
91275 Auerbach

B Zertifizierungsbericht

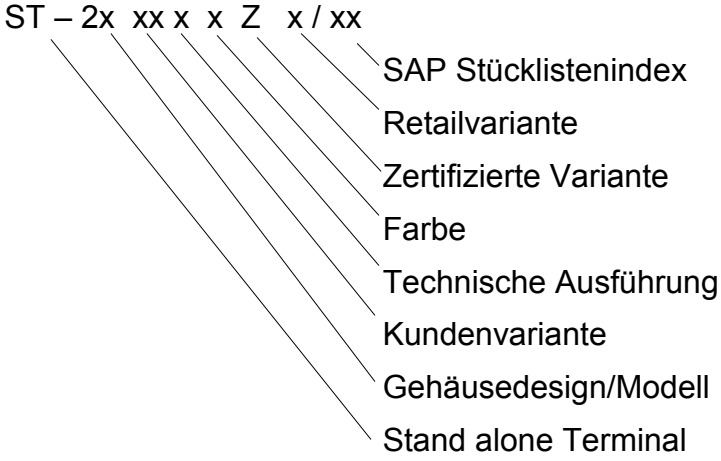
Der nachfolgende Bericht ist eine Zusammenfassung aus

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

1 Zusammenfassung

Der Evaluationsgegenstand (EVG) ist der universelle Chipkartenleser mit Keypad der Famile SmartTerminal ST-2xxx mit der Firmware-Version 5.11 des Herstellers Cherry GmbH.

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



Die Bedeutung der einzelnen Bestandteile der Kennzeichnung ist:

SAP Stücklistenindex:

Versionsnummer von 00 – 99 entsprechend der SAP Stückliste.

Retailvariante:

R wenn als Retailvariante ausgeführt; ansonsten kein Kennzeichen

Zertifizierte Variante:

Z wenn als zertifizierte und bestätigte Variante ausgeführt; ansonsten entfällt Kennzeichen

Farbe :

Buchstaben von A – Z, hier C – Gehäuseoberteil: grau, Gehäuseunterteil: Druckguß blau chromatiert

Technische Ausführung:

Buchstaben von A – Z, hier U – USB - Stecker

Kundenvarianten:

Nummer von 00 – 43, hier 00 – Standard

Gehäusedesign/Modell:

20 Chipkartenleser mit 16er Tastenfeld

Der EVG besitzt die Möglichkeit, mit kontaktbehafteten Speicher- und Prozessorchipkarten zu kommunizieren. Bei synchronen Chipkarten (Speicherchipkarten) werden Übertragungsprotokolle nach herstellerspezifischen Spezifikationen unterstützt. Für Prozessorkarten werden die Übertragungsprotokolle T=0 und T=1 angeboten. Prozessorkarten müssen die Spezifikationen [16] bzw. [17] erfüllen.

Propagiertes Ziel des EVG ist es, das Kartenterminal für Anwendungen zur Erzeugung von qualifizierten elektronischen Signaturen nach dem deutschen Signaturgesetz [12] 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 die Möglichkeit, die Firmware mit einer neuen Version zu aktualisieren und somit dem Endkunden einen größeren Investitionsschutz für sein Gerät zu gewähren. 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.

Der Benutzer darf für die Verwendung des Gerätes im Bereich der qualifizierten elektronischen Signatur nur solche Firmware aufspielen, die vom Hersteller als bestätigt und zertifiziert auf der Internetseite http://support.cherry.de gekennzeichnet ist und von dort heruntergeladen werden kann.

Die Sicherheitsfunktionen des EVG wurden so gewählt, dass den Sicherheitszielen des deutschen Signaturgesetzes [12] bzw. der Signaturverordnung [13]

- Keine Preisgabe oder Speicherung der Identifikationsdaten (§15 Abs. 2 Nr. 1a [13])
- Erkennbarkeit sicherheitstechnischer Veränderungen (§15 Abs. 4 [13])

entsprochen wird.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie verwenden kein zertifiziertes Protection Profile.

Die Vertrauenswürdigkeitskomponenten (Security Assurance Requirements SAR) sind dem Teil 3 der Common Criteria entnommen (siehe Teil C oder [1], Teil 3). Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6], Kapitel 5.1 beschrieben. Sie wurden komplett dem Teil der Common Criteria entnommen. Der EVG ist daher konform zum Teil 2 der Common Criteria.

Funktionalen Sicherheitsanforderungen für die IT-Umgebung des EVG sind in den Sicherheitsvorgaben [6] nicht enthalten.

Die funktionalen Sicherheitsanforderungen werden durch die folgenden Sicherheitsfunktionen des EVG umgesetzt:

Sicherheitsfunktion des EVG	Thema
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, ob es sich um ein PIN-Kommando handelt, welches explizit eine PIN-Eingabe

Sicherheitsfunktion des EVG	Thema
	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 APDU's. 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, dem Ziehen der Chipkarte oder dem Abbruch der PIN-Eingabe 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 Firmwaredownload (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 1: Sicherheitsfunktionen des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 6.1 dargestellt.

Die in den Sicherheitsvorgaben [6], Kapitel 8.2 für bestimmte Funktionen angegebene Stärke der Funktionen “hoch” wird bestätigt.

Die Bewertung der Stärke der Funktionen erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten Kryptoalgorithmen (vgl. §4 Abs. 3 Nr. 2 BSIG). Für Details siehe Kap. 9 dieses Berichtes.

Die Werte, die durch den TOE geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3 dar.

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 Evaluierungsgegenstand (EVG) heißt::

SmartTerminal ST-2xxx Firmware Version 5.11

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Datum	Auslieferungsart
1	HW	SmartTerminal ST-2xxx	ST-2x xx x x Z - x		In Einzelverpackung
2	SW	Firmware für den Chipkartenlese	5.11		● Zusammen mit der Hardware ● Über die Webseite http://support.cherry.de
3	DOC	Instructions SmartTerminal ST-2000U	644-0411.02 DE, US, FR	Dezember 2005	● PDF-Dokument auf der Installations-CD ● Papier als Beilage zur Hardware ● Download von der Webseite www.cherry.de
4	DOC	Betriebsdokumentation „AGD“ Common Criteria	644-0417.02 DE	Juli 2007	● PDF-Dokument auf der Installations-CD ● Papier als Beilage zur Hardware ● Download von der Webseite www.cherry.de
5	DOC	Benutzeranleitung für Firmware Upgrade auf V 5.11 SmartTerminal ST-2xxx	1.00		● PDF-Dokument auf der Installations-CD ● Download von der Webseite www.cherry.de

Tabelle 2: Auslieferungsumfang des EVG

Der EVG wird auf zwei verschiedene Arten ausgeliefert:

- Komplett als Chipkartenlesegerät in Einzelverpackung zusammen mit einer Installations-CD (nicht Umfang der Evaluierung), wobei die Positionen 1-4 der Tabelle 2 an den Kunden ausgeliefert werden. Der Kunde kann das Chipkartenlesegerät eindeutig an der Kennung ST-2x xx x x Z – x erkennen, wobei „Z“ wie oben beschrieben auf die zertifizierte Variante hinweist.
- Als Firmware von der Internetseite http://support.cherry.de. Hierbei lädt der Kunde die Firmware (Position 2 in Tabelle 2), die Benutzeranleitung zum Firmware-Upgrade (Position 5 in Tabelle 2) und Software zum Aufspielen der neuen Firmware sowie zum Auslesen der Version der vorhandenen Firmware (nicht im Evaluierungsumfang enthalten) herunter.

3 Sicherheitspolitik

Es ist ein erklärtes Ziel, den EVG für die Applikation „digitale Signatur“ nach dem deutschen Signaturgesetz [12] einzusetzen. Um ein elektronisches Dokument mit einer qualifizierten elektronischen Signatur zu versehen, 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

Die Annahmen in den Sicherheitsvorgaben sowie Teile der Bedrohungen und organisatorischen Sicherheitspolitiken werden nicht durch den EVG selbst abgedeckt. Diese Aspekte setzen voraus, dass bestimmte Sicherheitsziele durch die EVG-Einsatzumgebung erfüllt werden. Hierbei sind die folgenden Punkte relevant:

- Der TOE muss als Kartenterminal für die nichtöffentliche Umgebung eingesetzt werden.
- Der Anwender darf ausschließlich Prozessorkarten benutzen, die den Spezifikationen [16] bzw. [17] genügen.
- Der Anwender muss bei der Benutzung des Geräts gewisse Vorgaben beachten. Dazu gehören eine Überprüfung des Sicherheitssiegels, eine unbeobachtete Eingabe der PIN über das Keypad ausschließlich im Modus der sicheren PIN-Eingabe sowie eine Überprüfung der korrekten Firmware-Version.
- Bei einem Upgrade der Firmware muss sich der Anwender davon übezeugen, dass er zertifizierte und bestätigte Firmware auf sein Chipkartenlesegerät aufspielt.

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4 sowie in der Benutzerdokumention [9] - [11].

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 Secure Download" 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 implementiert die Sicherheitsfunktionen SF.1 (Schutz der PIN) und SF.2 (Speicherwiederaufbereitung). 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:

  Im Subsystem TSS6 ist die Sicherheitsfunktion SF3. (Firmwaredownload) implementiert.

6 Dokumentation

Die evaluierte Dokumentation, die in Tabelle 2 aufgeführt ist, wird zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem EVG in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des EVG, die im Kapitel 10 enthalten sind, müssen befolgt werden.

7 Testverfahren

Gemäß der gewählten Prüftiefe EAL3 mit Zusatz wurden umfangreiche Tests sowohl durch Hersteller als auch durch die Prüfstelle durchgeführt. Es wurden keine Fehler entdeckt und es traten keine Abweichungen bzgl. der beschriebenen Sicherheitsfunktionalität auf. Infolgedessen konnten alle Sicherheitsfunktionen erfolgreich getestet werden.

7.1 Herstellertests

Der Hersteller hat die drei Sicherheitsfunktionen des EVG getestet. Wie durch die Testabdeckungsanalyse nachgewiesen ist, hat der Hersteller den EVG systematisch auf dem Niveau der funktionalen Spezifikation und der Teilsysteme getestet.

Die Testergebnisse wurden in der Testdokumentation dokumentiert. Alle Testergebnisse stellten sich für die 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 Unabhängige Tests der Prüfstelle

Der Evaluator spezifiziert zu jeder Sicherheitsfunktion unabhängige Tests. Deren Ergebnisse wurden im Einzelprüfbericht zu den Prüfstellentests dokumentiert. 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.

7.3 Penetrationstests der Prüfstelle

Der Evaluator spezifizierte Penetrationstests zu den Prüfaspekten Schwachstellenanalyse und Missbrauch. Deren Ergebnisse wurden gemäß den Anforderungen der Common Criteria dokumentiert. Die tatsächlichen Ergebnisse stimmten mit den erwarteten Ergebnissen überein.

8 Evaluierte Konfiguration

Der EVG kann nur in einer Konfiguration betrieben werden. Das Zertifikat bezieht sich daher auf das Chipkartenlesegerät SmartTerminal ST-2xxx mit der Firmware Version 5.11.

9 Ergebnis der Evaluierung

9.1 CC spezifische Ergebnisse

Der Evaluierungsbericht [7] (Evaluation Technical Report, ETR) wurde von der Prüfstelle gemäß den Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005) [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen Anwendungshinweisen und Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind. Die Evaluierungsmethodologie CEM [2] wurde für die Komponenten bis zur Vertrauenswürdigkeitsstufe EAL3 verwendet. Darüber hinaus wurde die in der AIS 34 [4] definierte Methodologie verwendet**.**

Das Urteil PASS der Evaluierung wird für die folgenden Vertrauenswürdigkeitskomponenten bestätigt:

- Alle Komponenten der Klasse ASE
- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL3 der CC (siehe auch Teil C des Zertifizierungsreports)

- Die Komponenten
  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

Da die Evaluierung eine Re-Evaluierung zum Zertifikat BSI-DSZ-CC-0309-2006 darstellt, konnten bestimmte Evaluierungsergebnisse wiederverwendet werden. Diese Re-Evaluierung konzentrierte sich insbesondere auf die Anpassung von PIN-Kommandos und eine verbesserte Unterstützung bestimmter Kartenterminal-Treiber.

Die Evaluierung hat gezeigt:

- Funktionalität: Produktspezifische Sicherheitsvorgaben
  Common Criteria Teil 2 konform
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL 3 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

Die Ergebnisse der Evaluierung gelten nur für den EVG gemäß Kapitel 2 und für die Konfigurationen, die in Kapitel 8 aufgeführt sind.

9.2 Ergebnis der kryptographischen Bewertung

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

(i) Die EVG Sicherheitsfunktion SF3 (Sicherer Firmwaredownload) .

10 Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 2 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des EVG und alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind die folgen Auflagen und Hinweise zu beachten:

Die Sicherheitsfunktion SF.3 (Sicherer Firmwaredownload) stützt sich im wesentlichen auf die Algorithmen RSA-1024 und SHA-1. Gemäß der von der Bundesnetzagentur veröffentlichten Übersicht über geeignete Algorithmen [14] ist der RSA-Algorithmus mit einer Länge von 1024 Bit nur bis Ende 2007 für die Erstellung von qualifizierten Signaturen – und damit auch für die hier verwendete elektronische Signatur – geeignet. Über diesen Zeitraum hinaus liegen keine Aussagen hinsichtlich der Algorithmenstärke vor. Es wird empfohlen, im Rahmen einer Re-Evaluierung längere Schlüssel einzuführen, die auch für qualifizierte elektronische Signaturen geeignet sind.

11 Sicherheitsvorgaben

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

12 Definitionen

12.1 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

12.2 Glossary

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

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.

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.

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 Anwenderbedürfnisse erfüllen.

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

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.

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.

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-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.

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.

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

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

13 Literaturangaben

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 - Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005)

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005 - Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3

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

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind [8].

[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-0477-2007, Version 1.00, 22.05.2007, Common-Criteria-Dokument Sicherheitsvorgaben EAL3+, Cherry GmbH

[7] Evaluierungsbericht, Version 1, 31.07.2007, EVALUATION TECHNICAL REPORT (ETR), TÜVIT GmbH (vertrauliches Dokument)

[8] Konfigurationsliste für den EVG, Version 1.03, 10.07.2007, Common-Criteria-Dokument Konfigurationsliste (vertrauliches Dokument)

[9] Instructions SmartTerminal ST-2000U, Version 644-0411.02 DE, US, FR, Dezember 2005, Cherry GmbH

[10] Betriebsdokumentation „AGD“ Common Criteria, Version 644-0417.02 DE, Juli 2007, Cherry GmbH

[11] Benutzeranleitung für Firmware Upgrade auf V 5.11 SmartTerminal ST-2xxx,Version 1.0, Cherry GmbH

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

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

[14] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 22.02.2007, veröffentlicht am 12.04.2007 im Bundesanzeiger Nr. 69 S. 3759

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

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

[8] Inbesondere:

- AIS 34, Version 1.00, 1 Juni 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

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

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

Dies ist eine eingefügte Leerseite.

C Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 2.3 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part1:

Conformance results (chapter 7.4)

„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 CC Part 2 (functional requirements), CC 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:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC 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 Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
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)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 CC 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 11.1)

“Table 6 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 7 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 standard 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: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 11.4)

“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 11.5)

“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 11.6)

“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 11.7)

“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 11.8)

“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 11.9)

“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 19.3)

“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 19.4)

"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 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

D Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Die Sicherheitsvorgaben werden in einem eigenen Dokument zur Verfügung gestellt.

Dies ist eine eingefügte Leerseite.