



Zertifizierungsreport

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0280-2004

zu

Chipkartenterminalfamilie

KBPC CX / CX Top:

S26381-K329-V1xx HOS:02,

S26381-K329-V4xx HOS:01,

S26381-K339-V1xx HOS:01,

Firmware-Version 1.04

der

Fujitsu Siemens Computers GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455



Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik



Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0280-2004

Chipkartenterminalfamilie KBPC CX / CX Top
S26381-K329-V1xx HOS:02, S26381-K329-V4xx HOS:01,
S26381-K339-V1xx HOS:01,
Firmware-Version 1.04

der

Fujitsu Siemens Computers GmbH



Sogis MRA

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

Prüfergebnis:

Funktionalität: **produktspezifische Sicherheitsvorgaben
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 (xx dient als Platzhalter für verschiedene Ländervarianten) des Produktes 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 16. Dezember 2004

Der Vizepräsident des Bundesamtes für
Sicherheit in der Informationstechnik

Hange

L.S.



Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

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

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG¹ 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

Teil A: Zertifizierung

Teil B: Zertifizierungsbericht

Teil C: Auszüge aus den technischen Regelwerken

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

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

- BSIG²
- BSI-Zertifizierungsverordnung³
- BSI-Kostenverordnung⁴
- 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 2.1⁵
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM)
 - Teil 1, Version 0.6
 - Teil 2, Version 1.0
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)

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

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

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

⁴ Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 29. Oktober 1992, Bundesgesetzblatt I S. 1838

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.

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.

Die Produktfamilie Chipkartenterminal KBPC CX / CX Top, Firmware-Version 1.04⁶ hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation der Produktfamilie Chipkartenterminal KBPC CX / CX Top wurde von der Prüfstelle für IT- Sicherheit der TÜV Informationstechnik GmbH durchgeführt. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)⁷.

Antragsteller und Hersteller ist die Fujitsu Siemens Computers GmbH.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 16.12.2004 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 Zertifizierungsreport 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 Im Weiteren Chipkartenterminal KBPC CX / CX Top genannt.

⁷ Information Technology Security Evaluation Facility

4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-20.

Die Produktfamilie Chipkartenterminal KBPC CX / CX Top 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 Hersteller⁸ des Produktes angefordert werden. Unter der o. g. Internetadresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

⁸ Fujitsu Siemens Computers GmbH, Bürgermeister- Ulrich- Straße 100, D-86199 Augsburg

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..... | 3 |
| 2 | Identifikation des EVG..... | 9 |
| 3 | Sicherheitspolitik | 9 |
| 4 | Annahmen und Klärung des Einsatzbereiches | 10 |
| 5 | Informationen zur Architektur | 11 |
| 6 | Dokumentation..... | 11 |
| 7 | Testverfahren..... | 12 |
| 8 | Evaluierte Konfiguration..... | 14 |
| 9 | Ergebnisse der Evaluierung | 14 |
| 10 | Kommentare und Empfehlungen..... | 16 |
| 11 | Anhänge..... | 16 |
| 12 | Sicherheitsvorgaben..... | 16 |
| 13 | Definitionen..... | 17 |
| 14 | Literaturangaben | 19 |

1 Zusammenfassung

Beim Evaluationsgegenstand Chipkartenterminalfamilie KBPC CX / CX Top handelt es sich um USB-Tastaturen mit integriertem Chipkartenterminal des Herstellers Fujitsu Siemens Computers GmbH einschließlich der Firmware in Version 1.04. Die USB-Schnittstelle stellt die physikalische und logische Grenze des EVG zum PC-System dar. Die Treibersoftware gehört nicht zum Evaluationsumfang.

Der Evaluationsgegenstand gliedert sich dabei in verschiedene Produktvarianten mit der gleichen zu evaluierenden Firmware 1.04, welche die folgenden Bezeichnungen besitzen:

- Variante 1a: KBPC CX: **S26381-K329-V1xx HOS:02**
Tastatur mit Kartenschlitz von der rechten Seite, Farbe bright light grey
- Variante 1b: KBPC CX: **S26381-K329-V4xx HOS:01**
Tastatur mit Kartenschlitz von der rechten Seite, Farbe anthrazit
- Variante 2: KBPC CX Top: **S26381-K339-V1xx HOS:01**
Tastatur mit Kartenschlitz von oben, Farbe bright light grey

Die Platzhalter xx kennzeichnen die Tastaturbeschriftung (Länderangabe).

Der EVG besitzt neben der Funktion als normale PC-Tastatur mittels des eingebauten Chipkartenlesers die Möglichkeit, kontaktbehafte Speicher- und Prozessorchipkarten zu verarbeiten. Bei synchronen Chipkarten (Speicherchipkarten) werden Übertragungsprotokolle nach herstellereinspezifischen Spezifikationen unterstützt. Für Prozessorkarten werden die Übertragungsprotokolle T=0 und T=1 angeboten. Prozessorkarten müssen den Spezifikationen [ISO 7816] bzw. [EMV 2000] genügen.

Ziel ist es, den EVG für Anwendungen zur Erzeugung qualifizierter elektronischer Signaturen nach dem deutschen Signaturgesetz [SigG] einzusetzen. Dazu wird für Prozessorkarten die Funktion der sicheren PIN-Eingabe über den Nummernblock der Tastatur vom EVG unterstützt. Für Speicherchipkarten steht eine solche Funktion der sicheren PIN-Eingabe nicht zur Verfügung.

Der Evaluationsgegenstand ist für den universellen Einsatz in chipkartenbasierenden Applikationen ohne vorherige Authentisierung geeignet. Mögliche Anwendungen sind: Digitale Signatur, Homebanking (HBCI), Access Control (PC), Internet Shopping. Bei der Anwendung „qualifizierte elektronische Signatur“ dürfen ausschließlich im Sinne des SigG [6] und SigV [7] bestätigte Chipkarten und bestätigte Signaturanwendungsprogramme bzw. herstellere erklärte Signaturanwendungsprogramme verwendet werden.

Der Einsatz des EVG ist für nichtöffentliche Umgebungen zugelassen (Single- und MultiUser-PC im privaten Bereich und in der Büroumgebung). Unter nichtöffentlicher Umgebung fallen alle Bereiche, die nicht für die Allgemeinheit (Öffentlichkeit) zugänglich sind.

Die Sicherheitsanforderungen an den Evaluationsgegenstand werden durch die folgenden Sicherheitsfunktionen abgedeckt:

- Speicherwiederaufbereitung:

Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos, dem Entfernen der Chipkarte oder dem Abbruch über die Tastatur wird der PIN-Speicherbereich wiederaufbereitet und die LED-Anzeige der sicheren PIN- Eingabe ausgeschaltet.

- Schutz der PIN:

Das Umschalten des Nummernblocks in den sicheren PIN-Eingabemodus wird durch ein explizites CT-Kommando nach CCID durchgeführt. Dieses CT- Kommando enthält eine PIN-Handlingsvereinbarung und das Chipkartenkommando, welches die PIN in eine spezifizierte Stelle integriert. Anhand des CT-Kommando-Instructionbytes wird überprüft, ob es sich um ein PIN-Kommando handelt, welches eine PIN-Eingabe erwartet. Im PIN-Eingabemodus werden die persönlichen Identifikationsdaten im RAM zwischengespeichert um sie nach erfolgreichem Abschluss der Eingabe direkt mit dem PIN- Kommando zur Karte zu senden. Der PIN-Eingabemodus wird optisch durch rotes Blinken der PIN-LED angezeigt bis die PIN vollständig ist bzw. der Vorgang abgebrochen wird. Zum Abbruch zählen das Herausziehen der Karte, Betätigen der Abbruchtaste und das Überschreiten der definierten Eingabezeit. Der Eingabefortschritt wird dem System mittels der Übertragung eines Dummycodes mitgeteilt. Die PIN wird nur zur Chipkarte übertragen bzw. abgefragt, wenn das richtige CT-Kommando nach CCID und das richtige Chipkartenkommando nach ISO 7816 und EMV 2000 vorhanden sind.

Um sicherheitsrelevante Veränderungen am Evaluationsgegenstand für den Nutzer erkennbar werden zu lassen, sind über der Trennkannte zwischen Gehäuseoberteil und –unterteil authentische, fälschungssichere Siegel (Sicherheitsmaßnahme) angebracht. Ein Öffnen des Gehäuses ist ohne die Beschädigung der Siegel nicht möglich. Eine detaillierte Beschreibung und eine Abbildung des Siegels werden dem Nutzer in der mitgelieferten Betriebsdokumentation zugänglich gemacht.

Die Evaluation der Produktfamilie Chipkartenterminal KBPC CX / CX Top wurde von der Prüfstelle für IT- Sicherheit der TÜV Informationstechnik GmbH durchgeführt und am 09.11.2004 abgeschlossen. Das Prüflabor der TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)⁹.

⁹ Information Technology Security Evaluation Facility

Antragsteller und Hersteller ist Fujitsu Siemens Computers GmbH.

1.1 Vertrauenswürdigkeitspaket

Die Produktfamilie Chipkartenterminal KBPC CX / CX Top wurde erfolgreich nach den Common Criteria (CC) mit der Prüfstufe EAL3+ (EAL3 mit Zusatz¹⁰ : ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4) evaluiert.

Nachfolgende Tabelle enthält eine detaillierte Auflistung aller Anforderungen an die Vertrauenswürdigkeit des EVG:

| Klasse | Familie | Komponente |
|------------------------------------|-----------|---|
| Evaluation der Sicherheitsvorgaben | ASE_DES.1 | Beschreibung des TOE |
| | 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 |
| | ASE_TSS.1 | TOE- Übersichtsspezifikation |
| Konfigurationsmanagement | ACM_CAP.3 | Autorisierungskontrolle |
| | ACM_SCP.1 | TOE- 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 |
| Schwachstellenbewertung | AVA_MSU.3 | Analysieren und Testen auf unsichere Zustände |
| | AVA_SOF.1 | Stärke der TOE-Sicherheitsfunktionen |
| | AVA_VLA.4 | Hohe Widerstandsfähigkeit |

¹⁰ Gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 1 SigV [7].

1.2 Funktionalität

Propagiertes Ziel des EVG ist es, das Kartenterminal für Anwendungen zur Erzeugung nach dem deutschen Signaturgesetz (SigG) [6] einzusetzen. Dazu wird für Prozessorchipkarten die Funktion der sicheren PIN-Eingabe über den Nummernblock der Tastatur vom EVG unterstützt.

Der EVG ist für den Einsatz im nichtöffentlichen Bereich, wie den privaten Bereich oder die normale Büroumgebung mit geregelten Zugriffsmöglichkeiten vorgesehen. Er bietet Schutz gegen Angreifer mit hohem Angriffspotential. Der Benutzer wird in die Lage versetzt, die Unversehrtheit des EVG anhand seiner Versiegelung zu überprüfen.

Der EVG besitzt zwei Sicherheitsfunktionen und eine Sicherheitsmaßnahme. Diese werden in den folgenden Tabellen zusammengefasst:

| Sicherheitsfunktion | Beschreibung |
|-----------------------------------|---|
| Speicherwiederaufbereitung (SF.1) | <i>Die Kommunikation zwischen PC-System und Chipkarte basiert gemäß CCID 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 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.</i> |
| Schutz der PIN (SF.2) | <i>Das Umschalten des Nummernblocks im Kartenterminal in den sicheren PIN-Eingabemodus wird durch ein explizites CT-Kommando nach CCID durchgeführt. Dieses CT-Kommando enthält die PIN Handlingsvereinbarungen und das Chipkartenkommando, in welches die PIN an die spezialisierte Stelle integriert wird. Anhand des Instructionbytes des Chipkartenkommandos wird überprüft, ob es sich um ein PIN Kommando handelt, welches explizit eine PIN-Eingabe erwartet. Der PIN- Eingabemodus wird optisch durch rotes Blinken der PIN- LED angezeigt bis die PIN vollständig ist bzw. der Vorgang abgebrochen wird.</i> |
| Sicherheitsmaßnahme | Beschreibung |
| Versiegelung (SM.1) | <i>Anhand authentischer und fälschungssicherer Sicherheitssiegel, die im Rahmen der BSI 7500 Druckschrift „Produkte für die materielle Sicher-</i> |

| | |
|--|--|
| | <p><i>heit für die Sicherheitsstufe 2“ gelistet sind und die über die Trennkante zwischen Gehäuseunter- und -oberteil geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden. Dies wird dadurch sichergestellt, dass die Versiegelung nicht unbeschädigt entfernt und wieder aufgeklebt werden kann und ein Öffnen des EVG nicht ohne Beschädigung des Siegels möglich ist.</i></p> |
|--|--|

1.3 Stärke der Funktionen

Für den EVG gelten keine funktionalen Sicherheitsanforderungen, für die eine Betrachtung der Stärke (SOF) in Frage kommt.

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

- Bedrohungen

Alle Bedrohungen gehen von einem Angreifer mit einem hohen Angriffspotential 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 Sniffer-tools (Hardware oder Software) die über den TOE 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 TOE in seinen Bestandteilen (Hardware und Firmware) zu manipulieren, um die PIN zu ermitteln. |
| T.3b | Ein Angreifer könnte versuchen, die im TOE zwischengespeicherte PIN auszulesen. |
| T.4 | Ein Angreifer könnte versuchen, die PIN in einen ungeschützten Bereich der Chipkarte zu schreiben, um sie anschließend daraus auszulesen |
| T.5 | Ein Angreifer könnte versuchen, durch Manipulation des Sicherheitssiegels sicherheitstechnische Veränderungen am TOE vorzunehmen. |

- Organisatorische Sicherheitspolitiken sind nicht vorgesehen.

1.5 Spezielle Konfigurationsanforderungen

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

USB-Tastatur mit integriertem Chipkartenterminal der Familie KBPC CX / CX Top mit der Firmware-Version 1.04 des Herstellers Fujitsu Siemens GmbH.

Die Installation und Inbetriebnahme des EVG ist in der, der Lieferung in Papierform beiliegenden, Betriebsdokumentation [10] 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.

1.6 Annahmen über die Einsatzumgebung

Der Einsatz des EVG ist für Single und Multi- User Systeme im nicht öffentlichen Bereich, also in einer privaten Umgebung oder normalen Büro-umgebung zugelassen.

Der Endanwender wird über seine Verantwortung während der Nutzung des EVG informiert.

Folgende Annahmen zur Sicherheitsumgebung sind getroffen:

| Annahmen | Beschreibung |
|----------|--|
| AE.1 | Es wird angenommen, dass der TOE als Kartenterminal für die nichtöffentliche Umgebung eingesetzt wird. |
| AE.2 | Es wird angenommen, dass der Benutzer ausschließlich Prozessorkarten benutzt, die den Spezifikationen ISO 7816 bzw. EMV 2000 genügen. |
| AE.3 | Es wird angenommen, dass sich der Nutzer vor der Inbetriebnahme 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 den Nummernblock 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 den Nummernblock eingibt. |

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 ist die gesamte Tastatur mit integriertem Kartenleser, kurz „Chipkartenterminal“ genannt. Neben der normalen Tastaturfunktionalität stellt der EVG mit Hilfe eines integrierten Kartenlesers die Möglichkeit zur Verfügung kontaktbehaftete Speicher- und Prozessorchipkarten zu verarbeiten. Die sichere PIN-Eingabe wird vom TOE ausschließlich für Prozessorchipkarten unterstützt. Die Funktion der sicheren PIN-Eingabe steht für Speicherchipkarten nicht zur Verfügung. Die Prozessorchipkarten müssen den Spezifikationen ISO 7816 bzw. EMV 2000 genügen und unterstützen die Übertragungsprotokolle T=0 und T=1. Bei synchronen Chipkarten basiert das Übertragungsprotokoll auf den herstellerspezifischen Spezifikationen.

Der EVG besteht aus Hardware- und Firmwareanteilen. Er kann an jedem USB-fähigen PC-System betrieben werden.

Der TOE bietet Schutz gegen Angreifer mit hohem Angriffspotential. Der Benutzer ist zudem in der Lage und auch dazu angehalten, die Unversehrtheit des TOE zu überprüfen.

Zum Lieferumfang gehören:

- Chipkartenterminal KBPC CX / CX Top (versiegelt) in Einzelverpackung
- USB Kabel
- Handbuch „Fujitsu Siemens USB-Security-Tastaturen“, Version K329-Z170-7419-1 (gültig für alle Produktvarianten des EVG)
- CD-ROM mit Treiber Software (gehört nicht zum Umfang der Evaluierung)

3 Sicherheitspolitik

Um ein elektronisches Dokument digital zu signieren, muss sich ein Benutzer durch Besitz (Signaturkarte) und Wissen (PIN) gegenüber seiner Signaturkarte authentifizieren.

Propagiertes Ziel ist es, die Chipkartenterminalfamilie KBPC CX / CX Top für Anwendungen zur Erzeugung qualifizierter elektronischer Signaturen nach dem deutschen Signaturgesetz [6] einzusetzen. Im Vordergrund der EVG-Sicherheitspolitik steht deshalb der Schutz der persönlichen Identifikationsdaten (PIN).

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

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

Bei der Anwendung der „qualifizierten elektronischen Signatur“ dürfen ausschließlich im Sinne des SigG [6] und SigV [7] bestätigte Chipkarten und bestätigte Signaturanwendungsprogramme bzw. herstellere erklärte Signaturanwendungsprogramme verwendet werden.

Zugelassene Komponenten sind auf der Internetseite der Regulierungsbehörde für Telekommunikation und Post (RegTP) zu finden (www.regtp.de).

Der Einsatz des Kartenterminals ist für **nichtöffentliche** Umgebungen zugelassen, beispielsweise Single- und Multi-User-PCs im privaten Bereich und in der Büroumgebung. Unter nichtöffentlicher Umgebung fallen alle Bereiche, die nicht für die Allgemeinheit (Öffentlichkeit) zugänglich sind.

Der Endanwender wird über seine Verantwortung während der Nutzung des EVG durch die mitgelieferten Handbücher informiert. Die Regeln zur sicheren Aufbewahrung und Nichtweitergabe der PIN werden dem Anwender vom Herausgeber der Chipkarte mitgeteilt.

4.2 Angenommene Einsatzumgebung

Folgende Annahmen wurden in [8], Kapitel 3.1 über die IT- Einsatzumgebung des EVG getroffen (siehe dazu auch Kapitel 1.6):

| Annahmen | Beschreibung |
|----------|--|
| AE.1 | Es wird angenommen, dass der TOE als Kartenterminal für die nichtöffentliche Umgebung eingesetzt wird. |
| AE.2 | Es wird angenommen, dass der Benutzer ausschließlich Prozessorkarten benutzt, die den Spezifikationen ISO 7816 bzw. EMV 2000 genügen. |
| AE.3 | Es wird angenommen, dass sich der Nutzer vor der Inbetriebnahme durch die Kontrolle der Unversehrtheit der Siegel überzeugt, ob keine sicherheitstechnischen Veränderungen |

| Annahmen | Beschreibung |
|----------|--|
| | 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 den Nummernblock 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 den Nummernblock eingibt. |

4.3 Klärung des Einsatzbereiches

Es wurden keine Bedrohungen identifiziert, die nicht durch die Sicherheitsfunktionen des EVG, sondern durch dessen Einsatzumgebung abgewehrt werden.

Nähere Informationen zu den Sicherheitsfunktionen des EVG befinden sich in Kapitel 1.2 dieses Reportes oder in [8], Kapitel 6.1 und 6.2.

5 Informationen zur Architektur

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

- *Mikrocontroller* (XCHIP mit internem Datenspeicher, Programmspeicher, USBController, Multi-Protokoll Smart Card Interface),
- *USB-Interface* (mit Kabel und Stecker),
- *Anzeigeeinheit* (Leuchtdioden),
- *Tastenmatrix mit Nummernblock*,
- *Chipkarteninterface* (Kontaktiereinheit) u.
- *Quarz*.

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

- *System*,
- *USB*,
- *Chipkarte* u.
- *Keyboard*.

6 Dokumentation

Im Lieferumfang sind EVG ist folgende Dokumentationen enthalten:

- Handbuch „Fujitsu Siemens USB Security Tastaturen; Version K329-Z170-7419-1 (gültig für alle Produktvarianten des EVG)

7 Testverfahren

7.1 Herstellertests

- Testansatz des Herstellers:

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

Die Tests wurden getrennt nach den Sicherheitsfunktionen durchgeführt und dokumentiert. Für jeden Test wurde ein Testplan einschließlich Testziel erstellt, die Prozeduren zur Testdurchführung beschrieben, die erwarteten Testergebnisse definiert und die tatsächlich erzielten Ergebnisse dargestellt.

Die Sicherheitsfunktion „*Schutz der PIN*“ wurde vollständig mit der evaluierten Testkonfiguration überprüft. Die Sicherheitsfunktion „*Speicheraufbereitung*“ konnte auf diese Weise nicht überprüft werden, da sie nicht über die Schnittstellen des EVG getestet werden kann. Daher wurde für diese Sicherheitsfunktion der Ansatz gewählt, sie am Entwicklungssystem des Herstellers zu testen.

- Umfang der durchgeführten Herstellertests:

Der Hersteller hat die beiden Sicherheitsfunktionen des EVG mit sieben übergeordneten Tests getestet, die sich in weitere Testfälle unterscheiden ließen, da sie jeweils für verschiedene PIN-Speicherbereiche, Fehlersituationen oder Parameter als gemeinsamer Test formuliert wurden. Durch die Testabdeckungsanalyse wurde nachgewiesen, dass der Hersteller den EVG systematisch auf dem Niveau der Sicherheitsfunktionalitäten und Teilsysteme getestet hat.

- Gesamtergebnis der Herstellertests:

Die Ergebnisse der Test wurden durch den Hersteller in der Testdokumentation festgehalten. 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 Prüfstellentests

- Testansatz der unabhängigen Evaluatortests:

Gemäß der Teststrategie des Evaluators sollten die vorgesehenen unabhängigen Tests am EVG die Erfüllung der funktionalen Sicherheitsanforderung durch die Sicherheitsfunktionen zeigen. Darüber hinaus sollten alle vier Teilsysteme und ihre Schnittstellen durch die Tests erfasst werden.

Die Tests wurden 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. Die Sicherheitsfunktion „*Schutz der PIN*“ wurde vollständig mit der evaluierten Konfiguration des EVG überprüft. Die Sicherheitsfunktion „*Speicheraufbereitung*“ konnte auf diese Weise nicht überprüft werden, da sie nicht über die Schnittstellen des EVG getestet werden kann. Daher wurde für diese Sicherheitsfunktion der Ansatz gewählt, am Entwicklungssystem des Herstellers zu testen.

- Umfang der durchgeführten Evaluatortests:

Der Evaluator hat aus den Herstellertests der Sicherheitsfunktionen des EVG eine Stichprobe ausgewählt und getestet. Sie erfasst etwa 70 % der Herstellertests, die als elf Testfälle formuliert wurden. Die Stichprobe des Evaluators deckt alle Sicherheitsfunktionen des EVG ab und berücksichtigt deren Charakteristika laut funktionaler Spezifikation. Der Evaluator hat außerdem die beiden Sicherheitsfunktionen des EVG mit insgesamt 79 unabhängigen Tests getestet. Davon sind 23 Tests auf „*Speicheraufbereitung*“ bezogen und 56 Tests entfallen auf „*Schutz der PIN*“. Diese Testfälle betreffen sowohl den normalen Ablauf der sicheren PIN-Eingabe als auch verschiedene Arten von Fehlersituationen.

- Gesamtergebnis der unabhängigen Evaluatortests:

Der Evaluator spezifizierte zu jeder Sicherheitsfunktion unabhängige Tests. Deren Ergebnisse wurden 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. 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

- Basis der unabhängigen Schwachstellensuche:

Basis der unabhängigen Schwachstellensuche bildeten die Herstellerdokumente und Prüfberichte und die Schwachstellensuche gemäß CEM [2] bzw. AIS 34 [4].

- Penetrationstests zu Sicherheitsfunktionen:

Die Evaluatoren haben im Rahmen der Penetrationstests des EVG die Sicherheitsfunktion „*Schutz der PIN*“ auf Schwachstellen untersucht. Die Sicherheitsfunktion „*Speicherwiederaufbereitung*“ konnte auf diese Weise nicht überprüft werden, da sie nicht über die Schnittstellen des EVG getestet werden kann.

Weiterhin wurde im Rahmen der unabhängigen Penetrationstests die Sicherheitsmaßnahme „Versiegelung“ auf Schwachstellen hinsichtlich der Anbringung und Positionierung der Siegel am EVG untersucht.

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

- Urteil der Testaktivitäten:

Die Evaluatoren haben die Penetrationstests basierend auf der Schwachstellenanalyse des Herstellers und unabhängige Penetrationstests durchgeführt. Der Sicherheitsfunktionen des EVG verhielten sich während der Penetrationstests wie spezifiziert. Der Sicherheitsmaßnahme zur Versiegelung des EVG verhielt sich während der Penetrationstests ebenfalls entsprechend ihrem definierten Zweck. Die durch die Evaluatoren und den Hersteller identifizierten Schwachstellen sind in der beabsichtigten Einsatzumgebung des EVG nicht ausnutzbar. Der EVG widersteht somit Angreifern mit hohem Angriffspotential.

8 Evaluerte Konfiguration

Die Tests wurden an einem Prototyp des EVG Chipkartenterminalfamilie KBPC CX / CX Top durchgeführt. Er steht stellvertretend für die EVG-Familie und besitzt wie in den Sicherheitsvorgaben definiert die Firmware-Version 1.04. Beim verwendeten Mikrocontroller handelte es sich um eine Flash-Variante anstatt der noch nicht verfügbaren ROM-Masken-Version. Dies hat jedoch keine Auswirkungen auf die funktionalen Tests. Für die Tests wurde der EVG an einem IBM-kompatiblen PC-System mit 32-Bit Windows Betriebssystem betrieben.

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

- USB-Tastatur mit integriertem Chipkartenterminal der Familie KBPC CX / CX Top mit der Firmware-Version 1.04 des Herstellers Fujitsu Siemens GmbH,
- Produktvarianten: KBPC CX: S26381-K329-V1xx HOS:02
KBPC CX: S26381-K329-V4xx HOS:01
KBPC CX TOP: S26381-K339-V1xx HOS:01

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

9 Ergebnisse der Evaluierung

Der Technische Evaluierungsbericht [9] wurde nach den Erfordernissen der Common Criteria [1], der Common Evaluation Methodology [2], den Anforderungen des Zertifizierungs-Schemas [3] und den Anwendungshinweisen

und Interpretationen (AIS) [4] von der Prüfstelle TÜV Informationstechnik GmbH erstellt.

Die Gesamtergebnisse gemäß der Common Criteria [1], Teil 3 Vertrauenswürdigkeitsklassen (entsprechend der EAL 3 mit Zusatz von **AVA_VLA.4, AVA_MSU.3, ADV_IMP.1, ADV_LLD.1 und ALC_TAT.1, ADO_DEL.2**) sind in der folgenden Tabelle zusammengefasst:

| Vertrauenswürdigkeitsklassen und -komponenten | | Ergebnis |
|--|---------------|----------|
| Sicherheitsvorgaben | CC Klasse ASE | PASS |
| EVG Beschreibung | ASE_DES.1 | PASS |
| Sicherheitsumgebung | ASE_ENV.1 | PASS |
| ST- Einführung | ASE_INT.1 | PASS |
| Sicherheitsziele | ASE_OBJ.1 | PASS |
| PP- Postulate | ASE_PPC.1 | PASS |
| IT- Sicherheitsanforderungen | ASE_REQ.1 | PASS |
| Explizit dargelegte IT- Sicherheitsanforderungen | ASE_SRE.1 | PASS |
| EVG Übersichtsspezifikation | ASE_TSS.1 | PASS |
| Konfigurationsmanagement | CC Klasse ACM | PASS |
| Authorisierungskontrolle | ACM_CAP.3 | PASS |
| EVG CM Umfang | ACM_SCP.1 | PASS |
| Auslieferung und Betrieb | CC Klasse ADO | PASS |
| Erkennung vor Modifizierungen | ADO_DEL.2 | PASS |
| Installations-, Generierungs- und Anlaufprozeduren | ADO_IGS.1 | PASS |
| Entwicklung | CC Klasse ADV | PASS |
| Informelle funktionale Spezifikation | ADV_FSP.1 | PASS |
| Sicherheitsspezifischer Entwurf auf hoher Ebene | ADV_HLD.2 | PASS |
| Beschreibender Entwurf auf niedriger Ebene | ADV_LLD.1 | PASS |
| Teilmenge der Implementierung der TSF | ADV_IMP.1 | PASS |
| Informeller Nachweis der Übereinstimmung | ADV_RCR.1 | PASS |
| Handbücher | CC Klasse AGD | PASS |
| Systemverwalterhandbuch | AGD_ADM.1 | PASS |
| Benutzerhandbuch | AGD_USR.1 | PASS |
| Lebenszyklusunterstützung | CC Klasse ALC | PASS |
| Identifikation der Sicherheitsmaßnahmen | ALC_DVS.1 | PASS |
| Klar festgelegte Entwicklungswerkzeuge | ALC_TAT.1 | PASS |
| Tests | CC Klasse ATE | PASS |
| Analyse der Testabdeckung | ATE_COV.2 | PASS |
| Testen – Entwurf auf hoher Ebene | ATE_DPT.1 | PASS |
| Funktionales Testen | ATE_FUN.1 | PASS |
| Unabhängiges Testen - stichprobenartig | ATE_IND.2 | PASS |

| Vertrauenswürdigkeitsklassen und -komponenten | | Ergebnis |
|---|---------------|----------|
| Schwachstellenbewertung | CC Klasse AVA | PASS |
| Analysieren und Testen auf unsichere Zustände | AVA_MSU.3 | PASS |
| Stärke der EVG- Sicherheitsfunktionen | AVA_SOF.1 | PASS |
| Hohe Widerstandsfähigkeit | AVA_VLA.4 | PASS |

Die Evaluierung hat gezeigt, dass:

- die spezifizierten funktionalen Sicherheitsanforderungen des EVG konform zu den Common Criteria Part 2 sind,
- die Anforderungen an die Vertrauenswürdigkeit konform zu Common Criteria Part 3 Part, entsprechend der EAL 3 mit Zusatz von AVA_VLA.4, AVA_MSU.3, ADV_IMP.1, ADV_LLD.1 und ALC_TAT.1, ADO_DEL.2 sind.

Für den EVG gelten keine funktionalen Sicherheitsanforderungen, für die eine Betrachtung der Stärke (SOF) in Frage kommt.

Der EVG besitzt keine ausnutzbaren Schwachstellen.

10 Kommentare und Empfehlungen

Das Handbuch [10] enthält wichtige Informationen über die sichere Benutzung des EVG, welche zu befolgen sind. Weiterhin sind die in den Sicherheitsvorgaben [8] getroffenen Annahmen für die IT- Umgebung und die Nicht- IT- Umgebung zu beachten.

11 Anhänge

Keine.

12 Sicherheitsvorgaben

Die Sicherheitsvorgaben [8] sind Bestandteil dieses Zertifizierungsreports.

13 Definitionen

13.1 Abkürzungen

| | |
|--------------|---|
| APDU | Application Programming Data Unit |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| 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 |
| IBM | International Business machines |
| 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] Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22)
- [7] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59)
- [8] Common-Criteria-Dokument Sicherheitsvorgaben EAL3+ KBPC CX / CX Top, Version 1.22 vom 08.11.2004, Fujitsu Siemens Computers GmbH
- [9] Technischer Evaluierungsbericht (ETR) CC Evaluierung des KBPC CX / CX Top, Version 1.1 vom 08.11.2004, TÜV Informationstechnik GmbH (vertrauliches Dokument)
- [10] Handbuch „Fujitsu Siemens USB-Security-Tastaturen“, Version K329-Z170-7419-1; Fujitsu Siemens Computers GmbH

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.