Zertifizierungsreport

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0301-2006

zu

Chipkartenterminal KAAN Advanced
Hardware Version K104R3, Firmware Version 1.02

der

KOBIL Systems GmbH

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0301-2006

Chipkartenterminal KAAN Advanced Hardware Version K104R3, Firmware Version 1.02 der KOBIL Systems GmbH

Common Criteria Arrangement
für Komponenten bis EAL4

Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle nach den *Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3 (ISO/IEC 15408:2005),* unter Nutzung der *Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 (ISO/IEC 15408:2005)* und Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL4 evaluiert.

Prüfergebnis:

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

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

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

Die auf der Rückseite aufgeführten Anmerkungen sind Bestandteil dieses Zertifikates.

Bonn, den 20. Dezember 2006

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-5455 - Infoline +49 228 9582-111

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

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

Vorbemerkung

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

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

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

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

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

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

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

Gliederung

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

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

- BSIG[2]
- BSI-Zertifizierungsverordnung[3]
- BSI-Kostenverordnung[4]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN 45011
- BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3[5]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)
- Informationen von der Zertifizierungsstelle zur Methodologie für Vertrauenswürdigkeitskomponenten oberhalb von EAL 4 (AIS 34)

---

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

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

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

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

2 Anerkennungsvereinbarungen

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

2.1 ITSEC/CC - Zertifikate

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

2.2 CC - Zertifikate

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

Diese Evaluierung beinhaltet die Komponenten AVA_MSU.3 und AVA_VLA.4, die nicht unter der Common Criteria Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten anerkannt werden. Für die gegenseitige Anerkennung sind die 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 Chipkartenterminal KAAN Advanced, Hardware Version K104R3, Firmware Version 1.02 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts Chipkartenterminal KAAN Advanced, Hardware Version K104R3, Firmware Version 1.02 wurde von der Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH – Prüfstelle für IT-Sicherheit durchgeführt. Das Prüflabor Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH – Prüfstelle für IT-Sicherheit ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Antragsteller, Hersteller und Vertreiber ist

KOBIL Systems GmbH
Pfortenring 11
67547 Worms, Deutschland.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 20. Dezember 2006 vom BSI abgeschlossen.

Das bestätigte Vertrauenswürdigkeitspaket gilt nur unter der Voraussetzung, daß

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

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

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

[6] Information Technology Security Evaluation Facility

4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-18.

Das Produkt Chipkartenterminal KAAN Advanced, Hardware Version K104R3, Firmware Version 1.02 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

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

[7] KOBIL Systems GmbH
Pfortenring 11
67547 Worms, Deutschland

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

Die Chipkartenleser KAAN Advanced (USB- und RS232-Variante) sind universelle Chipkartenlesegeräte mit Tastatur zur sicheren PIN-Eingabe sowie einer updatefähigen Firmware[8]. Die Chipkartenleser können an allen Hostsystemen verwendet werden, die eine serielle RS232 bzw. eine USB Schnittstelle besitzen und sind ausschliesslich für den Einsatz im nicht-öffentlichen oder privaten Bereich konzipiert.

Die Geräte arbeiten mit allen Chipkarten-Datenübertragungsprotokollen gemäß ISO/IEC 7816 [12] (T=0, T=1) und EMV 2000 [15]. Datenübertragungsprotokolle für Speicherchipkarten (I^2C-, 2-Wire-, 3-Wire-Protokoll) werden ebenfalls unterstützt Die sichere PIN-Eingabe wird jedoch nur für asynchrone Prozessor-Chipkarten angeboten.

Der Leser erkennt die von der Host-Software übermittelten Kommandos zur PIN-Eingabe nach CT-BCS [10] bzw. CCID [13] und fügt die vom Benutzer über das Keypad eingegebenen Nummern als PIN an die entsprechenden Stellen des Kommandos an die Chipkarte ein. Dabei wird der Modus der sicheren PIN-Eingabe eindeutig durch eine LED angezeigt und nur die Tatsache an den Host gemeldet, dass eine der numerischen Tasten gedrückt wurde. Dies dient der Host-Applikation dem Anwender zu visualisieren, dass er eine Taste gedrückt hat bzw. wie viele Ziffern der PIN aktuell eingegeben sind.

Da die Chipkartenleser als Klasse 2 Leser insbesondere in der Lage sind, Identifikationsdaten (PIN) zu erfassen und an sichere Signaturerstellungseinheiten (Signatur-Chipkarten) nach §2 Nummer 10 SigG zu übermitteln, können sie auch für Applikationen gemäß Signaturgesetz und Signaturverordnung ([16], [17]) eingesetzt werden. Sie dienen des Weiteren zur Übermittlung des Hash-Wertes von der Anwendung zur Signaturkarte und zur Rückübertragung der Signatur von der Karte zur Signaturanwendung. Sie stellen somit eine Teilkomponente für Signaturanwendungskomponenten dar, die eine Sicherheitsbestätigung benötigen, 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. Evaluierte und bestätigte Produkte sind auf den Webseiten der Bundesnetzagentur[9] aufgeführt.

Das Zertifikat bezieht sich auf die Hard- und Firmware für das Chipkartenterminal KAAN Advanced. Die Treiber für das Chipkartenterminal KOBIL KAAN Advanced sowie sonstige zur Installation auf dem Host vorgesehene Software sind nicht Bestandteil des EVG und somit nicht Bestandteil des Zertifikats.

Die Evaluation des Produkts Chipkartenterminal KAAN Advanced, Hardware Version K104R3, Firmware Version 1.02 wurde von der Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH – Prüfstelle für IT-Sicherheit durchgeführt und am 08. November 2006 abgeschlossen. Das Prüflabor Deutsches Forschungszentrum für

---

[8] Das Aufspielen einer anderen Firmware-Version als die Version 1.02 ist nicht Bestandteil dieses Zertifikats. Andere Firmware-Versionen müssen in einem weiteren Verfahren evaluiert und zertifiziert werden, damit der Chipkartenleser auch nach dem Update als zertifiziert gelten kann.

[9] siehe www.bundesnetzagentur.de

Künstliche Intelligenz (DFKI) GmbH – Prüfstelle für IT-Sicherheit ist eine vom BSI anerkannte Prüfstelle (ITSEF)[10].

Antragsteller, Hersteller und Vertreiber ist

KOBIL Systems GmbH
Pfortenring 11
67547 Worms, Deutschland

1.1 Vertrauenswürdigkeitspaket

Die Vertrauenswürdigkeitskomponenten sind komplett dem Teil 3 der Common Criteria entnommen (siehe Annex C oder [1], Teil 3). Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL3 mit Zusatz. Die folgende Tabelle führt die zusätzlichen Vertrauenswürdigkeitskomponenten auf.

Anforderung	Beschreibung
EAL3	methodisch getestet und überprüft
+: ADO_DEL.2	Auslieferung und Betrieb: Erkennung von Modifikationen
+: ADV_IMP.1	Entwicklung: Teilmenge der Implementierung
+: ADV_LLD.1	Entwicklung: Beschreibender Entwurf auf niedriger Ebene
+: ALC_TAT.1	Lebenzyklus-Unterstützung: Klar festgelegte Entwicklungswerkzeuge
+: AVA_MSU.3	Schwachstellenbewertung: Analysieren und Testen auf unsichere Zustände
+: AVA_VLA.4	Schwachstellenbewertung: Hohe Widerstandsfähigkeit

Tabelle 1: Vertrauenswürdigkeitskomponenten und EAL-Zusätze

1.2 Funktionalität

Die funktionalen Sicherheitsanforderungen (SFR) des EVG sind konform zum Teil 2 der Commen Criteria und in der folgenden Tabelle aufgeführt.

Sicherheitsanforderungen	Thema
FCS	**Kryptographische Unterstützung**
FCS_COP.1	Kryptographischer Betrieb
FDP	**Schutz der Benutzerdaten**
FDP_ACC.1	Teilweise Zugriffskontrolle
FDP_ACF.1	Zugriffskontrolle basierend auf Sicherheitsattributen
FDP_ETC.1	Export von Benutzerdaten ohne Sicherheitsattribute
FDP_RIP.1	Teilweiser Schutz bei erhalten gebliebenen Informationen
FDP_UCT.1	Einfache Vertraulichkeit des Datenaustausches
FPT	**Schutz der TSF**
FPT_PHP.1	Passive Erkennung materieller Angriffe

[10] Information Technology Security Evaluation Facility

Sicherheitsanforderungen	Thema
FPT_PHP.3	Wiederstand gegen materielle Angriffe
FTP	**Vertrauenswürdiger Pfad/Kanal**
FTP_TRP.1	Vertrauenswürdiger Pfad

Tabelle 2: SFRs für den EVG aus den CC Teil 2

Hinweis: Die obige Tabelle zeigt lediglich die Titel der funktionalen Sicherheitsanforderungen. Nähere Informationen und Anwendungsbemerkungen sind im Security Target [6], Kapitel 5.1, zu finden.

Die oben genannten Sicherheitsanforderungen werden durch die folgenden Sicherheitsfunktionen und –maßnahmen abgedeckt:

Sicherheitsfunktion	Beschreibung
SF.PINCMD	Die Firmware im Lesegerät prüft die Kommandos an den Chipkartenleser anhand ihrer Kommandostruktur gemäß CCID [13] bzw. CT-BCS [10]. Werden diese Kommandos als solche zum Verifizieren bzw. Modifizieren der PIN erkannt und ist ein an die Chipkarte weiterzuleitendes Kommando mit einem der folgenden Instruction-Bytes enthalten: • VERIFY (ISO/IEC 7816-4): INS=0x20 • CHANGE REFERENCE DATA (ISO/IEC 7816-8): INS=0x24 • ENABLE VERIFICATION REQUIR EMENT (ISO/IEC 7816-8): INS=0x28 • DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26 • RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C • UNBLOCK APPLICATION (EMV2000): INS=0x18 wird in den Modus zur sicheren Erfassung der PIN über das integrierte Keypad geschaltet. Die RS232- und die USB-Variante des EVG unterscheiden sich lediglich im Protokoll-Anbindungs-Modul an den Host, so dass bei beiden Host-Interface Varianten ein identischer Datenstrom durch die Sicherheitsfunktion bearbeitet wird. Die Sicherheitsfunktion SF.PINCMD erkennt die von der Host-Software übermittelten Kommandos zur PIN-Eingabe und fügt die über das Keypad 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. Der Benutzer kann die Eingabe der PIN mit der (roten) Abbruchtaste jederzeit abbrechen, wodurch die Übertragung der PIN zur Chipkarte verhindert wird. Je nach Kommando-Ausprägung muss der Benutzer die Eingabe der PIN mit der (grünen) Bestätigungstaste abschliessen (alternativ kann die PIN-Länge vorgegeben werden, so dass die letzte Ziffer der PIN die Eingabe abschliesst). Der Summer ist durch den Benutzer abschaltbar und somit nicht Teil der Sicherheitsleistung des EVG.
SF.CLMEM	Die Speicherbereiche für die PIN-Daten werden im Rahmen der sicheren PIN-Eingabe (SF.PINCMD) nach Übertragung des Kommandos an die Chipkarte (auch bei Kommunikationsfehlern oder zwischenzeitlich gezogener Karte), bei Abbruch durch den Anwender und bei einem Timeout während der PIN-Eingabe wiederaufbereitet. Nach der Wiederaufbereitung ist die PIN nicht mehr im Speicher des EVG vorhanden.

Sicherheitsfunktion	Beschreibung
SF.SECDOWN	Eine neue Firmware kann in den EVG eingespielt werden. Dazu wird der EVG in den Bootloader-Modus versetzt, in dem alle Funktionen des EVG deaktiviert werden, bis auf die Entgegennahme einer neuen Firmware, die mit einer elektronischen Signatur des Herstellers versehen ist. Aus dem Bootloader-Modus kann nur eine neu entgegengenommene, korrekt signierte Firmware wieder aktiviert werden, eine Rückkehr zur vormals installierten Firmware ist nicht mehr möglich. Eine entgegengenommene Firmware mit fehlerhafter Signatur wird nicht aktiviert, sondern es wird wieder in den Bootloader-Modus verzweigt, der wiederum auf eine neue Firmware wartet. Die Verifikation einer Signatur der Firmware mit dem asymmetrischen ECDSA-Algorithmus und einer Bitlänge von 192 garantiert die Integrität und Authentizität der Firmware beim Laden einer neuen Firmware in den Chipkartenleser.Der Hash-Wert über die neu zu ladende Firmware wird basierend auf dem Algorithmus SHA-1 mit einer Länge von 160 Bit ermittelt. Die Verifikation der Integrität und Authentizität erfolgt im EVG durch Vergleich des ermittelten Hash-Wertes und des Hash-Wertes als Bestandteil der entschlüsselten Signatur. Der öffentliche Schlüssel ist hierfür im EVG gespeichert.
Sicherheitsmaßnahme SF.SEAL	Das Gehäuse des EVG ist durch eine Versiegelung so verschlossen, dass es ohne eine Beschädigung der Versiegelung nicht geöffnet werden kann. Die Versiegelung ist so beschaffen, dass eine Ablösung vom Untergrund (also vom Gehäuse) nicht ohne erkennbare Beschädigung der Versiegelung möglich ist.

Tabelle 3: Sicherheitsfunktionen und –maßnahmen des EVG

1.3 Stärke der Funktionen

Die Stärke der Funktionen des EVG ist für bestimmte Funktionen, wie in den Sicherheitsvorgaben [6, Kap. 8.2] angegeben, mit SOF-hoch postuliert.

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

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

Alle Bedrohungen gehen von einem Angreifer mit einem hohen Angriffpotential aus. Die zu schützenden Objekte sind die PIN als Identifikationsmerkmal des Karteninhabers sowie die Firmware und die Hardware des EVG. Folgende Bedrohungen für die zu schützenden Objekte wurden identifiziert:

Bedrohung	Zusammenfassung
T.REVEAL.1	Abhören der Kommunikation zwischen Host und Kartenlesers zum Ausspähen der PIN.
T.REVEAL.2	Ausspähen der PIN durch Senden eines Kommandos an den Kartenleser.
T.STORE.1	Auslesen von dauerhaft gespeicherten Daten.
T.MODIFY.1	Modifikation der Firmware
T.MODIFY.2	Manipulation der Hardware nach Öffnen des Gehäuses

Tabelle 4: Bedrohungen für den EVG

Organisatorische Sicherheitspolitiken sind im Security Target nicht angegeben.

1.5 Spezielle Konfigurationsanforderungen

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

Chipkartenterminal KAAN Advanced, Hardware Version K104R3, Firmware Version 1.02 des Herstellers KOBIL Systems GmbH.

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

Eine Konfiguration des EVG und eine damit verbundene Beeinflussung der Sicherheitsfunktionen durch den Nutzer ist nicht möglich. Das Aufspielen einer anderen Firmware als die in diesem Zertifikat genannte Version 1.02 stellt keine Konfiguration sondern eine Veränderung des EVG dar, die nicht Bestandteil des Zertifikats ist.

1.6 Annahmen über die Einsatzumgebung

Das Chipkartenterminal KAAN Advanced ist für den Gebrauch im privaten und nicht öffentlichen Bereich vorgesehen. Hinsichtlich der Benutzung des EVG werden die folgenden Annahmen im Security Target [6, Kapitel 3.1] genannt:

Annahme	Zusammenfassung
A.USER.RESP1	Sichere Handhabung und Nichtweitergabe der Signatur-PIN.
A.USER.RESP2	Überprüfung der LEDs bei der sicheren PIN-Eingabe
A.USER.RESP3	Überprüfung der Angabe von Zertifizierungs- und Bestätigungskennung beim Download von Firmware für das Chipkartenterminal KAAN Advanced.
A.USER.RESP4	Überprüfung der Versiegelung
A.USER.RESP5	Einsatz nur im privaten oder nicht-öffentlichen Bereich
A.USER.RESP6	Verwendung im Rahmen der qualifizierten elektronischen Signatur nur mit entsprechenden sicheren Signaturerstellungseinheiten
A.USER.RESP7	Verwendung im Rahmen der qualifizierten elektronischen Signatur nur zusammen mit entsprechenden Signaturanwendungskomponenten

Tabelle 5: Annahmen

1.7 Gewährleistungsausschluß

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

2 Identifikation des EVG

Der EVG heisst:

Chipkartenterminal KAAN Advanced,
Hardware Version K104R3, Firmware Version 1.02

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Type	Bezeichnung	Version	Form der Auslieferung
1	HW	Hardware KAAN Advanced (Hauptplatine im Gehäuse mit Anschlusskabel USB oder RS232)	K104R3	Einzelverpackung
2	SW	Firmware KAAN Advanced	1.02	• Download von http://www.kobil.de • Vorinstalliert auf der Hardware
3	DOK	Bedienungsanleitung KAAN Base & KAAN Advanced (USB /RS232)	DB11.DEEN.2	pdf oder gedrucktes Dokumenten
4	SW	Installations-CD mit Tools zum Aufspielen neuer Firmware und zur Überprüfung der Firmware-Version		• CD-ROM • Donwload von http://www.kobil.de

Tabelle 6: Auslieferungsumfang des EVG

Abgesehen von der Benutzerdokumentation sind die Inhalte der CD (Punkt 4 in Tabelle 6) nicht Gegenstand der Evaluierung.

Hinsichtlich der Auslieferung des EVG oder von Bestandteilen des EVGs gibt es die folgenden zwei Alternativen.

2.1 Auslieferung von Firmware zusammen mit Hardware

Vom Produzenten werden die fertig montierten und mit der Firmware Version 1.02 ausgestatteten Chipkartenterminals KAAN Advanced zum Auslieferungslager der Firma KOBIL Systems GmbH versendet. Dort erfolgt die Verpackung in Einzelkartons unter Beilegung der Bedienungsanleitung in gedruckter Form und der Software CD. Bei dieser Auslieferungsart umfasst der Lieferumfang des EVG die Punkte 1, 3 und 4 aus Tabelle 6.

Ein Benutzer kann einen zertifizierten Chipkartenleser an der auf dem Typschild vermerkten Hardware-Version des EVG erkennen und die Firmware-Version mit dem vom Hersteller bereitgestellten Tool auslesen.

2.2 Auslieferung der Firmware über das Internet

Über die Internet-Seiten des Herstellers KOBIL Systems GmbH (http://www.kobil.de oder http://www.kobil.com) kann der Benutzer die Firmware Version 1.02 sowie die Benutzerdokumentation herunterladen. Die zertifizierte Firmware ist dabei als solche eindeutig gekennzeichnet. Der Benutzer muss beim Herunterladen diese Kennzeichnungen beachten, da im Umfang dieses Zertifikats nur das Aufspielen der zertifizierten Firmware-Version 1.02 enthalten ist. Bei dieser Auslieferungsart umfasst der Lieferumfang somit die Punkte 2 und 3 der Tabelle 6.

Beim Aufspielen der Firmware auf ein Chipkartenterminal KAAN Advanced muss der Benutzer beachten, dass die auf dem Typschild des Gerätes angegebene Hardware-Version mit der in diesem Zertifikat genannten Hardware-Version K104R3 übereinstimmt.

Treiber und Tools zum Aufspielen oder Auslesen der Version der Firmware können ebenfalls von den o.g. Internetseiten heruntergeladen werden, wobei die CD in ihrem Originalumfang nicht bereit gestellt wird und somit auch nicht zum Lieferumfang bei der Auslieferung über das Internet gehört.

3 Sicherheitspolitik

Die Sicherheitseigenschaften des EVG dienen vor allem dazu, das Gerät für die Anwendung von qualifizierten elektronischen Signaturen verwenden zu können.

Um eine qualifizierte elektronische Signatur ausstellen zu können, muss sich ein Benutzer durch den Besitz einer sicheren Signaturerstellungseinheit und das Wissen der Signatur-PIN authentisieren. Die Signatur-PIN wird dabei vom Benutzer auf dem Chipkartenterminal eingegeben.

Die Sicherheitspolitik des Chipkartenterminals KAAN Advanced zielt demnach auf den Schutz der PIN und der Integrität der Firmware sowie auf die zuverlässige Anzeige von sicherheitstechnischen Änderungen an der Hardware ab.

4 Annahmen und Klärung des Einsatzbereiches

4.1 Annahmen über den Einsatz

Die folgenden Annahmen aus dem Security Target [6, Kap. 3.1] müssen beim Einsatz des EVG durch den Benutzer beachtet werden:

Annahme	Inhalt
A.USER.RESP1	Die Regeln zur sicheren Handhabung und Nichtweitergabe der PIN werden dem Anwender vom Herausgeber der Chipkarte mitgeteilt, insbesondere die unbeobachtete Eingabe der PIN.
A.USER.RESP2	Während der PIN-Eingabe über das Keypad des Lesers überprüft der Endanwender den Status der LEDs dahingehend, dass der Mode der sicheren PIN-Eingabe aktiv ist.
A.USER.RESP3	Zertifizierte bzw. bestätigte Firmware, die von KOBIL Systems zum Download angeboten wird, ist durch Angabe der Zertifizierungs- bzw. Bestätigungs-IDs gekennzeichnet. Der Endanwender überzeugt sich vor der Installation einer neuen Firmware davon, dass diese nach SigG [16] / SigV [17] bestätigt und nach Common Criteria [1] zertifiziert ist.
A.USER.RESP4	Der Endanwender prüft die Versiegelung vor jeder PIN-Eingabe auf Unversehrtheit.

Tabelle 7: Annahmen über den Einsatz des EVG

4.2 Angenommene Einsatzumgebung

Hinsichtlich der Einsatzumgebung des EVG muss der Endanwender insbesondere bei der Erzeugung qualifizierter elektronischer Signaturen die folgenden Vorgaben beachten:

Annahme	Zusammenfassung
A.USER.RESP5	Der EVG wird ausschliesslich im nicht-öffentlichen oder privaten Bereich eingesetzt.
A.USER.RESP6	Für die qualifizierte Signatur wird der EVG nur in Verbindung mit Signatur-Chipkarten (Sichere Signatur-Erstellungseinheit, SSEE) verwendet, die den Anforderungen des SigG [16] / SigV [17] entsprechen.
A.USER.RESP7	Für die qualifizierte Signatur wird der EVG nur in Verbindung mit Signatur-Anwendungskomponenten verwendet, die den Anforderungen des SigG [16] / SigV [17] entsprechen.

Tabelle 8: Annahmen über die Einsatzumgebung

5 Informationen zur Architektur

5.1 Hardware

Die Hardware des TOE(EVG) besteht aus einem versiegelten Gehäuse, über das folgende Schnittstellen nach außen geführt sind:

- Hostanbindung (USB oder RS232)
- Chipkartenschnittstelle und
- Tastatur, LEDs und Summer

Im Gehäuse befindet sich die Hauptplatine, die mit allen wesentlichen Bauteilen für die Ausführung der Firmware bestückt ist. Die Grundstruktur des EVG folgt der von-Neumann-Architektur mit einem Prozessor. Der Speicher ist logisch in Programm- und Datenspeicher aufgeteilt, die getrennt addressiert werden. Code kann nur ausgeführt werden, wenn er im Programmspeicher liegt. Physisch teilt sich der Speicher in einen flüchtigen Anteil (CRAM) auf dem Prozessorchip sowie nicht flüchtige Anteile (EEPROM) auf.

5.2 Firmware

Die Firmware gliedert sich in zwei Teile, die separat voneinander ausgeführt werden und die beiden Betriebsmodi Update-Modus und normaler Betriebsmodus realisieren.

Der Update-Modus dient dazu, eine neue Firmware zu installieren. Dabei nimmt die auf dem Gerät vorhandene Firmware die neue Firmware über das DFU-Protokoll vom Host entgegen und prüft deren Signatur. Ist die Prüfung erfolgreich verlaufen, wird die Firmware in den dafür vorgesehenen Anteil des EEPROM geschrieben und das Chipkartenterminal so eingestellt, dass der nächste Start im normalen Betriebsmodus erfolgt. Schlägt die Signaturprüfung fehl, so verbleibt das Gerät im Update-Modus.

Im normalen Betriebsmodus nimmt der EVG Kommandos vom Host entgegen und führt sie aus bzw. leitet sie an die Chipkartenschnittstelle weiter. Aus dem normalen Betriebsmodus kann mit Hilfe spezieller Kartenterminal-Kommandos zum Update-Modus übergegangen werden.

6 Dokumentation

Für das Chipkartenterminal KAAN Advanced stellt der Hersteller die folgende Dokumentation bereit:

- Bedienunsanleitung und Sicherheitshinweise KAAN Base & KAAN Advanced (USB+RS232), Dokumenten-ID DB11.DEEN.2.

7 Testverfahren

7.1 Testverfahren des Herstellers

Die Testkonfiguration, die vom Hersteller während der Tests benutzt wurde, entspricht der auszuliefernden Konfiguration des EVG (siehe Kapitel 2). Der Testansatz basiert auf der Überprüfung des Verhaltens der Sicherheitsfunktionen an den externen Schnittstellen. Hierfür wurden neben einem PC mit Windows 2000 (SP4) spezifische Werkzeuge und Hilfsmittel eingesetzt, die eine präzise Ansteuerung und Beobachtung der über die externen Schnittstellen ausgetauschten Daten ermöglichen. Darüber hinaus hat der Hersteller einzelne Sicherheitsfunktionen speziell untersucht.

Die Testabdeckung und -tiefe der Herstellertests orientiert sich an den EVG-Sicherheitsfunktionen. Alle Sicherheitsfunktionen sind mindestens einem Test unterzogen worden. Hierbei wurden alle relevanten Details der funktionalen Spezifikation und des Entwurfs auf hoher Ebene berücksichtigt.

Alle Tests bestätigten das korrekte Verhalten der Sicherheitsfunktionen.

7.2 Unabhängige Funktionstests der Prüfstelle

Die Prüfstelle hat ihre Tests an einem handeslüblichen Gerät durchgeführt, das wie in Kapitel 2.1 beschrieben ausgeliefert wird.

Der Evaluator hat zu allen drei Sicherheitsfunktionen (SF.SECDOWN, SF.PINCMD und SF.SEAL, siehe Kapitel 1.2), die von außen beobachtbar sind, unabhängige Tests entwickelt, durchgeführt und aufgezeichnet. Hierfür wurden neben PCs mit Windows XP bzw. Linux (Kernel 2.6.11) Treiber von KOBIL und spezifische Testsoftware verwendet. Im Rahmen einer Stichprobe wurden darüberhinaus in der Testumgebung des Entwicklers weitere Tests wiederholt.

In sämtlichen durchgeführten Tests wurde das korrekte Verhalten der Sicherheitsfunktionen festgestellt.

7.3 Penetrationstests der Prüfstelle

Ausgehend von der Analyse der Schwachstellen des Entwicklers und des Evaluators hat der Evaluator Penetrationstests konzipiert und durchgeführt. Hierbei sollten Herstelleraussagen zur Nichtausnutzbarkeit von Schwachstellen anhand von gezielten Tests überprüft und zusätzlich weitere mögliche Schwachstellen mit Testfällen abgedeckt werden. Durch Verwendung von quelloffenen Treibern hat der Evaluator eine größere Unabhängigkeit von der Hostumgebung erreicht und zusätzliche Testmöglichkeiten genutzt.

Bei einem Test wurde eine Abweichung vom erwarteten Ergebnis festgestellt. Die Bewertung des Evaluators ergibt jedoch, daß die Durchführung des Angriffs jenseits normaler Praktikabilität liegt und die Schwachstelle somit residual ist.

8 Evaluierte Konfiguration

Die Tests von Hersteller und Prüfstelle wurden an handelsüblichen Geräten durchgeführt. Das Zertifikat bezieht sich somit auf das folgende Produkt:

Chipkartenterminal KAAN Advanced,
Hardware Version K104R3, Firmware Version 1.02

Die Standorte für die Entwicklung und Fertigung des EVG sind Bestandteil der Evaluierung. Daher ist es verpflichtend, dass der TOE an den folgenden Entwicklungs- und Produktionsstätten hergestellt wird:

- Gebäude der KOBIL Systems GmbH
  Pfortenring 11
  67547 Worms
- Q&S Manufacturing Co., Ltd., Factory Building A
  Fu Gang Village, Qing Xi Town, Dongguan City, China
  Postal Code 523658

9 Ergebnisse der Evaluierung

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

Die Evaluationsmethodology CEM [2] wurde für die Komponente aus dem Vertrauenswürdigkeitsstufe EAL3 verwendet. Für Komponenten oberhalb von EAL4 wurde die Methodology in Zusammenarbeit mit der Zertifizierungsstelle festgelegt [4, AIS 34]).

Das Urteil für die CC, Teil 3 Anforderungen an die Vertrauenswürdigkeit (gemäß EAL3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4 und die Klasse ASE für die Sicherheitsvorgaben) sind in der folgenden Tabelle dargestellt.

Vertrauenskeitsklassen und Komponenten	Kurzform	Urteil
Prüfung und Bewertung der 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

Vertrauenskeitsklassen und Komponenten	Kurzform	Urteil
Konfiguratationsmanagement	CC Klasse ACM	PASS
Autorisierungskontrolle	ACM_CAP.3	PASS
EVG-CM-Umfang	ACM_SCP.1	PASS
Auslieferung und Betrieb	CC Klasse ADO	PASS
Erkennung von Modifikationen	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
Teilmenge der Implementierung der TSF	ADV_IMP.1	PASS
Beschreibender Entwurf auf niedriger Ebene	ADV_LLD.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
Lebenszyklus-Unterstützung	CC Klasse ALC	PASS
Identification der Sicherheitsmaßnahmen	ALC_DVS.1	PASS
Klar festgelegte Entwicklerwerkzeuge	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
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

Tabelle 9: Urteil zu den Vertrauenswürdigkeitskomponenten

Die Evaluierung hat gezeigt, dass:

- die Sicherheitsanforderungen für den EVG aus den Sicherheitsvorgaben konform zu Common Criteria Part 2 sind
- die Vertrauenswürdigkeit des EVG Common Criteria Teil 3 konform ist, EAL3 mit Zusatz von ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 und AVA_VLA.4.

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

(i) die EVG Sicherheitsfunktion SF.SECDOWN

Die Resultate der Evaluierung sind nur anwendbar auf den EVG Chipkartenterminal KAAN Advanced, Hardware Version K104R3, Firmware Version 1.02 (siehe Kapitel 2).

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

10 Auflagen und Empfehlungen

10.1 Auflagen und Empfehlungen für den Hersteller

Vor jeder Auslieferung einer neuen Version der Firmware mit veränderter Sicherheitsfunktionalität muss der Hersteller ein neues Signaturschlüsselpaar für die Erzeugung und Prüfung der Firmware-Signatur verwenden. Somit kann ohne Benutzerinteraktion allein durch die Signaturprüfung im EVG verhindert werden, dass ältere Versionen installiert werden.

Bei der Signatur der Firmware (siehe die Sicherheitsfunktion SF.SECDOWN in Kapitel 1.2) verwendet der Hersteller Algorithmen, die bis Ende 2009 für die Erstellung von qualifizierten elektronischen Signaturen geeignet sind (siehe [18], Kapitel 3.2a), aber in diesem Verfahren nicht separat bewertet wurden. Sollten sich die gewählten Parameter als nicht mehr ausreichend zur Sicherung der Integrität und Authentizität der Firmware erweisen, müssen entsprechend stärkere Algorithmen gewählt werden. Es wird empfohlen, spätestens bis Ende 2009 die Algorithmen entsprechend den Einschätzungen der Bundesnetzagentur zu verstärken.

10.2 Empfehlungen für den Benutzer

Die Sicherheitsvorgaben [6] und die Benutzerdokumentation [8] enthalten die notwendigen Informationen über die Verwendung des EVG sowie die Sicherheitshinweise.

11 Anhänge

Keine

12 Sicherheitsvorgaben

Die Sicherheitsvorgabe [6] wird zur Veröffentlichung in einem separaten Dokument bereitgestellt.

13 Definitionen

13.1 Abkürzungen

BSI Bundesamt für Sicherheit in der Informationstechnik, Bonn

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

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

IT Informationstechnik

PP Protection Profile - Schutzprofil

SF Sicherheitsfunktion

SOF Strength of Function - Stärke der Funktionen

ST Security Target - Sicherheitsvorgaben

EVG Evaluationsgegenstand

TSC TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle

TSF TOE Security Functions - EVG-Sicherheitsfunktionen

TSP TOE security policy - EVG-Sicherheitspolitik

13.2 Glossar

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

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

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

Informell - Ausgedrückt in natürlicher Sprache.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Literaturangaben

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

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

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

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

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

[6] Sicherheitsvorgaben BSI-DSZ-0301-2006, Version 1.19, 30.05.2006, KOBIL Chipkartenterminal KAAN Advanced (USB/RS232) Security Target, KOBIL Systems GmbH

[7] Evaluierungsbericht, 1.2, 03.11.2006, Evaluierung KAAN Advanced Evaluierungsbericht (vertrauliches Dokument)

[8] Bedienungsanleitung KAAN Base & KAAN Advanced (USB / RS232), Dokument-ID DB11.DEEN.2, KOBIL Systems GmbH

[9] Anwendungsunabhängiges CardTerminal Application Programming Interface (CT-API) für Chipkartenanwendungen, Revision 1.1, 14. 10. 1998, Deutsche Telekom AG (PZ Telesec), GMD Darmstadt, TÜV Iformationstechnik GmbH, TeleTrusT Deutschland e.V.

[10] Multifunktionale KartenTerminals (MKT) – Spezifikation, Teil 4: Anwendungsunabhängiger CardTerminal Basic Command Set (CT-BCS), Version 1.0, 15. 04. 1999, TeleTrusT Deutschland e.V.

[11] Interoperability Specification for ICCs and Personal Computer Systems, Revision 1.0, December 1997, PC/SC Workgroup

[12] Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange, 2005-01-05 und

Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Commands for security operations, 2004-06-11,

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

[13] Universal Serial Bus Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00, March 20, 2001, USB Implementors Forum, Inc.; Device Working Group (DWG)

[14] Druckschrift 7500: Produkte für die materielle Sicherheit, Oktober 2000, Bundesamt für Sicherheit in der Informationstechnik (BSI) (vertrauliches Dokument)

[15] EMV™ Integrated Circuit Card Specifications for Payment Systems, Version 4.0, 2000, EMVCo LLC

[16] Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG), 16. 05. 2001, BGBl. I, S. 876ff, 21. 05. 2001. Geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04. 01. 2005, BGBl. I, S. 2f, 10. 01. 2005

[17] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. 11. 2001, BGBl. I, S. 3074ff, 21. 11. 2001. Geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04. 01. 2005, BGBl. I, S. 2f, 10. 01. 2005.

[18] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 2. Januar 2006, veröffentlicht am 23. März 2006 im Bundesanzeiger Nr. 58, S. 1913-1915

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.