Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0525-2010

zu

SmartCase KB SCR eSIG (S26381-K529-Vxxx) Hardware-Version HOS:01, Firmware-Version 1.20

der

Fujitsu Technology Solutions 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-0525-2010

Tastatur mit SmartCard-Leser

SmartCase KB SCR eSIG (S26381-K529-Vxxx)
Hardware-Version HOS:01, Firmware-Version 1.20

von	Fujitsu Technology Solutions GmbH
PP-Konformität:	keine
Funktionalität:	Common Criteria Teil 2 erweitert
Vertrauenswürdigkeit:	Common Criteria Teil 3 konform EAL 3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 und AVA_VLA.4

Common Criteria
Recognition
Arrangement
für Komponenten bis
EAL4

Common Criteria

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 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, 11. Januar 2010

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Abteilungspräsident

L.S.

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 das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

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] [1]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 [2]
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS) [4]
- 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 erstmalig in Kraft getreten (SOGIS-MRA).

Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der Common Criteria bis einschließlich der Evaluationsstufe EAL7 erweitert und von

---

2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

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

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

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

den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Schweden und Spanien. Das BSI erkennt die Zertifikate der nationalen Zertifizierungsstellen von Frankreich und Großbritannien und seit Januar 2009 auch von den Niederlanden 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 Januar 2009 die nationalen Stellen folgender Nationen beigetreten: Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Malaysia, Pakistan, 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 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 SmartCase KB SCR eSIG (S26381-K529-Vxxx) Hardware-Version HOS:01, Firmware-Version 1.20 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts SmartCase KB SCR eSIG (S26381-K529-Vxxx) Hardware-Version HOS:01, Firmware-Version 1.20 wurde von TÜV Informationstechnik GmbH durchgeführt. Die Evaluierung wurde am 10. November 2009 beendet. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Antragsteller ist: Fujitsu Technology Solutions GmbH

Das Produkt wurde entwickelt von: Fujitsu Technology Solutions 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 SmartCase KB SCR eSIG (S26381-K529-Vxxx) Hardware-Version HOS:01, Firmware-Version 1.20 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://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] Fujitsu Technology Solutions GmbH
Bürgermeister-Ulrich-Str. 100
86199 Augsburg

Dies ist eine eingefügte Leerseite.

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 Evaluierungsgegenstand (EVG), das Chipkartenterminal KB SCR eSIG (S26381-K529-Vxxx HOS:01), stellt eine Tastatur mit einem integrierten Klasse 2 Leser dar, das Prozessorchipkarten nach [11] und [12] über verschiedene Applikationsschnittstellen ([16], [17] u.a.) verarbeiten kann.

Der EVG arbeitet mit allen Chipkarten-Datenübertragungsprotokollen gemäß ISO7816 (T=0, T=1), siehe [11]. Datenübertragungsprotokolle für Speicherchipkarten (I^2C-, 2-Wire-, 3-Wire-Protokoll) werden ebenfalls unterstützt.

Der EVG erkennt die von der Host-Software übermittelten Kommandos zur PIN-Eingabe und fügt die eingegebenen Nummern als PIN an die entsprechenden Stellen des Kommandos an die Chipkarte ein. Dabei wird nur die Tatsache an den Host gemeldet, dass eine der numerischen Tasten gedrückt wurde. Die Host-Applikation nutzt diese Information, um dem Anwender zu visualisieren, dass er eine Taste gedrückt hat bzw. wie viele Nummern der PIN aktuell eingegeben sind. Die PIN selbst verlässt den EVG nie im Klartext. Die PIN- Eingabe ist nur über den Nummernblock der Tastatur möglich.

Während sich der EVG im sicheren PIN- Eingabemodus befindet, ist eine PIN- Eingabe über den alphanumerischen Bereich nicht möglich. Der sichere PIN- Eingabemodus wird dem Benutzer durch eine rote LED signalisiert. Der EVG kann an allen Hostsystemen verwendet werden, die eine USB-Schnittstelle besitzen. Die Stromversorgung für den EVG erfolgt über den USB- Bus. Auf der Hostseite werden die Applikationsschnittstellen CT-API und PC/SC zur Verfügung gestellt, die für alle Chipkartenarten genutzt werden können. Alle Funktionalitäten an den Schnittstellen werden gemäß [16] und [17] abgebildet. Die Schnittstelle zwischen Host und dem Kartenterminal basiert auf dem Funktionsumfang von [15]. Die USB-Schnittstelle stellt die physikalische und logische Abgrenzung des EVG zum Host-System dar. Ziel ist es das Kartenterminal u.a. für die Applikation „digitale Signatur“ nach dem deutschen Signaturgesetz [13] einzusetzen.

Da der EVG als Klasse 2 Leser auch in der Lage ist, Identifikationsdaten (PIN) zu erfassen und an sichere Signaturerstellungseinheiten (Signatur-Chipkarten) nach §2 Nummer 10 SigG auf sicherem Weg zu übermitteln, können sie auch für Applikationen gemäß Signaturgesetz und Signaturverordnung [14] eingesetzt werden. Der EVG dient des weiteren zur Übermittlung des Hash-Wertes von der Anwendung zur Signaturkarte und zur Rückübertragung der Signatur von der Karte zur Signaturanwendung.

Der EVG stellt somit eine Teilkomponente für Signaturanwendungskomponenten dar, die eine Sicherheitsbestätigung benötigt, um für qualifizierte elektronische Signaturen nach §2 Nummer 3 SigG eingesetzt werden zu können. Zur Verwendung des EVG gemäß SigG/SigV sind sowohl Applikationen (Signaturanwendungen) als auch Chipkarten, die im SigG-Kontext evaluiert und bestätigt wurden, einzusetzen. Der EVG erfüllt die speziellen Anforderungen nach §15 Absatz 2 Nr.1a (keine Preisgabe oder Speicherung der Identifikationsdaten) und Absatz 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV. Ferner bietet der EVG die Möglichkeit eines gesicherten Firmware-Upgrade, um für zukünftige Anforderungen vorbereitet zu sein.

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 EAL 3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 and 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.

Die funktionalen Sicherheitsanforderungen für die IT-Umgebung des EVG werden in den Sicherheitsvorgaben [6] im Kapitel 5 dargestellt.

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

<table>
<tr><th>Sicherheitsfunktion</th><th>Beschreibung</th></tr>
<tr><td>SF.1
PIN Command
(Sichere PIN- Eingabe)</td><td>Das Umschalten des Kartenterminals in den sicheren PIN- Eingabemodus wird durch ein explizites CT-Kommando nach [15] durchgeführt. Dieses CT-Kommando enthält die PIN-Handling-Vereinbarungen und das Chipkartenkommando, 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 erwartet.
In der folgenden Tabelle sind die zugelassenen Instructionbytes nach [11] bzw. [12] aufgeführt:
<table>
<tr><th>INS-Byte</th><th>Bezeichnung</th><th>Bedeutung</th><th>Norm</th></tr>
<tr><td>0x20</td><td>VERIFY</td><td>PIN eingeben</td><td>ISO/IEC 7816-4</td></tr>
<tr><td>0x24</td><td>CHANGE REFERENCE DATA</td><td>PIN ändern</td><td>ISO/IEC 7816-8</td></tr>
<tr><td>0x26</td><td>DISABLE VERIFICATION REQUIREMENT</td><td>PIN aktivieren</td><td>ISO/IEC 7816-8</td></tr>
<tr><td>0x28</td><td>ENABLE VERIFICATION REQUIREMENT</td><td>PIN deaktivieren</td><td>ISO/IEC 7816-8</td></tr>
<tr><td>0x18</td><td>APPLICATION</td><td>Applikation entblocken</td><td>EMV 2000</td></tr>
<tr><td>0x2C</td><td>RESET RETRY COUNTER</td><td>PIN entsperren</td><td>ISO/IEC 7816-8</td></tr>
</table>
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 ein rot 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.
Dem Benutzer wird der Fortschritt seiner Eingabe mit dem Dummycode „*“ für jede eingegebene Ziffer angezeigt. Die Ausgabe der Dummycodes erfolgt über die USB-Schnittstelle, die dann von der entsprechenden PC-Anwendung angezeigt wird. Innerhalb des EVG wird aber mit der korrekten PIN gearbeitet.</td></tr>
<tr><td>SF.2
PIN Memory</td><td>Die Kommunikation zwischen PC-System und Chipkarte basiert gemäß [15] auf den sogenannten APDUs. Wird eine APDU über die USB- Schnittstelle im</td></tr>
</table>

Sicherheitsfunktion	Beschreibung
(Speicherwiederauf-bereitung)	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. Der Speicherbereich beinhaltet sowohl die PIN als auch die APDU. Außerdem wird die LED zur Anzeige der sicheren PIN- Eingabe ausgeschaltet.
SF.3 Secure Firmware Download (Sicherer Firmware-Update)	Die Verifikation einer Signatur der Firmware mit dem asymmetrischen RSA-Algorithmus und einer Bitlänge von 2048 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-256 mit einer Länge von 256 Bit ermittelt. Die Verifikation der Integrität und Authentizität erfolgt im EVG durch Vergleich des ermittelten Hash- Wertes und des Hash- Wertes als Bestandteil der entschlüsselten Signatur. Der öffentliche Schlüssel ist hierfür im EVG gespeichert.
Versiegelung (SM.1)	Anhand drei authentischer und fälschungssicherer Sicherheitssiegel, welche über die Trennkante zwischen Gehäuseunter- und Oberteil geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden. Dies wird dadurch sichergestellt, dass ein Öffnen nicht ohne Beschädigung des Siegels möglich ist. Die Beschaffenheit (Zerstöreigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann. Eine 7-stellige fortlaufende Nummer auf dem Siegel erlaubt eine eindeutige Identifizierung. Das eingesetzte Siegel erfüllt die Sicherheitsstufe 2 gemäß [19] und ist in der Produktliste [18] gelistet.

Tabelle 1: Sicherheitsfunktionen des EVG

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

Die in den Sicherheitsvorgaben [6] Kapitel 5.2 für bestimmte Funktionen angegebene Stärke der Funktionen “high” wird bestätigt.

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

Die Werte, die durch den TOE geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3.2, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3 dar.

Der EVG ist ein Chipkartenterminal der Familie SmartCase KB SCR eSIG (S26381-K529-Vxxx HOS:01) mit der Firmware-Version 1.20 in einer nicht veränderbaren Hardware-Konfiguration.

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:

SmartCase KB SCR eSIG (S26381-K529-Vxxx) Hardware-Version HOS:01, Firmware-Version 1.20

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifier	Version	Auslieferungsart
1	HW/SW	SmartCase KB SCR eSIG (S26381-K529-Vxxx) Vxxx bezeichnet unterschiedliche Ausführungen des Terminals: Die Hunderterstelle hinter dem V kennzeichnet die Gehäusefarbe, z.B.: 1 = marble grey; 2 = schwarz Die Zehner- und Einerstelle hinter dem V kennzeichnet die Tastaturbeschriftung, z.B: 10 = US (United States) 11 = H (Hungary) 20 = D (German) 65 = GB (Great Britain)	Hardware: HOS:01 Firmware: 1.20	Direkter Versand vom Hersteller zum Kunden.
2	DOC	USB-Security-Tastatur KB SCR eSIG Betriebsanleitung	Ausgabe Oktober 2009	
3	DOC	USB-Security-Keyboard KB SCR eSIG Operating Manual	October 2009 edition	
4	SW	FWCheck_KBSCReSIG.exe Programm zur Prüfung der korrekten Firmwareversion des EVG	SHA-256 Hash: 3D828D5159E5BA52FA59D56CED20EF30B0D9FD757F6A5AAE85880EA0 832BB9B2	

Tabelle 2: Auslieferungsumfang des EVG

Das Gehäuse des Chipkartenterminals ist versiegelt. Die Siegel sind vor der Inbetriebnahme durch den Kunden entsprechend der Betriebsanleitung auf Unversehrtheit zu prüfen. Ebenso ist entsprechend der Betriebsanleitung zu prüfen, dass die richtige Hardware- und Firmware ausgeliefert wird.

Ein Firmware-Upgrade kann auf zwei unterschiedliche Arten geschehen:

- Der Kunde erhält von Fujitsu Technology Solutions GmbH eine CD mit einem Setup-Programm, das die neue Firmware und ein Tool zum Auslesen der Firmwareversion und Laden der neuen Firmware enthält sowie die aktuellen Treiber. Der Kunde kann dann die Software installieren und die neue Firmware aufspielen. Die Firmware (HEX-File) ist signiert. Die Signatur wird im Chipkartenterminal überprüft, bevor die Firmware in den Controller geladen werden kann.

- Der Kunde lädt das Setup Programm mit neuer Firmware, einem Tool zum Auslesen der Firmwareversion und Laden der Firmware und den aktuellen Treiber von der Fujitsu Technology Solutions GmbH Homepage. Der Kunde kann dann die Software installieren und die neue Firmware aufspielen. Die Firmware (HEX-File) ist signiert. Die Signatur wird im Chipkartenterminal überprüft, bevor die Firmware in den Controller geladen werden kann.

Die Verifikation der Signatur der Firmware wird mittels Einsatz des asymmetrischen RSA-Algorithmus mit einer Bitlänge von 2048 sowie durch den Einsatz des Hash-Verfahrens SHA-256 garantiert, wodurch die Integrität und Authentizität der Firmware beim Laden in den EVG gewährleistet ist. Das Einspielen einer nicht zertifizierten Firmware wird somit vom EVG verhindert.

3 Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionen des EVG umgesetzt. Sie behandelt die folgenden Sachverhalte:

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

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

Die Sicherheitsziele des EVG sehen vor, die Identifikationsdaten des Benutzers nicht zu speichern und/oder preis zu geben. Sicherheitstechnische Veränderungen am EVG müssen erkennbar sein. Das Einspielen einer neuen Firmware wird nur akzeptiert, wenn zuvor die Integrität und Authentizität der Firmware verifiziert wurde.

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 EVG muss als Kartenterminal für die nichtöffentliche Umgebung eingesetzt werden.
- Der Anwender darf ausschließlich Prozessorkarten benutzen, die den Spezifikationen [11] bzw. [12] genügen.
- Der Anwender muss das Sicherheitssiegel (Siegelnummer) regelmäßig vor Benutzung des Gerätes auf Unversehrtheit prüfen.
- Eine unbeobachtete Eingabe der Identifikationsdaten (PIN) ist durch den Benutzer zu gewährleisten.
- Während der PIN- Eingabe über den Nummernblock muss der Benutzer den Status der LEDs dahingehend überprüfen, dass der Modus der sicheren PIN- Eingabe aktiv ist.

- Der Benutzer muss die PIN über den Nummernblock eingeben.
- Der Anwender muss mit einem vom Hersteller bereitgestellten Softwaretool regelmäßig vor der Benutzung des Gerätes verifizieren, ob die Versionsnummer des EVGs mit der bestätigten Version übereinstimmt. Applikationen gemäß §2 Nummer 11 SigG, siehe [13], sollten automatisch verifizieren, dass nur bestätigte Versionen des EVGs verwendet werden, um diese Aufgabe dem Endanwender abzunehmen.
- Der Anwender muss darauf achten, dass bei einem Firmware-Update die zum Download bereitgestellte Firmware explizit als zertifizierte und bestätigte Version gekennzeichnet ist. Der EVG muss als Kartenterminal für die nichtöffentliche Umgebung eingesetzt werden.

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5 Informationen zur Architektur

Der EVG besteht aus folgenden Teilsystemen:

ID	Subsystem	Beschreibung
TSS1	USB SUBSYSTEM	Dieses Subsystem ist verantwortlich für die Einhaltung der USB 2.0 Anforderungen, damit das Gerät als Tastatur mit Chipkartenleser vom Host-Rechner erkannt wird. Diese Funktionalität wird durch die Implementierung folgender Funktionen über die physikalische Schnittstelle PHYINT1 erreicht: ● USB Hardware Handler ● USB Chapter9 Handler ● Command Dispatcher
TSS2	CCID SUBSYSTEM	Dieses Subsystem ist verantwortlich für die Einhaltung der CCID 1.10 Anforderungen zum Austausch von Meldungen zwischen dem Host-Rechner und dem Chipkartenleser. Die Einhaltung der CCID 1.10 Anforderungen stellt die Kompatibilität mit Standard CCID Host-Treibern sicher. Die folgenden Funktionen sind als Teil dieses Subsystems implementiert: ● CCID Class Descriptor Handler ● CCID Asynchronous Event Handler ● CCID Command-Response Handler
TSS3	PIN COMMAND SUBSYSTEM	Dieses Subsystem ist verantwortlich für die Einhaltung der PCSC 2.0 Teil 10 Anforderungen zur sicheren PIN Authentifizierung. Die folgenden Funktionen sind implementiert: ● APDU Handler ● Secure Key scan ● LED Handler
TSS4	HID SUBSYSTEM	Dieses Subsystem ist verantwortlich für die Einhaltung der HID Ver. 1.11 Anforderungen zum Austausch von Tastaturmeldungen mit dem Host-Rechner. Die folgenden Funktionen sind implementiert: ● HID Class Descriptor Handler ● Keyboard Scanner ● Report Handler
TSS5	SECURE DOWNLOAD SUBSYSTEM	Diese Funktion ist verantwortlich, dass nur digital signierte Firmware-Binärdateien, die ausschließlich für diese Gerät bestimmt sind, geladen werden können. Ein Firmware- Upgrade ist nur erfolgreich wenn der berechnete Hashwert der Firmware mit dem übergebenen Hashwert übereinstimmt. Die folgenden Funktionen sind implementiert:

ID	Subsystem	Beschreibung
		● USB Handler ● SHA-256 Hash and RSA-2048 Handler ● Flash Handler
TSS6	SMARTOS SUBSYSTEM	Dieses Subsystem ist verantwortlich für die Einhaltung der ISO 7816 Anforderungen. Die folgenden Funktionen sind implementiert. ● Card Hardware Interface Handler ● T=0 / T=1 Protocol Handler ● Memory Card Protocol Handler
TSS7	PIN MEMORY SUBSYSTEM	Diese Sicherheitsfunktion implementiert die Speichermanagementfunktion, angestoßen durch TSS3 (PIN COMMAND SUBSYSTEM) über die Schnittstelle TSSINT8. Nachfolgend die Funktionalitäten dieser SF: ● Verwalten des PIN Speichers, der APDU vom HOST und der APDU zur Chipkarte ● Löschen des PIN Speichers vor der Benutzereingabe während einer PIN-Prüfung ● Löschen der alten PIN und der neuen PIN während einer PIN-Modifikation ● Löschen des Speichers nach Abschluss der PIN-Prüfung / Modifikation

Tabelle 3: EVG Teilsysteme

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

7.1 Exakte Beschreibung der Testkonfiguration

Für die Evaluatortests wurden nachfolgende Testwerkzeuge/Testmittel verwendet:

SW:

- SCKBx86.sys, Version 1.9.0.0, PC-SC Treiber für den SmartCase KB Chipkartenleser
- CTPCSC32.dll, Version 2.70.0.0 (CT-API zur PC/SC Schnittstelle, CT-API Wrapper) SPR532.dll, Version 1.21.0.0, und SprRes.dll, Version 1.2.0.2
- Testctp.exe, Version 0.9.9.173 (Test script files: *.tcr)
- Tcot.exe, Version 1.2.0.1 (Test script files: *.xml)
- Pintest.exe, Version 1.3.0.2 (Test script files: *.xml)
- Device Monitor.exe, HHD Software USB Monitor 2.37
- STCFUx32.sys, Version 2.1.0.1 (STC DFU Treiber)

- FwUpdate.exe, Version 3.3.0.0, Generic Device Firmware Upgrade Utility (download firmware: *.bin)
- FWCheck_KBSCReSIG.exe, Version 1.20.0.0, FWCheck_KBSCReSIG Application

HW:

- Compaq DeskPro Desktop PC (IBM-kompatibles PC-System)
- 32-Bit-OS Windows 2000
- EVG mit USB Schnittstelle

7.2 Hersteller-Prüfungen entsprechend ATE_FUN

a) Testobjekt
SmartCase KB SCR eSIG (S26381-K529-V120 HOS:01) mit der Firmwareversion 1.20

b) Host-Betriebssystem
Der EVG kann mit einem PC oder ein Notebook und einem handelsüblichen Betriebssystem wie bspw. WinXP SP3 oder Vista SP1 als Hostsystem verbunden werden. Hierzu wird die Verbindung über folgende Schnittstelle bereitgestellt:
    - USB 1.1 oder USB 2.0 Schnittstelle zum Host[8]

c) Vom Hersteller zum Testen verwendete Hostsystem:
Fujitsu Siemens x86 basierender PC mit WinXP SP3 32bit (5.1.2600 SP3 Build 2600); 1.73 GHZ, 512MB RAM
    - Fujitsu Siemens x86 basierender PC mit Vista SP1

d) Angaben zu weiteren Komponenten, welche zum Testen verwendet wurden:
    - Starscope Simulator oder Smartcard mit Java Card Betriebssystem
    - Netkey Smartcard (Mehrfachsignaturkarte)
    - IFDTEST Suite PC/SC Cards
    - USB CATC Advisor

e) Zum Testen verwendete Softwarewerkzeuge:
Der EVG wurde unter Zuhilfenahme nachfolgender Softwarewerkzeuge getestet:
    - IFDtest.exe Microsoft Chipkartentestwerkzeug
    - Testresman.exe PCSC Applikation zur Ausführung d. Scenariodateien
    - ICCTest.exe Stresstest- / Belastungstestwerkzeug
    - Pinpad tool EXE Name nicht bekannt
    - PCSC Applikation zum Testen der PINPAD Funktionalität des Keyboards
    - FWUPDATE.exe Werkzeug für das Firmware-Upgrade
    - CH8CK.EXE Chapter08 Testwerkzeug
    - USBCVr13Beta3.exe Chapter09 Testwerkzeug
    - TCoT.exe Teletrust Compliance-Testwerkzeug

[8] der korrespondierende Treiber ist nicht Bestandteil des EVG

- Drvrcfg.exe Treiberkonfigurationstesttool
- EMVTest.exe Testtool zum Testen der EMV-Compliance

Die Tests zur Sicherheitsfunktion SF1 wurden unter Zuhilfenahme von Prozessorchipkarten, welche die nachfolgenden asynchronen Protokolle unterstützen, durchgeführt:

- T=0 ISO 7816 konform,
- T=1 ISO 7816 konform.

f) Testansatz
Die Herstellertests wurden mit dem Ziel durchgeführt, die funktionalen Sicherheitsanforderungen des EVG zu bestätigen. Die gewählte Herstellerstrategie war es, den EVG gegen die sicherheitsdurchsetzenden Funktionen zu testen. Hierzu spezifizierte der Hersteller korrespondierende Testziele sowie geeignete Testfälle für die Sicherheitsfunktionen

- SF.1 Sichere PIN-Eingabe
- SF.2 Speicherwiederaufbereitung
- SF.3 Sicherer Firmware-Update

Die Testfälle deckten die spezifizierten Sicherheitsfunktionen vollständig ab. Insgesamt führte der Hersteller 40 Testfälle zu SF.1 Sichere PIN-Eingabe, 5 Testfälle zu SF.2 Speicherwiederaufbereitung und 10 Testfälle zu SF.3 Sicherer Firmware-Update durch.

g) Testtiefe
In Hinblick auf die Testtiefe stellen die Herstellertests sicher, dass die Wirksamkeit der EVG-Sicherheitsfunktionen ausreichend geprüft wurden. Der Hersteller führte die EVG-Sicherheitsfunktionstests auf der Ebene der Subsysteme durch, indem er hierauf entsprechende Testfälle abbildete und somit deren Funktionstüchtigkeit nachweisen konnte. Die Tests wurden nicht nur für die vorgenannten Sicherheitsfunktionen, sondern auch darüber hinaus für alle Subsysteme und Module des EVG durchgeführt. Dabei gewährleisten die Tests auch, dass alle externen Schnittstellen des EVG sowie alle internen Schnittstellen zwischen den EVG Subsystemen verwendet wurden. In Hinblick auf die Testtiefe stellen diese Tests sicher, dass die EVG Sicherheitsfunktionen die spezifizierte Wirkung aufweisen.

h) Testergebnisse
Vom Hersteller wurden für jede EVG-Sicherheitsfunktion geeignete funktionale Tests spezifiziert, durchgeführt und dokumentiert. Die Testergebnisse für alle durchgeführten Tests stellten sich wie erwartet ein. Hierbei traten keine Fehler oder andere Mängel in Hinblick auf die Sicherheitsfunktionalität auf. Somit zeigen die Testergebnisse, dass die EVG-Sicherheitsfunktionen sich wie spezifiziert verhalten. Alle Sicherheitsfunktionen konnten erfolgreich getestet werden und der Hersteller lieferte ausreichende Informationen zur Beschreibung der Funktionsrealisierung. Der Hersteller konnte nachweisen, dass alle Sicherheitsfunktionen tatsächlich die spezifizierten Eigenschaften aufweisen.

7.3 Prüfungen des Evaluators

7.3.1 Unabhängiges Testen entsprechend ATE_IND

a) Getestete EVG-Konfigurationen
USB-Chipkartenterminal der Familie SmartCase KB SCR eSIG (S26381-K529-V120 HOS:01) mit der Firmware-Version 1.20. Die EVG-Konfiguration entspricht der Beschreibung der funktionalen Spezifikation. Alle Tests wurden über die USB-Host-Schnittstelle durchgeführt.

b) Testumfang
Es wurden Tests zu drei Sicherheitsfunktionen durchgeführt. Die Sicherheitsfunktionen lauten:

- SF.1 Sichere PIN-Eingabe
- SF.2 Speicherwiederaufbereitung
- SF.3 Sicherer Firmware-Update

Die Evaluatorstrategie hierbei war es, die Funktionalität des EVG wie in den Sicherheitsvorgaben [6] beschrieben zu testen. Die Stichprobe der Tests zu den EVG-Sicherheitsfunktionen wurde so gewählt, dass alle externen Schnittstellen gemäß der funktionalen Spezifikation sowie alle Subsysteme der Architekturbeschreibung abgedeckt sind.

c) Die Testumgebung für die unabhängigen Tests ist äquivalent zu der Herstellertestumgebung, welche auch eine Untermenge der verwendeten Testsoftware beinhaltet, die vom Hersteller zur Durchführung der Herstellertests verwendet wurde. Insgesamt führte der Evaluator 109 unabhängige Testfälle durch. Dabei wurden 84 Testfälle zu SF.1 Sichere PIN-Eingabe, 15 Testfälle zu SF.2 PIN Speicherwiederaufbereitung und 10 Testfälle zu SF.3 Sicherer Firmware-Update durchgeführt.

d) Herstellertests
Um die Gültigkeit der Herstellertests zu bestätigen wählte der Evaluator eine Stichprobe aus. Dabei wurde darauf geachtet, dass bei der Stichprobe alle Sicherheitsfunktionen sowie alle EVG stimulierenden externen Schnittstellen berücksichtigt wurden. Zusätzlich wurden Testfälle aus dem Testplan des Herstellers mit nachfolgender Anzahl wiederholt.
Während der unabhängigen Evaluatortests wurden 9 Testfälle zur Sicherheitsfunktion SF.1 Sichere PIN-Eingabe, 1 Testfall zu SF.2 Speicherwiederaufbereitung und 4 Testfälle zu SF.3 Sicherer Firmware-Update durchgeführt. Insgesamt wurden 14 Herstellertestfälle wiederholt.

e) Ergebnisse
Die Ergebnisse der unabhängigen Evaluatortests und der vom Evaluator wiederholten Herstellertests bestätigen die EVG-Funktionalität wie in [6] beschrieben. Alle tatsächlichen Testergebnisse stimmten mit den erwarteten Testergebnissen überein. Es wurden keine Hinweise auf Fehler identifiziert.

7.3.2 Schwachstellenanalyse

Penetrationstest-Anstrengungen des Evaluators, aufbauend auf der Schwachstellenanalyse des Herstellers und der unabhängigen Schwachstellenanalyse:

Getestete EVG-Konfiguration:

- Das SmartCase KB SCR eSIG mit der Firmware-Version 1.20 wurde entsprechend der Bedienungsanleitung konfiguriert.

Basis der unabhängigen Schwachstellensuche (aus der die Penetrationstests folgern):

- Schwachstellensuche in Herstellerdokumenten und Prüfberichten
- Schwachstellensuche gemäß [CEM] bzw. [AIS 34]

Penetrationstests zu Sicherheitsfunktionen:

- Der Evaluator hat im Rahmen der Penetrationstests des EVG drei Sicherheitsfunktionen, d.h *SF.1 Sichere PIN-Eingabe,* SF.2 *Speicherwiederaufbereitung* und *SF.3 Sicherer Firmware-Update* auf Schwachstellen untersucht.
- Im Zuge der Penetrationstests wurde verifiziert, dass der EVG bei Verbindungsabbruch des Hosts, bei Kartenleserabbruch, Chipkartenentfernung im Betrieb oder im sicheren Eingabemodus den Speicherbereich für die PIN-Daten überschreibt.
- Der Evaluator hat im Rahmen der unabhängigen Penetrationstests des EVG basierend auf der unabhängigen Schwachstellenanalyse die unvollständige Paddingverifikation während der RSA-Signaturverifikation unter Berücksichtigung des Standards PKCS#1 V1.5 untersucht.
- Ferner wurden im Zuge der Evaluatortests die Siegeleigenschaften verifiziert.
- Mit Penetrationstests zur Widerstandsfähigkeit des EVG gegenüber Angriffen mit hohem Angriffspotential hat der Evaluator die vollständige und korrekte Implementierung der Sicherheitsfunktionen überprüft und nach versteckten Funktionen und weiteren Kommandos gesucht.
- Der Evaluator führte ferner Penetrationstests zum Analysieren und Testen des EVG auf unsichere Zustände durch.

Urteil der Testaktivitäten:

- Die Sicherheitsfunktionen des EVG haben sich während der Penetrationstests wie spezifiziert verhalten.
- Die Schwachstellen sind in der beabsichtigten Einsatzumgebung des EVG nicht ausnutzbar. Der EVG bietet Schutz gegen Angreifer mit hohem Angriffspotential.

8 Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf das Chipkartenterminal der Familie SmartCase KB SCR eSIG (S26381-K529-VXXX HOS:01) mit der Firmware-Version 1.20. Das Tastaturlayout sowie die Gehäusefarbe können hierbei variieren. Der Platzhalter „XXX“ wird entsprechend ersetzt.

Bei den Tests wurde das Chipkartenterminal an IBM-kompatiblen PC-Systemen mit 32-Bit-Windows-Betriebssystemen betrieben, die nicht Bestandteil des EVG sind.

9 Ergebnis der Evaluierung

9.1 CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR), [7] 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 EAL 3 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 EAL 3 der CC (siehe auch Teil C des Zertifizierungsreports)
- Die Komponenten ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 und AVA_VLA.4

Die Evaluierung hat gezeigt:

- Funktionalität: Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL 3 mit Zusatz von
  ADO_DEL.2, ADV_IMP.1, ADV_LLD.1,
  ALC_TAT.1, AVA_MSU.3 und AVA_VLA.4
- Die folgenden Sicherheitsfunktionen erfüllen die behauptete Stärke der Funktionen: high:
  SF.3 Sicherer Firmware-Update

  Um die Stärke der Funktionen zu ermitteln, wurden die Interpretationen des Schemas genutzt (AIS, siehe [4]).

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 folgenden Kryptoalgorithmen werden vom EVG verwendet, um seine Sicherheitspolitik umzusetzen:

- Hashfunktionen:
  - SHA-256
- Algorithmen zur Ver- und Entschlüsselung:
  - RSA 2048

Dies gilt für die folgende Sicherheitsfunktion:

SF.3 Sicherer Firmware-Update

Die Stärke der Kryptoalgorithmen wurde im Rahmen der Evaluierung nicht bewertet (vgl. §9 Abs. 4 Nr. 2 BSIG). Gemäß der „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. November 2008, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen“ sind die Kryptoalgorithmen geeignet für Erzeugung und Prüfung von elektronischen Signaturen. Der Zeitraum, für den diese Einschätzung gilt, ist im offiziellen Katalog [8] angegeben und im Kapitel 10 zusammengefasst.

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 folgenden Auflagen und Hinweise zu beachten:

Innerhalb des SmartCase KB SCR eSIG mit Firmware Version 1.20 wurden die nachfolgenden kryptografischen Mechanismen implementiert: RSA 2048 und SHA-256

Mit Bezug auf „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. November 2008, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen“

- wird der RSA-Algorithmus mit einer Länge von 2048 Bit nach heutigem Kenntnisstand für den Zeitraum bis Ende 2015 als ausreichend sicher angesehen,
- wird die Hashfunktion SHA-256 nach heutigem Kenntnisstand der Analyse von Hashfunktionen bis Ende 2015 als geeignet für qualifizierte elektronische Signaturen angesehen.

Darüber hinaus erfordert der sichere Betrieb des SmartCase KB SCR eSIG, Firmware Version 1.20, die Implementierung und permanente Einhaltung nachfolgender Sicherheitsmaßnahmen/ Sicherheitsanforderungen:

- Die Tastatur darf als Kartenterminal nur in nichtöffentlichen Bereichen eingesetzt werden.
- Überzeugen Sie sich vor Inbetriebnahme der Tastatur, dass keine sicherheitstechnischen Veränderungen vorgenommen wurden, kontrollieren Sie auch die Unversehrtheit der Siegel.
- Um die Authentizität während des Betriebs sicher zu stellen, notieren Sie sich bitte die 7-stelligen Siegelnummern.
- Geben Sie die PIN nur über den Nummernblock des Terminals ein.
- Achten Sie darauf, dass Sie während der PIN-Eingabe nicht beobachtet werden.
- Achten Sie darauf, dass während der PIN-Eingabe die PIN Leuchtdiode rot blinkt, da sich nur dann das Kartenterminal im Modus zur sicheren PIN-Eingabe befindet.
- Verwenden Sie nur Prozessorkarten, die den Spezifikationen [11] bzw. [12] genügen, um den Schutz der persönlichen Identifikationsdaten (PIN) zu gewährleisten.
- Verwenden Sie bei der Anwendung “qualifizierte elektronische Signatur“ nur im Sinne des SigG und SigV bestätigte Chipkarten und bestätigte Signaturanwendungs-programme bzw. herstellererklärte Signaturanwendungsprogramme. Zugelassene Komponenten sind auf der Internetseite der Bundesnetzagentur für Elektrizität, Gas,

Telekommunikation, Post und Eisenbahnen zu finden. Das Produkt stellt einen Teil (Chipkartenterminal) der am Signiervorgang beteiligten Komponenten (Signaturkarte, Applikation mit Signierfunktion) dar.

11 Sicherheitsvorgaben

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

12 Definitionen

12.1 Abkürzungen

AP	Advanced Performance
APDU	Application Programming Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz
CC	Common Criteria for IT Security Evaluation – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
CCRA	Common Criteria Recognition Arrangement
CT	Card Terminal – Kartenterminal
DIN	Deutsches Institut für Normung e.V.
EAL	Evaluation Assurance Level – Vertrauenswürdigkeitsstufe
EMV	Europay International, Mastercard, Visa
EVG	Evaluationsgegenstand (EVG)
HBCI	Home Banking Computer Interface
I2C	Inter-integrated Circuit
ICC	Integrated Chip Card
ISO	International Organization for Standardization
IT	Information Technology - Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility – Prüfstelle für IT-Sicherheit
PC	Personal Computer
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PP	Protection Profile – Schutzprofil
RAM	Random Access Memory
SF	Security Function – Sicherheitsfunktion
SFP	Security Function Policy – Politik der Sicherheitsfunktion

SigG	Signaturgesetz
SigV	Signaturverordnung
SOF	Strength of Function – Stärke der Funktion
SF	Sicherheitsfunktion
SM	Sicherheitsmaßnahme
SSEE	Sichere Signaturerstellungseinheit – “Signaturkarte”
ST	Security Target – Sicherheitsvorgaben
TOE	Target of Evaluation – Evaluationsgegenstand
TSC	TSF Scope of Control – Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functions – EVG-Sicherheitsfunktionen
TSP	TOE Security Policy – EVG-Sicherheitspolitik
TÜVIT	TÜV Informationstechnik
US	United States
USB	Universal Serial Bus

12.2 Glossar

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[9].

[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-CC-0525, Version 1.16, 09. September 2009, „Sicherheitsvorgaben EAL3+, SmartCase KB SCR eSIG / K529“, Fujitsu Technology Solutions GmbH

[7] Evaluierungsbericht, Version 3, 05. November 2009, „Evaluation Technical Report (ETR), Common Criteria CC 2.3, ET V3 – KB SCR eSIG“, TÜVIT GmbH (vertrauliches Dokument)

[8] Übersicht über geeignete Algorithmen vom 17. November 2008; Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung; Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

[9] Konfigurationsliste für den EVG, Version 1.00, 28. September 2009, „Konfigurationsliste“ (Autor: ZF Electronics GmbH) (vertrauliches Dokument)

[10] Dokumentation für den EVG, Ausgabe Oktober 2009, “USB-Security-Tastatur KB SCR eSIG Betriebsanleitung”

[11] DIN ISO 7816 - 1 Identification cards - Integrated circuit(s) cards with contacts – Physical Characteristics
DIN ISO 7816 - 2 Identification cards - Integrated circuit(s) cards with contacts – Dimensions and locations of the contacts
DIN ISO 7816 - 3 Identification cards - Integrated circuit(s) cards with contacts – electrical characteristics and transmission protocols
DIN ISO 7816 - 4 Information technology - Identification cards - Integrated circuit(s) cards with contacts – Inter-industry commands for interchange
DIN ISO 7816 - 8 Identification cards – Integrated circuit(s) cards with contacts – Security related interindustry commands

[9] Inbesondere:

- AIS 32, Version 1, 2 Juli 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 2, 24. Oktober 2008, Evaluation Methodology for CC Assurance Classes for EAL5+

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

[13] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16. Mai 2001 (BGBl. I S. 876) zuletzt geändert durch Art. 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)

[14] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), vom 16. November 2001 (BGBL 2001 Teil I Nr. 59, S. 3074–3084) zuletzt geändert durch Art. 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

[15] Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.1

[16] Interoperability Specification for ICCs and Personal Computer Systems, PC/SC Workgroup, Version 2.0

[17] Anwendungsunabhängiges CardTerminal Application Programming Interface für Chipkartenanwendungen CT-API Version 1.1.1 / Juni 2001

[18] BSI TL 03400: Produkte für die materielle Sicherheit, Juli 2008

[19] BSI TL 03415: Anforderungen und Prüfbedingungen an Sicherheitsetiketten, Januar 2009

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.

Anhang B: Evaluierungsergebnisse zur Entwicklungs- und Produktionsumgebung Seite 41

Dies ist eine eingefügte Leerseite.

Anhang B zum Zertifizierungsreport BSI-DSZ-CC-0525-2009

Evaluierungsergebnisse zur Entwicklungs- und Produktionsumgebung

Das IT-Produkt SmartCase KB SCR eSIG (S26381-K529-Vxxx) Hardware-Version HOS:01, Firmware-Version 1.20 (Evaluierungsgegenstand – EVG) wurde von einer anerkannten Prüfstelle nach der Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 in Übereinstimmung mit den Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005) evaluiert.

Die folgenden Ergebnisse der Zertifizierung vom 19. November 2009 in Hinsicht auf die Entwicklungs- und Produktionsumgebung wurden erzielt. Die Common Criteria Vertrauenswürdigkeitsanforderungen

- ACM – Konfigurationsmanagement (ACM_CAP.3, ACM_SCP.1),
- ADO – Auslieferung und Betrieb (ADO_DEL.2, ADO_IGS.1) and
- ALC – Lebenszyklus-Unterstützung (ALC_DVS.1, ALC_TAT.1),

sind für die folgenden Entwicklungs- und Produktionsstandorte des EVG erfüllt:

a) SCM Microsystems (India) Pvt. Ltd., Module 0506, 0507 &0508 ‘D’ Block South, 5th floor, Tidel Park 4, Canal Bank Road, Taramani, Chennai 600113, India

b) ZF Electronics GmbH, Cherrystraße, 91275 Auerbach

Für die oben genannten Standorte wurden die Anforderungen in Übereinstimmung mit den Sicherheitsvorgaben [6] erfüllt. Die Evaluatoren bestätigen, dass die Sicherheitsziele und Anforderungen an den EVG-Lebenszyklus bis hin zur Auslieferungen durch die Prozesse an diesen Standorten erfüllt werden (siehe auch die Sicherheitsvorgaben [6]).

Dies ist eine eingefügte Leerseite.