Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-CC-0480-2009

zu

EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A03, Firmware Version 69.18), SecOVID Reader III (Artikel-Nr. HCPNCKS/B05, Firmware Version 69.18) und KAAN TriB@nk (Artikel-Nr. HCPNCKS/C05, Firmware Version 68.17)

der

KOBIL Systems 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-0480-2009

Signaturanwendungskomponente

EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A03, Firmware V. 69.18), SecOVID Reader III (Artikel-Nr. HCPNCKS/B05, Firmware V. 69.18) und KAAN TriB@nk (Artikel-Nr. HCPNCKS/C05, Firmware V. 68.17)

von	KOBIL Systems GmbH
PP-Konformität:	Keine
Funktionalität:	Common Criteria Teil 2 konform
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 akkreditierten und lizenzierten Prüfstelle nach der Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 und Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL 4 unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005) evaluiert.

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

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

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

Bonn, 12. Januar 2009

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

IT Security Certified

SOGIS - MRA

Bernd Kowalski L.S.
Abteilungspräsident

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

Dies ist eine eingefügte Leerseite.

Vorbemerkung

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

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

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

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

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

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

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

Gliederung

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

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

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

2 Anerkennungsvereinbarungen

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

2.1 Europäische Anerkennung von ITSEC/CC - Zertifikaten

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

Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der

---

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

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

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

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

Evaluationsstufe EAL7 erweitert. Das BSI erkennt die Zertifikate der nationalen Zertifizierungsstellen von Frankreich und Großbritannien im Rahmen dieses Abkommens an.

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

2.2 Internationale Anerkennung von CC - Zertifikaten

Im Mai 2000 wurde eine Vereinbarung (Common Criteria-Vereinbarung) über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und Schutzprofilen auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 verabschiedet (CC-MRA).

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

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

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

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

3 Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Produkt in den Varianten EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A03, Firmware Version 69.18), SecOVID Reader III (Artikel-Nr. HCPNCKS/B05, Firmware Version 69.18) und KAAN TriB@nk (Artikel-Nr. HCPNCKS/C05, Firmware Version 68.17) hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts in den Varianten EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A03, Firmware Version 69.18), SecOVID Reader III (Artikel-Nr. HCPNCKS/B05, Firmware Version 69.18) und KAAN TriB@nk (Artikel-Nr. HCPNCKS/C05, Firmware Version 68.17) wurde von der Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH durchgeführt. Die Evaluierung wurde am 10. Dezember 2008 beendet. Das Prüflabor Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Sponsor, Antragsteller und Entwickler ist: KOBIL Systems 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 in den Varianten EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A03, Firmware Version 69.18), SecOVID Reader III (Artikel-Nr. HCPNCKS/B05, Firmware Version 69.18) und KAAN TriB@nk (Artikel-Nr. HCPNCKS/C05, Firmware Version 68.17) ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

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

[7] KOBIL Systems GmbH
Pfortenring 11
67547 Worms

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) sind die Chipkartenterminals KOBIL Chipkartenterminals EMV-TriCAP Reader, SecOVID Reader III und KAAN TriB@nk.

Der EVG stellt Funktionen für das Lesen von Chipkarten bereit. Er verfügt über ein LCD, eine Tastatur zur sicheren PIN-Eingabe sowie eine updatefähige Firmware. Die drei existierenden Bauformen unterscheiden sich in der Firmware, nicht jedoch durch die Hardware betreffende Merkmale.

Der Anschluss an einen PC erfolgt über eine Docking Station, die an eine USB-Schnittstelle des PCs (Online-Betrieb) angeschlossen wird. Im Online-Betrieb stellen alle drei Chipkartenterminals gleichermaßen die folgende Funktionalität zur Verfügung, die Bestandteil der Evaluierung und damit des vorliegenden Zertifikats ist:

- Sichere Entgegennahme der Identifikationsdaten (PIN) vom Benutzer und Weitergabe derselben ausschließlich an die Sichere Signatur-Erstellungseinheit (SSEE).
- Anzeige des Betriebsmodus der sicheren PIN Eingabe
- Sicherer Software-Download für Aktualisierungen des EVG
- Erkennbarkeit sicherheitstechnischer Veränderungen am EVG

Die Geräte können auch ohne Anschluss an den Host-PC betrieben werden (Offline-Betrieb). Sie unterscheiden sich dann durch die folgenden unterschiedlichen Leistungsmerkmale, die sie nur im Offline-Betrieb bereitstellen. Die folgende Funktionalität im Offline-Betrieb ist **nicht** Bestandteil der Evaluierung und des Zertifikats:

- **EMV-TriCAP Reader:** Erzeugung von Kreditkarten-Authentifikationsdaten gemäß EMV-CAP zum sicheren Bezahlen und Online Banking im Internet, sowohl im Offline- als auch im Online-Betrieb.
- **SecOVID Reader III:** Erzeugung von Einmal-Passwörtern mit Hilfe von Chipkarten nach dem KOBIL SecOVID Verfahren für alle Arten von Benutzer-Authentisierungen.
- **KAAN TriB@nk:** Erzeugung von Einmal-Passwörtern gemäß dem SmartTAN(+) Verfahren für sicheres Online Banking sowie das Auslesen der GeldKarte. Außerdem steht die Secoder Funktion für den Zugriff auf die ZKA SECCOS Chipkarte bereit.

Ziel der Evaluierung und Zertifizierung ist die Verwendung der Chipkartenterminals im Online-Betrieb im Rahmen der Erzeugung qualifizierter elektronischer Signaturen gem. SigG / SigV [14, 15].

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

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

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements, SFR) an den EVG werden in den Sicherheitsvorgaben [6] Kapitel 5.1 beschrieben. Sie wurden komplett dem Teil 2 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 5.3 dargestellt.

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

Sicherheitsfunktion des EVG	Zusammenfassung
SF.PINCMD	Sichere PIN-Eingabe über das Tastenfeld des Kartenlesers. Dabei erkennt die Firmware von der Host-Software übermittelte Kommandos zur PIN-Eingabe und fügt die über das Keypad eingegebenen Nummern als PIN an die entsprechenden Stellen des Kommandos an die Chipkarte ein. Im Rahmen der sicheren PIN-Eingabe, die eindeutig im Display angezeigt wird, verlässt die PIN das Gerät ausschließlich in Richtung Chipkarte.
SF.CLMEM	Während der Verarbeitung im Speicher des Lesers befindliche PIN-Daten werden nach Abschluss der PIN-Eingabe (auch im Fehlerfall), bei Abbruch durch den Anwender und bei einem Timeout während der PIN-Eingabe aufbereitet, so dass diese nicht mehr vorhanden sind.
SF.SECDOWN	Ein Firmwareupdate wird erst nach erfolgreicher Prüfung der eingebetteten Signatur aktiviert.
SF.SEAL	Relevante innere Bereiche des Gehäuses können nur durch sichtbares Beschädigen der Versiegelung erreicht werden.

Tabelle 1: Sicherheitsfunktionen des EVG

Die Beschreibung der Sicherheitsfunktionen in Tabelle 1 ist eine Zusammenfassung der Darlegung in den Sicherheitsvorgaben. Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 6.1 dargestellt.

Die in den Sicherheitsvorgaben [6], Kapitel 5.1 für bestimmte Funktionen angegebene Stärke der Funktionen “hoch” wird bestätigt.

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

Dieses Zertifikat umfasst die folgenden Ausprägungen des EVG im Online-Betrieb:

- EMV TriCAP Reader
- SecOVID Reader III
- KAAN Trib@nk

Für mehr Details siehe Kapitel 8.

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:

EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A03, Firmware Version 69.18), SecOVID Reader III (Artikel-Nr. HCPNCKS/B05, Firmware Version 69.18) und KAAN TriB@nk (Artikel-Nr. HCPNCKS/C05, Firmware Version 68.17)

Die folgenden Tabellen beschreiben den Auslieferungsumfang, der sich bei den Produktvarianten unterscheidet:

Nr	Typ	Identifier	Version/ Artikelnummer	Auslieferungsart
1	HW	KOBIL Chipkartenterminal EMV-TriCAP Reader	Art. Nr. HCPNCKS/A03	Einzelverpackung
2	SW	Firmware EMVTriCAP, zusammen mit einer Setup-Routine zum Laden der Firmware auf das Chipkartenterminal	Version 69.18 – EMVTriCAP	● Download von http://www.kobil.de ● Vorinstalliert auf der Hardware
3	DOC	KOBIL EMV-TriCAP Reader – Manual	Dokumenten-ID DB22.DEEN.1, Version 2.10 vom 21. 05. 2008	PDF oder gedrucktes Dokument

Tabelle 2: Auslieferungsumfang des EVG als EMV-TriCAP Reader

Nr	Typ	Identifier	Version/ Artikelnummer	Auslieferungsart
1	HW	KOBIL Chipkartenterminal SecOVID Reader III	Art. Nr. HCPNCKS/B05	Einzelverpackung
2	SW	Firmware SecOVID III, zusammen mit einer Setup-Routine zum Laden der Firmware auf das Chipkartenterminal	Version 69.18 – SecOVID III	● Download von http://www.kobil.de ● Vorinstalliert auf der Hardware
3	DOC	KOBIL SecOVID Reader III – Manual	Dokumenten-ID DB21.DEEN.1, Version 2.16 vom 21. 05. 2008	PDF oder gedrucktes Dokument

Tabelle 3: Auslieferungsumfang des EVG als SecOVID III

Nr	Typ	Identifier	Version/ Artikelnummer	Auslieferungsart
1	HW	KOBIL Chipkartenterminal KAAN TriB@nk	Art. Nr. HCPNCKS/C05	Einzelverpackung
2	SW	Firmware KAANTriB@nk, zusammen mit einer Setup-Routine zum Laden der Firmware auf das Chipkartenterminal	Version 68.17 – KAANTriB@nk	● Download von http://www.kobil.de ● Vorinstalliert auf der Hardware
3	DOC	KAAN TriB@nk – Manual	Dokumenten-ID DB25.DE.1, Version 1.17 vom 21. 05. 2008	PDF oder gedrucktes Dokument
4	DOC	KAAN TriB@nk Beipackzettel	Version 1.19 vom 10. 11. 2008	gedrucktes Dokument

Tabelle 4: Auslieferungsumfang des EVG als KAAN TriB@nk

Zusätzlich zu den in Tabelle 2, Tabelle 3 und Tabelle 4 genannten Punkten wird der EVG in jeder der drei Varianten mit einer Docking-Station und einem USB-Kabel zum Anschluss an einen PC ausgeliefert. Außerdem stellt der Hersteller das Dokument

- KOBIL EMV-TriCAP Reader, SecOVID Reader III, KAAN TriB@nk – Developer Notes, Version 1.0, 23. 10. 2008

für Entwickler auf Anfrage zur Verfügung, die das Produkt in ihre Software integrieren möchten.

Zusätzlich ist in der Einzelverpackung eine CD-ROM beigelegt, auf der Treiber und weiterführende Software zu finden sind. Diese Anteile sind nicht Bestandteil der Evaluierung.

Zur Identifizierung des EVG kann der Endnutzer das Typenschild auf der Rückseite des Gerätes nutzen, das u.a. die Artikel-Nummer beinhaltet. Exemplarisch enthält ein Typenschild auf der Rückseite eines KOBIL KAAN TriB@nk neben verschiedenen Logos und einem Barcode folgenden Text:

```
KOBIL KAAN TriB@nk
HCPNCKS/C05
HW: KCT106r1
SNR: SB081200300
```

Die Version der Firmware wird beim Start des Gerätes im Display angezeigt. Die Version der Dokumentation ist auf der ersten Seite (KAAN Trib@nk) bzw. der letzten Seite (EMV-TriCAP und SecOVID III) der Dokumentation abgedruckt.

Das Gerät ist mit Siegeln jeweils links und rechts unterhalb des Displays sowie ein Siegel an der Gehäuseunterkante gesichert.

2.1 Materielle Auslieferung

Der EVG wird einschließlich Bedienungsanleitung, Docking Station und ergänzender Software auf CD (nicht Teil des EVG) betriebsbereit an den Endkunden ausgeliefert. Bis auf die Treiberinstallation, die aus der Evaluierung ausgenommen ist, ist keine Installation notwendig. Die jeweilige Ausprägung der Firmware ist vom Hersteller in die Hardware eingebracht.

2.2 Elektronische Auslieferung

Die zweite Möglichkeit der Auslieferung besteht in der Bereitstellung der signierten Firmware auf der Webseite des Herstellers. Die Installation der Firmware ist in den ausgelieferten Handbüchern (Booklets) beschrieben, wobei es keinen Unterschied zwischen den Produktvarianten gibt. Im Abschnitt „Firmware-Update“ sind die folgenden Schritte zum Aufspielen der neuen Firmware beschrieben:

- Laden der Firmware von der Web-Site des Herstellers,
- Starten des Programms und Befolgen der am PC-Bildschirm angezeigten Anweisungen,
- Folgeaktionen, falls das Update mit der Meldung „Update failed“ am LCD abgebrochen wird.

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 „qualifizierte elektronische Signatur“ nach dem deutschen Signaturgesetz [14] einzusetzen. Um ein Dokument qualifiziert elektronisch zu signieren, muss sich ein Benutzer u.a. durch Besitz (Signaturkarte) und Wissen (PIN) gegenüber seiner Signaturkarte authentifizieren.

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

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

4 Annahmen und Klärung des Einsatzbereiches

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

Sicherheitsziel für die Umgebung	Zusammenfassung
OE.USER.RESP1	Der Nutzer wird vom Herausgeber der Chipkarte über den Umgang mit der PIN, speziell bei der Eingabe am Leser, belehrt.
OE.USER.RESP2	Der Nutzer prüft vor der PIN-Eingabe die Anzeige im LC-Display dahingehend, dass der Modus zur sicheren PIN-Eingabe aktiv ist.
OE.USER.RESP3	Der Nutzer verwendet nur zertifizierte und bestätigte Hard- und Software-Versionen des EVG, speziell dessen Firmware.
OE.USER.RESP4	Der Nutzer prüft die Versiegelung vor jeder PIN-Eingabe auf Unversehrtheit.
OE.USER.RESP5	Der EVG wird ausschließlich in nicht-öffentlichen oder privaten Bereichen eingesetzt.
OE.USER.RESP6	Für die Erzeugung qualifizierter Signaturen wird der EVG nur in

Sicherheitsziel für die Umgebung	Zusammenfassung
	Verbindung mit sicheren Signaturerstellungseinheiten (SSEE, Signaturkarten) verwendet, die den Anforderungen des SigG/SigV genügen.
OE.USER.RESP7	Für die qualifizierte Signatur wird der EVG nur in Verbindung mit Signatur-Anwendungskomponenten (SAK) verwendet, die den Anforderungen des SigG/SigV genügen.

Tabelle 5: Sicherheitsziele für die Umgebung des EVG

Die Beschreibung der Sicherheitsziele für die Umgebung des EVG in Tabelle 5 ist eine Zusammenfassung der Darlegung in den Sicherheitsvorgaben. Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5 Informationen zur Architektur

Der EVG besteht aus Hardware und darin eingebetteter Firmware.

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

- ES_HOST (Hostanbindung),
- ES_ICC (Chipkartenschnittstelle) und
- ES_UI (Tastatur und LCD)

Im Gehäuse befindet sich die Hauptplatine, die mit allen wesentlichen Bauteilen für die Ausführung der Firmware bestückt ist. Der Speicher ist in Programm- und Datenspeicher aufgeteilt, die getrennt adressiert werden. Es werden zwei Betriebsmodi (normaler Betriebsmodus und Update-Modus) des EVG realisiert.

Die Firmware gliedert sich in zwei Teile, die separat voneinander ausgeführt werden. Welcher Teil auszuführen ist, wird durch das Einstellen der entsprechenden Startadresse in der Bootkonfiguration vorgenommen. Die Bootkonfiguration ist persistent gespeichert. Durch die beiden Firmware-Teile werden die beiden Betriebsmodi Update-Modus und normaler Betriebsmodus realisiert.

Der Update-Modus ist im Update-Modul realisiert und dient dazu, eine neue Firmware im EEPROM zu installieren. Im Update-Modus nimmt der EVG einen der beiden Firmware-Teile über das DFU-Protokoll vom Host entgegen. Nach Abschluss der Übertragung wird die Signatur der Firmware mit Hilfe des ECDSA/SHA1-Moduls geprüft. Ist die Prüfung erfolgreich verlaufen, wird die Firmware in das EEPROM geschrieben. Sind von beiden Firmware-Teilen neue Versionen mit gültiger Signatur ins EEPROM geschrieben worden, wird die Bootkonfiguration so eingestellt, dass nach einem Reset die neue Firmware für den normalen Betriebsmodus gestartet und damit der Update-Modus verlassen wird. Andernfalls kann über das DFU-Protokoll eine neue Firmware-Übertragung vom Host angestoßen werden.

Im normalen Betriebsmodus beim Online-Betrieb nimmt der EVG Kommandos vom Host entgegen und führt sie aus oder leitet sie an die Chipkartenschnittstelle weiter. Der normale Betriebsmodus kann durch das spezielle Kommando DFU_Detach (USB) bzw. SoftwareUpdate verlassen werden. Daraufhin wird die Bootkonfiguration auf den Bootloader eingestellt und ein Reset eingeleitet. Das Main-Teilsystem steuert den gesamten Programmablauf im normalen Betriebsmodus. Es realisiert die Protokolle zur Kommunikation mit dem Host, analysiert und interpretiert die vom Host erhaltenen Befehle

und steuert die Hardware-Schnittstelle ES_HOST zum PC an. Im Reader-Teilsystem ist die sichere PIN-Eingabe (Funktionen SF.PINCMD und SF.CLMEM) realisiert. Das Teilsystem steuert die Hardware-Bestandteile der Benutzerschnittstelle ES_UI (LCD und Tastatur) an. Das ICC-Teilsystem steuert die Hardware-Schnittstelle ES_ICC zur Chipkarte an. Das Hilfsteilsystem enthält Hilfsfunktionen, die allen anderen Teilsystemen zur Verfügung stehen.

Im normalen Betriebsmodus wird auch die Unterscheidung gemacht, ob das Gerät im Online- oder Offline-Betrieb gestartet wird. Im Offline-Betrieb stehen die entsprechenden Funktionalitäten zur Verfügung, die nicht Teil der Evaluierung und somit des Zertifikats sind.

6 Dokumentation

Die evaluierte Dokumentation, die in Tabelle 2, Tabelle 3 und Tabelle 4 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 Testverfahren des Herstellers

Der Testansatz des Herstellers basiert auf der Überprüfung des Verhaltens der Sicherheitsfunktionen an den externen Schnittstellen. Hierfür wird neben einem PC mit Windows 2000 (SP4) kontrolliert veränderte Firmware genutzt, um interne Eigenschaften prüfen zu können, spezifische Werkzeuge und Hilfsmittel eingesetzt, die eine präzise Stimulation und Beobachtung der über die externen Schnittstellen ausgetauschten Daten ermöglichen.

Alle Sicherheitsfunktionen sind mindestens einem Test unterzogen worden. Alle relevanten Details der funktionalen Spezifikation und des Entwurfs auf hoher Ebene wurden berücksichtigt. Isolierte Tests der Teilsysteme über die internen Schnittstellen wurden nicht durchgeführt, weil die internen Schnittstellen durch die Testabdeckung an den externen Schnittstellen vollständig getestet werden.

Zusätzlich wurde vom Hersteller untersucht, ob die Versiegelung des Gerätes eine kritische Manipulation im Inneren des Gehäuses ermöglicht, ohne die Siegel sichtlich zu beschädigen.

Alle Tests bestätigten das korrekte Verhalten der Sicherheitsfunktionen.

7.2 Testverfahren der Prüfstelle

Die Testkonfiguration, mit der der Evaluator den EVG funktional getestet hat, entspricht der Konfiguration, in der der EVG auch produktiv eingesetzt wird.

Der Evaluator hat zu allen drei Sicherheitsfunktionen (SF.SECDOWN, SF.PINCMD und SF.SEAL), die von außen sichtbar sind, unabhängige Tests entwickelt, durchgeführt und aufgezeichnet. Hierfür wurden neben PCs mit Windows XP bzw. Linux Treiber von KOBIL und spezifische Testsoftware verwendet. Im Rahmen einer Stichprobe wurden insbesondere auch Tests der Sicherheitsfunktion SF.CLMEM wiederholt.

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

Ausgehend von der Analyse der Schwachstellen des Entwicklers und des Evaluators hat der Evaluator Penetrationstests konzipiert. Das Ziel bestand darin, die Herstelleraussagen zur Nichtausnutzbarkeit von Schwachstellen anhand von gezielten Tests zu überprüfen. Zusätzlich sollten weitere mögliche Schwachstellen, die der Hersteller nicht dokumentiert hat, mit Testfällen abgedeckt werden.

Die Ergebnisse der Tests, die vom Evaluator durchgeführt wurden, ergaben keine Abweichung vom erwarteten Ergebnis. Alle Schwachstellen wurden als nicht ausnutzbar bewertet.

8 Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Produktvarianten des EVG, die im zertifizierten Zustand über die mitgelieferte Docking-Station mit dem PC verbunden sein müssen (Online-Betrieb):

Produkt-Ausführung	Artikel-Nummer	Firmware	Dokumentation
KAAAN TriB@nk	HCPNCKS/C05	KAAN Trib@nk V69.17	DB25.DE.1 1v17_20080521_de
EMV-TriCAP	HCPNCKS/A03	EMV TriCAP V69.18	DB22.DEEN.1 2v10_20080521_de_uk
SecOVID III	HCPNCKS/B05	SecOVID III V69.18	DB21.DEEN.1 2v16_20080521_de_uk

Tabelle 6: Evaluierte Produktvarianten

Der Betrieb einer der Produktvarianten ohne eine Verbindung mit dem PC über die mitgelieferte Docking-Station (sog. Offline-Betrieb) ist nicht zertifiziert. Die Leistungsmerkmale im Offline-Betrieb sind nicht Gegenstand der Untersuchung.

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 EAL4 verwendet. Darüber hinaus wurde die in der AIS 34 [4] definierte Methodologie verwendet.

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

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

- Die Komponenten
  ADO_DEL.2 - Erkennung von Modifizierungen
  ADV_IMP.1 - Teilmenge der Implementierung der TSF
  ADV_LLD.1 - Beschreibender Entwurf auf niedriger Ebene
  ALC_TAT.1 - Klar festgelegte Entwicklungswerkzeuge
  AVA_MSU.3 - Analysieren und Testen auf unsichere Zustände
  AVA_VLA.4 - Hohe Widerstandsfähigkeit

Die Evaluierung hat gezeigt:

- Funktionalität: Common Criteria Teil 2 konform
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
  EAL 3 mit Zusatz von
  ADO_DEL.2 - Erkennung von Modifizierungen
  ADV_IMP.1 - Teilmenge der Implementierung der TSF
  ADV_LLD.1 - Beschreibender Entwurf auf niedriger Ebene
  ALC_TAT.1 - Klar festgelegte Entwicklungswerkzeuge
  AVA_MSU.3 - Analysieren und Testen auf unsichere Zustände
  AVA_VLA.4 - Hohe Widerstandsfähigkeit
- Die folgenden Sicherheitsfunktionen erfüllen die behauptete Stärke der Funktionen hoch:
  SF.SECDOWN (Prüfung von Firmwareupdates),
  SF.SEAL (Versiegelung des Gerätes)

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 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

10 Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 2, Tabelle 3 und Tabelle 4 genannte Betriebsdokumentation sowie die Sicherheitsvorgaben [6] enthalten die notwendigen Informationen zur Anwendung des EVG und alle darin enthaltenen Sicherheitshinweise sind zu beachten.

11 Sicherheitsvorgaben

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

12 Definitionen

12.1 Abkürzungen

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

EAL Evaluation Assurance Level – Vertrauenswürdigkeitsstufe

EEPROM Electrically Erasable Programmable Read Only Memory

EVG Evaluierungsgegenstand (EVG)

IT Information technologie - Informationstechnologie

ITSEF Information Technology Security Evaluation Facility – Prüfstelle für IT-Sicherheit

LCD Liquid Crystal Display – Flüssigkristallanzeige

PIN Persönliche Identifikationsnummer

PP Protection Profile – Schutzprofil

SAK Signaturanwendungskomponente

SF Security Function – Sicherheitsfunktion

SFP Security Function Policy – Politik der Sicherheitsfunktion

SigG/SigV Signaturgesetz und -verordnung [14 und 15]

SOF Strength of Function – Stärke der Funktion

SSEE Sichere Signaturerstellungseinheit – “Signaturkarte”

ST Security Target – Sicherheitsvorgaben

TOE Target of Evaluation – Evaluierungsgegenstand

TSC TSF Scope of Control – Anwendungsbereich der TSF-Kontrolle

TSF TOE Security Functions - EVG-Sicherheitsfunktionen

TSP TOE Security Policy - EVG-Sicherheitspolitik

12.2 Glossary

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

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

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

EVG-Sicherheitsfunktionen - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfasst, auf die Verlass sein muss, um die TSP korrekt zu erfüllen.

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

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

Informell - Ausgedrückt in natürlicher Sprache.

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

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

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

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

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

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

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

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

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

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

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

13 Literaturangaben

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

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

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

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

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

[6] Security Target BSI-DSZ-CC-0480-2008, Version 1.13, 10.11.2008, Signatur-Modul für die KOBIL Chipkartenterminals EMV-TriCAP Reader / SecOVID Reader III / KAAN TriB@nk – Security Target, KOBIL Systems GmbH

[7] Evaluation Technical Report, Version 1.1, 09.12.2008, ETR Evaluierung EMV-TriCAP / SecOVID III / KAAN TriB@nk, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH (vertrauliches Dokument)

[8] Konfigurationsliste für den EVG, Version 1.13, 20.11.2008, Signatur-Modul für die KOBIL Chipkartenterminals EMV-TriCAP Reader / SecOVID Reader III / KAAN TriB@nk – Entwicklungsumgebung und Konfigurationskontrolle, KOBIL Systems GmbH (vertrauliches Dokument)

[9] KOBIL EMV-TriCAP Reader – Manual, DB22.DEEN.1, Version 2.10, 21. 05. 2008, KOBIL Systems GmbH

[10] KAAN TriB@nk Beipackzettel, Version 1.19, 10. 11. 2008, KOBIL Systems GmbH

[11] KOBIL SecOVID Reader III – Manual, DB21.DEEN.1, Version 2.16, 21. 05. 2008, KOBIL Systems GmbH

[12] KAAN TriB@nk – Manual, DB25.DE.1, Version 1.17, 21. 05. 2008, KOBIL Systems GmbH

[13] KOBIL Systems GmbH: KOBIL KAAN TriB@nk / EMV TriCAP Reader / SecOVID Reader III – Developer Notes, Version 1.0, 23. 10. 2008.

[14] 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

[15] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. 11. 2001, BGBl. I, S. 3074ff, 21. 11. 2001.

[16] Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten, Version 1.4, 19. 07. 2005, Bundesnetzagentur

[8] Inbesondere:

- AIS 34, Version 1.00, 1. Juni 2004, Evaluation Methodology for CC Assurance Classes for EAL5+

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 B zum Zertifizierungsreport BSI-DSZ-CC-0480-2009

Evaluierungsergebnisse zur Entwicklungs- und Produktionsumgebung

Das IT-Produkt mit den Produktvarianten EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A03, Firmware Version 69.18), SecOVID Reader III (Artikel-Nr. HCPNCKS/B05, Firmware Version 69.18) und KAAN TriB@nk (Artikel-Nr. HCPNCKS/C05, Firmware Version 68.17) (Evaluierungsgegenstand – EVG) wurde von einer akkreditierten und lizensierten Prüfstelle nach der Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 und Anweisungen der Zertifizierungsstelle für Komponenten oberhalb von EAL 4 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 12. Januar 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) und
- ALC – Lebenszyklus-Unterstützung (ALC_DVS.1, ALC_TAT.1),

sind für den folgenden Entwicklungs- und Produktionsstandort des EVG erfüllt:

a) Kobil Systems GmbH, Pfortenring 11, 67547 Worms, Deutschland, 1. Stockwerk und 3. Stockwerk, (Entwicklung, Test, Endfertigung)

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 das Sicherheitsvorgaben [6]).

Dies ist eine eingefügte Leerseite