debis

Services by DaimlerChrysler

Zertifizierungsreport

CardMan®

CardMan® Compact

CardMan® Keyboard

CardMan® Mobile

CardMan® Software Development Kit, Version 2.2

Utimaco Safeware AG

debisZERT: BSI-ITSEC-0406-1998

debis IT Security Services

Die Dienstleister der Moderne

Vorwort

Die Produkte[1]

- CardMan®,
- CardMan® Compact,
- CardMan® Keyboard,
- CardMan® Mobile und
- CardMan® Software Development Kit, Version 2.2

der Utimaco Safeware AG wurden gegen die ITSEC evaluiert. Die Evaluierung wurde im Rahmen des Zertifizierungsschemas debisZERT der debis IT Security Services durchgeführt. Die Zertifizierung erfolgte im Dienstleistungsbereich 4: *Zertifikate mit Anerkennung durch das BSI* (Bundesamt für Sicherheit in der Informationstechnik).

Das Ergebnis lautet:

Sicherheitsfunktionalität:	Wiederaufbereitung
Evaluationsstufe:	**E2**
Mechanismenstärke:	Typ B Mechanismen: bei korrekter Implementierung nicht überwindbar im Sinne der ITSEC

Für weitere Auskünfte und Kopien dieses Reports ist die Zertifizierungsstelle wie folgt erreichbar:

✉ debis IT Security Services	✆	0228 / 9841-110
- Zertifizierungsstelle -	Fax:	0228 / 9841-60
Rabinstr. 8	Email:	zerti@itsec-debis.de
53111 Bonn	WWW:	www.itsec-debis.de

Die Ordnungsmäßigkeit der Evaluierung wird hiermit bestätigt.

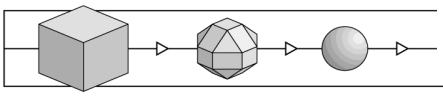
Bonn, den 20.4.98

Dr. Heinrich Kersten

Leiter der Zertifizierungsstelle

---

1 Über den Gültigkeitsbereich des Registered Trademarks gibt der Hersteller Auskunft. Im folgenden Report wird das Zeichen ® nicht mehr verwendet.



Revisionsliste

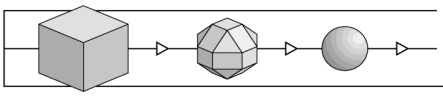
Die nachfolgende Revisionsliste gibt Auskunft über den Erstellungsprozeß für die Erstausgabe des Zertifizierungsreports.

Re-Zertifizierungen aufgrund von Produktänderungen sind in Kapitel 7 aufgeführt.

Revision	Datum	Vorgang
1.0	13.3.98	Erst-Erstellung (nach Musterreport Version 1.0).
1.1	20.4.98	Produktbezeichnung „Cardman II“ wurde beim Hersteller in „CardMan“ geändert. Der Zusatz (PCMCIA) entfällt. Die Produkte selbst sind nicht geändert. Im Zertifizierungsreport sind die neuen Bezeichnungen übernommen worden. Registered Trademark ® wurde auf dem Deckblatt und im Vorwort eingefügt. Musterreport Version 1.1

Inhalt

1 Überblick 5
1.1 Evaluierung 5
1.2 Zertifizierung 5
1.3 Zertifizierungsreport 5
1.4 Zertifikat 6
1.5 Anwendung der Ergebnisse 6
2 Wesentliche Ergebnisse der Evaluierung 9
2.1 Grundlegendes 9
2.2 Ergebnis 9
2.3 Hinweise 10
3 Sicherheitsvorgaben 11
3.1 Produktbeschreibung 11
3.1.1 Definition des Evaluationsgegenstandes 11
3.1.2 Beschreibung des Evaluationsgegenstandes 11
3.1.3 Einsatzumgebung 16
3.2 Subjekte, Objekte und Aktionen 17
3.2.1 Subjekte 17
3.2.2 Objekte 17
3.2.3 Aktionen 18
3.3 Sicherheitsziele und angenommene Bedrohungen 18
3.3.1 Sicherheitsziele 18
3.3.2 Angenommene Bedrohungen 18
3.4 Sicherheitsfunktionen 18
3.4.1 (F1) Löschen der Puffer im Hauptspeicher 18
3.4.2 (F2) Wiederaufbereitung der Gerätepuffer 18
3.4.3 Wirksamkeit der Sicherheitsfunktionen 19
3.5 Stärke der Mechanismen und Evaluationsstufe 19
4 Hinweise und Empfehlungen zum zertifizierten Objekt 21
5 Hinweise zu den Vorgaben und Kriterien 23
5.1 Grundbegriffe 23
5.2 Evaluationsstufen 23
5.3 Sicherheitsfunktion und Sicherheitsmechanismen 25
6 Anhänge 28
6.1 Glossar 28
6.2 Referenzen 32
6.3 Abkürzungen 33
7 Re-Zertifizierungen und technische Anhänge 35



(Diese Seite ist beabsichtigterweise leer.)

1 Überblick

1.1 Evaluierung

1 Die Evaluierung wurde durch die Utimaco Safeware AG, Dornbachstr. 30, 61440 Oberursel, beauftragt.

2 Die Evaluierung wurde durchgeführt von der Industrieanlagen-Betriebsgesellschaft mbH (IABG) und am 11.3.98 beendet.

3 Die Evaluierung wurde gegen die ITSEC und ITSEM durchgeführt. Einige Hinweise zu den Inhalten der ITSEC und ITSEM finden sich im Abschnitt 5.

1.2 Zertifizierung

4 Die Zertifizierung wurde gemäß den Regeln des Zertifizierungsschemas debisZERT der debis IT Security Services durchgeführt. Die Zertifizierungsstelle arbeitet im Einklang mit der DIN EN 45011.

5 Die Zertifizierungsstelle der debis IT Security Services hat das Zertifizierungsverfahren nach Maßgabe der Dokumente

/Z01/ Zertifizierungsschema der debis IT Security Services , Version 1.1, 9.1.98

/V04/ Dienstleistungsbereich 4: Zertifikate mit Anerkennung durch das BSI, Version 1.1, 9.1.98

durchgeführt.

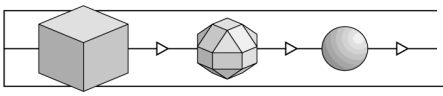
1.3 Zertifizierungsreport

6 Dieser Zertifizierungsreport gibt die Ergebnisse der Evaluierung von CardMan, CardMan Compact, CardMan Keyboard, CardMan Mobile und CardMan Software Development Kit, Version 2.2 wieder - im folgenden als EVG = Evaluationsgegenstand bezeichnet.

7 Der Zertifizierungsreport gilt nur für die angegebene Version des EVG. Er kann jedoch auf neue bzw. andere Versionen ausgedehnt werden, sobald eine erfolgreiche Re-Evaluierung stattgefunden hat.

8 Der Zertifizierungsreport dient

- dem Auftraggeber als Nachweis der durchgeführten Evaluierung und



- dem Nutzer als Grundlage für den sicherheitsgerechten Einsatz von CardMan, CardMan Compact, CardMan Keyboard, CardMan Mobile und CardMan Software Development Kit, Version 2.2.

9 Der Zertifizierungsreport enthält die Seiten 1 bis 36. Kopien des Zertifizierungsreports können beim Auftraggeber oder bei der Zertifizierungsstelle angefordert werden.

10 Der Zertifizierungsreport kann einerseits durch Nachweise über erfolgte Re-Zertifizierungen, andererseits durch Anhänge zu besonderen technischen Problemen ergänzt werden. Solche Nachweise bzw. Anhänge werden in der Druckschrift

/Z02/ Zertifizierte IT-Produkte, IT- Systeme und IT-Dienstleistungen

angekündigt.

1.4 Zertifikat

11 Eine Kurzfassung der Ergebnisse enthält das Sicherheitszertifikat debisZERT: BSI-ITSEC-0406-1998.

12 Eine Kurzbeschreibung von CardMan, CardMan Compact, CardMan Keyboard, CardMan Mobile und CardMan Software Development Kit, Version 2.2 und die Zertifizierungsergebnisse werden in der Druckschrift

/Z02/ Zertifizierte IT-Produkte, IT- Systeme und IT-Dienstleistungen

und über WWW veröffentlicht.

13 Das Zertifikat wird durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt, das seinerseits die Gleichwertigkeit des Zertifikats zu seinen eigenen Zertifikaten im internationalen Kontext bestätigt.

14 Das Zertifikat trägt das vom BSI genehmigte Logo. Die Tatsache der Zertifizierung wird in der Broschüre 7148 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufgeführt.

1.5 Anwendung der Ergebnisse

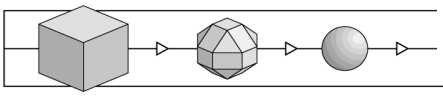
15 Die Prozesse der Evaluierung und Zertifizierung werden nach dem Stand der Technik durchgeführt, können aber keine *absolute* Garantie dafür geben, daß das zertifizierte Objekt frei von Schwachstellen ist. Mit steigender Evaluationsstufe verringert sich allerdings die Wahrscheinlichkeit erheblich, daß ausnutzbare Schwachstellen unentdeckt bleiben.

16 Um die Ergebnisse der Evaluierung sinnvoll nutzen zu können, wird dringend empfohlen, den Zertifizierungsreport aufmerksam zu lesen. Insbesondere die Informationen zur Art der Nutzung des zertifizierten Objektes, zu den betrach-

teten Bedrohungen, zur Einsatzumgebung und zu den geprüften Konfigurationen sind wichtige Vorgaben für die Praxis.

17 Das Evaluierungsergebnis gilt nur unter der Voraussetzung, daß alle Vorgaben aus dem Zertifizierungsreport beachtet werden.

Sofern von diesen Vorgaben abgewichen wird, gilt das Evaluierungsergebnis nur noch bedingt. In einem solchen Fall ist eine ergänzende Analyse erforderlich, um festzustellen, ob und in welchem Umfang das zertifizierte Objekt auch unter den geänderten Bedingungen noch Sicherheit bieten kann. Die genannte Prüfstelle und die Zertifizierungsstelle können bei der Analyse unterstützen.



(Diese Seite ist beabsichtigterweise leer.)

2 Wesentliche Ergebnisse der Evaluierung

2.1 Grundlegendes

18 Das Ergebnis der Evaluierung ist im ETR (Evaluation Technical Report) dargestellt. Die Evaluierung erfolgte gegen die im Abschnitt 4 dieses Zertifizierungsreports wiedergegebenen Sicherheitsvorgaben.

2.2 Ergebnis

19 Die Prüfstelle kommt zu folgendem Ergebnis:

- Der EVG genügt den Anforderungen der Evaluationsstufe **E2** gemäß ITSEC, d.h. alle Anforderungen an die Korrektheit und Wirksamkeit gemäß dieser Stufe sind erfüllt. Dies sind:

  ITSEC E2.1 bis E2.37 für die Korrektheit mit den Phasen

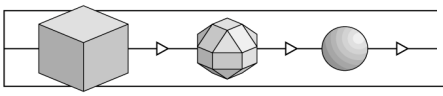
Konstruktion - Entwicklungsprozeß	(Anforderungen, Architekturentwurf, Feinentwurf, Implementierung),
Konstruktion - Entwicklungsumgebung	(Konfigurationskontrolle, Sicherheit beim Entwickler),
Betrieb - Betriebsdokumentation	(Benutzerdokumentation, Systemverwalter-Dokumentation)
Betrieb - Betriebsumgebung	(Auslieferung und Konfiguration, Anlauf und Betrieb).

  ITSEC 3.12 bis 3.37 für die Wirksamkeit mit den Aspekten

Wirksamkeitskriterien - Konstruktion	(Eignung der Funktionalität, Zusammenwirken der Funktionalität, Stärke der Mechanismen, Bewertung der Konstruktionsschwachstellen),
Wirksamkeitskriterien - Betrieb	(Benutzerfreundlichkeit, Bewertung der operationellen Schwachstellen).

- Die Mechanismen des EVG für die Sicherheitsfunktion **Wiederaufbereitung** sind kritische Mechanismen, und zwar Typ B Mechanismen; hierfür ist gemäß /ITSEC/ und /ITSEM/ keine Mechanismenstärke anzugeben.

  Im Rahmen der Schwachstellenanalyse konnte jedoch festgestellt werden, daß selbst unter Zugrundelegung eines Aufwands gemäß der Stufe „hoch“ bei den



angenommenen Einsatzbedingungen (s. Hinweise für Anwender) keine ausnutzbare Schwachstelle erkennbar ist.

2.3 Hinweise

20 Die Prüfstelle hat **keine Auflagen** an den **Hersteller** auszusprechen.

21 Für den **Anwender** sind folgende **Hinweise** wichtig:

1. Das Evaluierungsergebnis ist gültig, wenn der EVG unter den Betriebssystemen MS DOS 6.x, MS Windows 3.x, MS Windows 95 / Windows NT oder OS / 2 Warp 3.0 und 4.0 betrieben wird.

2. Der EVG ist vor unberechtigtem physischem Zugriff (Auswechseln von Hardware-Komponenten) zu schützen, z.B. durch Aufstellen des EVG in nur berechtigten Benutzern zugänglichen Räumen.

3 Sicherheitsvorgaben

Die der Evaluierung zugrunde liegenden Sicherheitsvorgaben sind seitens des Auftraggebers in englischer Sprache bereitgestellt worden. Sie werden hier in der deutschen Übersetzung wiedergegeben.

3.1 Produktbeschreibung

3.1.1 Definition des Evaluationsgegenstandes

Der Evaluationsgegenstand (EVG) besteht aus den folgenden Produktbestandteilen:

- Smartcard-Lesegerät, welches eines der folgenden Geräte sein kann:
  - CardMan Compact Smartcard-Leser für die serielle Schnittstelle oder
  - CardMan Smartcard-Leser für die serielle Schnittstelle oder
  - CardMan Mobile PC-Card (PCMCIA) Smartcard-Leser oder
  - CardMan Keyboard.
- Software: 'CardMan Software Development Kit' , Version 2.2 für verschiedene Betriebssystemplattformen,
- CardMan SDK API Dokumentation (Programmierhandbuch) (gedrucktes Dokument in englischer Sprache).

Der EVG wird im restlichen Dokument als "CardMan" bezeichnet.

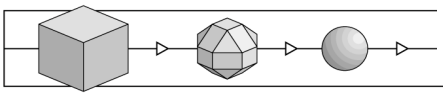
3.1.2 Beschreibung des Evaluationsgegenstandes

Überblick

CardMan ist eine Kombination von Hardware- und Software-Bestandteilen, um die Benutzung von Smartcards in einem weiten Bereich von Sicherheitsapplikationen in der Informationstechnik zu unterstützen, wie z.B.

- Sichere Zugangssysteme (PC-Sicherheit),
- Kryptosysteme (Funktionen für Schlüsselverwaltung),
- Sichere Datenübertragungssysteme (Digitale Signatur, Homebanking).

Der CardMan Smartcard-Leser ist ein kleines und handliches Interface für den Zugriff auf fast alle ISO 7816 kompatiblen Smartcards.



Der CardMan Software Development Kit enthält Bibliotheken und Gerätetreiber, die in kundenspezifische Anwendungsprogramme integriert werden können. Die Bibliotheken bieten komplexe Funktionen zur Realisierung von Anwendungen, die mit den CardMan Smartcard-Lesern kommunizieren.

Allgemeine Beschreibung der Hardware

Der CardMan Leser ist in vier verschiedenen Versionen verfügbar (wie in Abschnitt 1.1 dieses Dokuments aufgelistet). Drei dieser Versionen sind für die Benutzung mit einer seriellen Schnittstelle vorgesehen und haben identisches Design ihrer Elektronik, eine Version, die PC-Card, ist für die Benutzung in Laptops und Notebooks vorgesehen (funktioniert aber auch in PCMCIA-Einschüben für Desktop-PCs).

Der Aufbau der unterschiedlichen Versionen des Smartcard-Lesers wird im folgenden beschrieben.

CardMan Compact

CardMan Compact ist eine Smartcard-Leseeinheit in einem eigenen Gehäuse.

Der Leser wird mit einem dort fest montierten Kabel an der seriellen Schnittstelle der Workstation angeschlossen. Die Spannungsversorgung wird der seriellen Schnittstelle entnommen.

CardMan

CardMan ist eine spezielle Version von CardMan Compact. Es handelt sich ebenfalls um einen Leser in einem eigenen Gehäuse. Beim CardMan ist das serielle Kabel am Leser steckbar, wobei 2 Buchsen auf verschiedenen Seiten verfügbar sind. Die Spannungsversorgung wird der seriellen Schnittstelle entnommen. Der Leser verfügt über zwei LEDs (grün und rot) an der Vorderseite zur Anzeige des Status des Lesers und der Karte.

CardMan Keyboard

Beim CardMan Keyboard ist der Leser in das Gehäuse der Tastatur integriert. Die Karte wird an der hinteren rechten Seite der Tastatur eingeschoben. Die Elektronik des Lesers ist funktionell mit der von CardMan und CardMan Compact identisch. Der Leser wird mit einem separaten fest montierten Kabel an einer seriellen Schnittstelle der Workstation angeschlossen.

Die Tastatur ist mit einem ISO 102 Tasten-Layout und mit einem ANSI 101 Tasten-Layout verfügbar, die ISO 102 Tasten-Layout-Version ist für viele verschiedene Sprachen erhältlich (Deutsch, Englisch etc.).

CardMan Mobile

CardMan Mobile ist eine Typ-II PC-Card (PCMCIA-Karte). Sie paßt in jeden PC-Card-Einschub für Typ-II-Karten. Die Smartcard wird an der offenen Seite der PC-Card einge-

schoben.

Die Verbindung wird über den PC-Card-Bus der Workstation hergestellt, zusätzliche Verbindungen sind nicht notwendig. Die Karte emuliert eine serielle Schnittstelle an der Workstation.

Installation der Hardware

Wenn eine der seriellen Versionen des CardMan benutzt wird (CardMan, CardMan Compact oder CardMan Keyboard), wird der CardMan an eine freie serielle Schnittstelle angeschlossen. Die serielle Schnittstelle muß mit ihrer E/A-Adresse und ihrem Interrupt so konfiguriert sein, daß keine Konflikte auftreten.

Wenn die PC-Card benutzt wird, wird sie in einen PCMCIA-Typ-II-Einschub der Workstation eingeschoben. Die Karte emuliert eine serielle Schnittstelle und muß als freie serielle Schnittstelle mit E/A-Adresse und Interrupt konfiguriert werden.

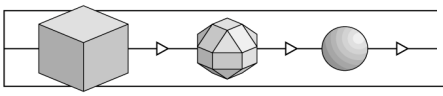
Die weitere Konfiguration wird von der Software vorgenommen, die den Smartcard-Leser betreibt (siehe unten).

Beschreibung der Software

Das CardMan Software Development Kit (SDK) ist ein Paket von Bibliotheken und Include-Dateien, die für jedes unterstützte Betriebssystem zusammengefaßt sind und auf Disketten ausgeliefert werden.

Das SDK besteht aus :

- Include-Dateien (.H) zum Einbinden in C-Quelldateien (ANSI-kompatibel).
- Bibliotheken, abhängig vom Betriebssystem:
  - statische Bibliotheken (.LIB) im Format des Microsoft Linkers zum Dazubinden unter DOS Version 6.0 und höher,
  - 16Bit dynamisch linkbare Bibliotheken (.DLL) für Windows 3.1 und 3.11,
  - 32Bit dynamisch linkbare Bibliotheken (.DLL) für Windows 95, Windows NT 3.51 und Windows NT 4.0 (Workstation und Server),
  - 32Bit dynamisch linkbare Bibliotheken für OS/2 WARP Version 3.0 und 4.0.
- einem Gerätetreiber für die serielle Kommunikation zwischen der Workstation und dem Smartcard-Leser, genauer:
  - einem Gerätetreiber (.EXE) für DOS Version 6.0 und höher,
  - einem VxD (.386) für Windows 3.1 und 3.11,



– einem Geräteservice für Windows 95, Windows NT 3.51 und Windows NT 4.0 (Workstation und Server),

– einem Gerätetreiber für OS/2 WARP Version 3.0 und 4.0.

Die Software überträgt die Daten in einem geschlossenen Kanal vom Anwendungsprogramm zur Smartcard und zurück. Nur für die Übertragung über die serielle Schnittstelle werden die Dienste des Betriebssystems benutzt.

Die Kommunikation zwischen den Bibliotheksfunktionen und dem Gerätetreiber wird mit speziellen Betriebssystemmechanismen durchgeführt, dabei wird ein Puffer im Shared Memory benutzt.

Alle Puffer, die für Datenübertragung in der Software auf der Host-Seite benutzt werden, werden unmittelbar nach ihrer Benutzung überschrieben. Alle Puffer, die in der Firmware und Hardware des CardMan für Datenübertragung benutzt werden, werden kontrolliert wiederaufbereitet und dieselbe Information kann nicht ein zweitesmal ausgelesen werden.

Umfang der API Funktionen

Die Bibliotheken des CardMan SDK enthalten einen Satz von API Funktionen für die Kommunikation eines benutzerspezifischen Anwendungsprogrammes mit dem Smartcard-Leser und der Smartcard.

Das API ist für jede Betriebssystemplattform identisch. Die Funktionen sind in die folgenden Schichten unterteilt.

Protokollschicht

Diese Schicht enthält Funktionen zum Ansprechen des Smartcard-Lesers und zur Durchführung von Basisfunktionen der Smartcards:

– Verbinden und Trennen des Lesers,

– Auslesen des Status des Lesers,

– Kontrolle der LEDs des Lesers (nur CardMan),

– Sperren und Entsperren der Leserschnittstelle,

– Senden von Power On und Power Off an die Smartcard,

– Anpassen des Leser-Protokolls an die Smartcard (Übertragungsrate etc.),

– Protokollauswahl und

– Kommunikation mit der Smartcard.

Die Kommunikationsfunktionen sind für jedes unterstütze Protokoll (T=0, T=1, T=14, Synchron) verfügbar.

Kartenschicht

Für jede unterstützte Familie von Smartcards gibt es einen Satz von kartenspezifischen Funktionen. Die vom EVG unterstützten Kartenfamilien sind:

- BULL CP8 SCOT
- Siemens SLE 4428,
- Siemens SLE 4442,
- Siemens SLE 44C200,
- GEMPLUS MCOS.

Die Funktionen, die in jeder Bibliothek verfügbar sind, sind vom jeweiligen Kartenbetriebssystem abhängig, sie spiegeln die Hauptfunktionen jedes Smartcard-OS wieder, zum Beispiel:

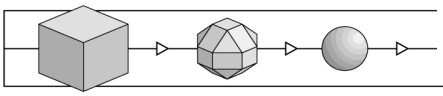
- Karte initialisieren,
- PIN präsentieren,
- Daten lesen (Wort, Inhaltsverzeichnis, Satz etc.),
- Daten schreiben (Wort, Inhaltsverzeichnis, Satz etc.),
- Status lesen,
- kartenspezifische Verschlüsselungsalgorithmen ausführen (RSA, DES etc.).

Alle Funktionen des CardMan SDK benutzen nur die Funktionen der jeweils darunterliegenden Schichten des SDK bzw. den Gerätetreiber aus dem CardMan SDK.

Eine ausführliche gedruckte Dokumentation (in englischer Sprache), die mit dem EVG ausgeliefert wird, beschreibt das Interface und alle Interface-Funktionen.

Installation und Anwendung der Software

Das CardMan SDK wird mit einem mitgelieferten Installationsprogramm von Disketten installiert; nur für DOS muß die Installation manuell durchgeführt werden, indem eine selbstentpackende komprimierte Datei ausgeführt wird. Das jeweilige Installationsprogramm fragt den Pfad für die Installation ab. Der Rest der Installation wird automatisch durchgeführt.



Das CardMan SDK wird in einer Entwicklungsumgebung installiert, in der Anwendungen entwickelt werden, die die API-Funktionen benutzen.

Wenn die dynamisch linkbaren Bibliotheken benutzt werden sollen, müssen sie in ein Verzeichnis geladen werden, aus dem sie von einer laufenden Anwendung geladen werden können.

Wenn der Gerätetreiber benutzt werden soll, muß er, entsprechend dem Betriebssystem der Zielmaschine korrekt installiert werden:

– durch einen Eintrag in CONFIG.SYS für DOS Version 6.0 und höher,

– durch einen Eintrag in SYSTEM.INI für Windows 3.1 und 3.11,

– unter Verwendung der Systemsteuerung unter Windows 95, Windows NT und OS/2 WARP.

Wenn eine kundenspezifische Anwendung ausgeliefert wird, die mit dem CardMan SDK entwickelt wurde, müssen die benötigten Bibliotheken und der passende Gerätetreiber aus dem CardMan SDK zu den ausgelieferten Anwendungsprogrammen hinzugefügt werden.

Auf dem Zielrechner, auf dem die Anwendung installiert wird, müssen die Bibliotheken in einem Pfad installiert werden, wo sie von der laufenden Anwendung geladen werden können. Der Gerätetreiber muß korrekt installiert werden.

3.1.3 Einsatzumgebung

Anforderungen an die Hardware

Der EVG läuft auf Standard Personal Computern mit einem Mikroprozessor kompatibel zu Intel 80386 und höher. Der PC benötigt eine freie serielle Schnittstelle für die Verbindung mit dem CardMan Smartcard-Leser. Das CardMan Keyboard mit dem integrierten Smartcard-Leser benötigt ebenfalls eine serielle Schnittstelle für den Anschluß des Lesers. Bei Benutzung des CardMan Mobile wird keine freie serielle Schnittstelle benötigt, aber mindestens eine der vier verfügbaren seriellen Verbindungen darf nicht mit einer physikalisch existierenden seriellen Schnittstelle ausgestattet sein.

Bezüglich der übrigen Hardwarebestandteile wie Festplatten und weiteres bestehen keine Anforderungen.

Der EVG unterstützt Smartcards, die zu ISO 7816 konform sind und die eines der Protokolle T=0, T=1, T=14 oder gewisse synchrone Kommunikationsprotokolle unterstützen. Die Stromaufnahme muß unter 10 mA liegen, bei Benutzung des CardMan im CardMan Keyboard kann die Stromaufnahme bis 50 mA betragen.

Anforderungen an die Software

Das CardMan Software API unterstützt die folgenden Betriebssysteme:

– MS-DOS Version 6.0 und höher,

– Windows 3.1, Windows für Workgroups 3.11,

– Windows 95,

– Windows NT 3.51 Workstation und Server, Windows NT 4.0 Workstation und Server,

– OS/2 WARP Version 3.0 und Version 4.0.

Das CardMan Software API wird für folgende Compiler ausgeliefert:

– Microsoft C (Version 6.0 und höher) und Visual C (Version 1.0 und höher) und alle damit objektkompatiblen ANSI C Compiler,

– OS/2 Visual Age C Compiler.

Besondere Maßnahmen

Um die Sicherheitsfunktionalität des Systems zu wahren, müssen die folgenden besonderen Maßnahmen getroffen werden:

– Generierung sicherer Anwendungen

Um sichere Anwendungen zu generieren, müssen die Funktionen des API gemäß den Anweisungen in der Dokumentation (Programmierhandbuch) verwendet werden. Das bewirkt, daß die Funktionen so verwendet werden, daß sich die Sicherheitsmechanismen nicht gegenseitig deaktivieren oder umgehen.

3.2 Subjekte, Objekte und Aktionen

3.2.1 Subjekte

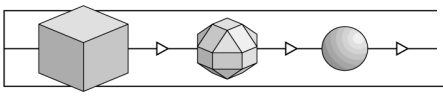
(S1) Ein Prozeß, der auf dem Zielsystem läuft und nicht Bestandteil des EVG ist.

(S2) Eine Person, die Zugang zur Hardware des Smartcard-Lesers hat.

3.2.2 Objekte

(O1) Im Hauptspeicher gespeicherte Übertragungsdaten aus der Kommunikation mit der Smartcard.

(O2) Im Speicher des Gerätes (Smartcard-Leser) gespeicherte Übertragungsdaten.



3.2.3 Aktionen

(A1) Zugang zu den Übertragungsdaten im Hauptspeicher (O1) durch einen Prozeß (S1) nach dem Abschluß der Datenübertragung durch den EVG.

(A2) Zugang zu den Übertragungsdaten im Gerätespeicher (O2) durch eine Aktion irgendeiner Person (S2) nach dem Abschluß der Datenübertragung durch den EVG.

3.3 Sicherheitsziele und angenommene Bedrohungen

3.3.1 Sicherheitsziele

Der EVG wurde entwickelt, um den Zugriff mit beliebigen Methoden auf Übertragungsdaten von oder zu einer Smartcard zu verhindern, nachdem die Datenübertragung abgeschlossen wurde. Dies gilt sowohl für die Daten, die im Hauptspeicher gespeichert werden als auch für die Daten, die im Gerät des Smartcard-Lesers gespeichert werden. Alle Speicherobjekte, die vom EVG für Datenübertragung benutzt werden, werden gelöscht, bevor sie von anderen Prozessen benutzt oder über die Hardware ausgelesen werden können.

3.3.2 Angenommene Bedrohungen

Der EVG wirkt den folgenden angenommenen Bedrohungen entgegen:

(T1) Ein beliebiger Prozeß außerhalb des EVG (S1) erhält Kenntnis von Übertragungsdaten, die im Hauptspeicher gespeichert werden (O1) durch Lesen des entsprechenden Speichers (A1).

(T2) Eine beliebige Person (S2) erhält Kenntnis von Übertragungsdaten, die im Gerät gespeichert sind (O2), nach Abschluß der Übertragung durch Auslesen der Speicherinhalte (A2) des Geräts.

3.4 Sicherheitsfunktionen

3.4.1 (F1) Löschen der Puffer im Hauptspeicher

Der EVG stellt eine Funktion zur Verfügung, mit der die im Hauptspeicher allokierten Puffer, in denen Übertragungsdaten enthalten sein könnten, überschrieben werden. Die Puffer werden unmittelbar nach dem Abschluß der Übertragung überschrieben.

3.4.2 (F2) Wiederaufbereitung der Gerätepuffer

Der EVG stellt sicher, daß die Information in den Pufferspeichern des Gerätes (bei jeder Version des Smartcard-Lesers), die Übertragungsdaten enthalten könnten, nur ein einziges Mal ausgelesen werden kann, d.h., daß die Information nicht noch einmal ausgelesen werden kann, nachdem der EVG die Daten gelesen hat.

3.4.3 Wirksamkeit der Sicherheitsfunktionen

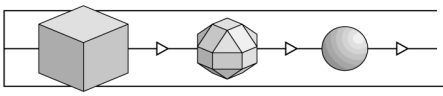
Die Sicherheitsfunktion (F1) wirkt der Bedrohung (T1) entgegen, die Sicherheitsfunktion (F2) wirkt der Bedrohung (T2) entgegen.[2]

3.5 Stärke der Mechanismen und Evaluationsstufe

Alle aufgezählten Produktkombinationen des EVG sind identisch in ihren Sicherheitsfunktionen und in ihren sicherheitskritischen und sicherheitsrelevanten Teilen, Funktionen und Mechanismen. Die angestrebte Evaluationsstufe für den EVG ist **E2**, die angestrebte Mechanismenstärke ist **hoch**.

---

2 Dieses Szenario ist wesentlich zur Erfüllung der Vorgaben des Signaturgesetzes bzw. der Signaturverordnung.

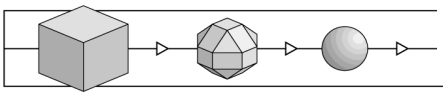


(Diese Seite ist beabsichtigterweise leer.)

4 Hinweise und Empfehlungen zum zertifizierten Objekt

22 Die Ausführungen in Kapitel 2 sind als Ergebnis der Evaluierung zu beachten.

23 Bei der Zertifizierung haben sich keine weitergehenden Hinweise oder Empfehlungen für den Anwender ergeben.



(Diese Seite ist beabsichtigterweise leer.)

5 Hinweise zu den Vorgaben und Kriterien

24 Dieser Abschnitt soll einen Überblick über die Vorgaben und Kriterien geben, die bei der Evaluierung zugrunde lagen, und deren Bewertungsmaßstäbe erläutern.

5.1 Grundbegriffe

25 *Sicherheit* ist nach dem Verständnis der ITSEC dann gegeben, wenn ausreichendes Vertrauen darin besteht, daß das Produkt oder System seine *Sicherheitsziele* erfüllt.

26 *Sicherheitsziele* setzen sich in der Regel aus Forderungen nach

- Vertraulichkeit
- Verfügbarkeit
- Integrität

von bestimmten Datenobjekten zusammen. Solche Sicherheitsziele werden bei einem Produkt durch den Hersteller oder Anbieter, bei einem System durch den Anwender festgelegt.

27 Den festgelegten Sicherheitszielen stehen *Bedrohungen* gegenüber, nämlich der Verlust der Vertraulichkeit, der Verlust der Verfügbarkeit, der Verlust der Integrität bestimmter Datenobjekte.

28 Solche Bedrohungen werden Realität, wenn Subjekte unerlaubt Daten mitlesen oder abhören, Dritten vorenthalten oder unbefugt ändern können.

29 *Sicherheitsfunktionen* in dem betrachteten Produkt oder System sollen solche *Angriffe* abwehren.

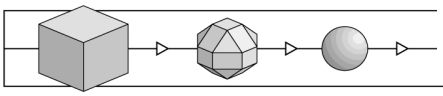
30 Es stellen sich dabei zwei Grundfragen:

- Funktionieren die Sicherheitsfunktionen korrekt?
- Sind sie wirksam?

Vertrauen in die Erfüllung der Sicherheitsziele kann man also dann haben, wenn *Korrektheit* und *Wirksamkeit* geprüft (*evaluiert*) worden sind.

5.2 Evaluationsstufen

31 Eine Evaluierung kann nur mit begrenztem Aufwand und in begrenzter Zeit durchgeführt werden. Die mögliche Tiefe einer Evaluierung ist also stets begrenzt. Das Angemessenheitsprinzip verbietet es andererseits, bei geringem Sicherheitsbedarf eine extrem aufwendige Prüfung durchzuführen; ebenso un-



angemessen wäre es, bei höchstem Sicherheitsbedarf nur „oberflächlich“ zu prüfen.

32 Es ist deshalb sinnvoll, unterschiedliche Prüftiefen (und damit Prüfaufwände) festzulegen: In den ITSEC werden 6 Evaluationsstufen zur Prüfung von Korrektheit und Wirksamkeit definiert. E1 bezeichnet die niedrigste, E6 die höchste Stufe.

33 Die Vertrauenswürdigkeit eines Produktes oder Systems kann also diesen Stufen „gemessen“ werden.

34 Die folgenden Auszüge aus den ITSEC lassen erkennen, welche Prüfaspekte im Rahmen einer Evaluierung behandelt werden und welche Prüftiefe welcher E-Stufe entspricht.

35 Die Aufzählung beinhaltet zunächst gewisse Anforderungen an die Korrektheit und läßt die Tiefe der Prüfung erkennen („EVG“ meint das zu prüfende Produkt oder System):

E1 „Auf dieser Stufe müssen für den EVG die Sicherheitsvorgaben und eine informelle Beschreibung des Architekturentwurfs vorliegen. Durch funktionale Tests muß nachgewiesen werden, daß der EVG die Anforderungen der Sicherheitsvorgaben erfüllt.“

E2 „Zusätzlich zu den Anforderungen für die Stufe E1 muß hier eine informelle Beschreibung des Feinentwurfs vorliegen. Die Aussagekraft der funktionalen Tests muß bewertet werden. Ein Konfigurationskontrollsystem und ein genehmigtes Distributionsverfahren müssen vorhanden sein.“

E3 „Zusätzlich zu den Anforderungen für die Stufe E2 müssen der Quellcode bzw. die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen, bewertet werden. Die Aussagekraft der Tests dieser Mechanismen muß bewertet werden.“

E4 „Zusätzlich zu den Anforderungen für die Stufe E3 muß ein formales Sicherheitsmodell Teil der Sicherheitsvorgaben sein. Die sicherheitsspezifischen Funktionen, der Architekturentwurf und der Feinentwurf müssen in semiformaler Notation vorliegen.“

E5 „Zusätzlich zu den Anforderungen für die Stufe E4 muß ein enger Zusammenhang zwischen dem Feinentwurf und dem Quellcode bzw. den Hardware-Konstruktionszeichnungen bestehen.“

E6 „Zusätzlich zu den Anforderungen für die Stufe E5 müssen die sicherheitsspezifischen Funktionen und der Architekturentwurf in einer formalen Notation vorliegen, die konsistent mit dem zugrundeliegenden formalen Sicherheitsmodell ist."

36 In jeder der Stufen E1 bis E6 müssen darüber hinaus Wirksamkeitsaspekte nach folgendem Schema untersucht werden:

Alle E-Stufen

"Die Bewertung der Wirksamkeit erfordert die Betrachtung der folgenden Aspekte des EVG:

a) die Eignung der sicherheitsspezifischen Funktionen des EVG, den in den Sicherheitsvorgaben aufgezählten Bedrohungen zu widerstehen;

b) die Fähigkeit der sicherheitsspezifischen Funktionen und Mechanismen des EVG, in einer Weise zusammenzuwirken, daß sie sich gegenseitig unterstützen und ein integriertes, wirksames Ganzes bilden;

c) die Fähigkeit der Sicherheitsmechanismen des EVG, einem direkten Angriff zu widerstehen;

d) ob bekannte Sicherheitsschwachstellen in der Konstruktion des EVG in der Praxis die Sicherheit des EVG kompromittieren können;

e) daß der EVG nicht in einer Weise konfiguriert werden kann, die unsicher ist, aber von der ein Systemverwalter oder ein Endnutzer vernünftigerweise glauben könnte, daß sie sicher ist;

f) ob bekannte Sicherheitsschwachstellen beim Betrieb des EVG in der Praxis die Sicherheit des EVG kompromittieren können."

5.3 Sicherheitsfunktion und Sicherheitsmechanismen

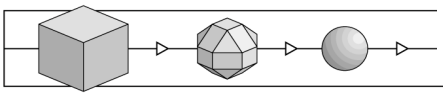
37 Typische Beispiele für Sicherheitsfunktionen sind die *Identifikation und Authentisierung* (von Subjekten), die *Zugriffskontrolle*, die *Beweissicherung* (Protokollierung), die *Protokollauswertung*, die *Übertragungssicherung*. Ein Produkt oder System kann solche Sicherheitsfunktionen beinhalten.

38 Meist kommen solche Sicherheitsfunktionen in einer typischen Kombination („Funktionalitätsklasse“) vor.

Beispiel: Die Funktionalitätsklasse F-C2 setzt sich aus den Funktionen *Identifikation und Authentisierung*, *Zugriffskontrolle*, *Beweissicherung*, *Protokollauswertung* und *Wiederaufbereitung* zusammen. Diese Klasse ist bei vielen kommerziellen Betriebssystemen gegeben.

39 Jede Sicherheitsfunktion kann auf unterschiedlichste Weise realisiert werden.

Beispiel: Die Funktion *Identifikation und Authentisierung* kann unter anderem durch ein Paßwort-Verfahren, durch Verwendung von Chipkarten mit Challenge-Response Verfahren oder durch biometrische Verfahren realisiert sein.



40 Jede Realisierung dieser Art heißt *(Sicherheits-)Mechanismus* der Sicherheitsfunktion *Identifikation und Authentisierung*.
Für andere Sicherheitsfunktionen gilt sinngemäß das gleiche.

41 Die Wiederstandskraft eines Sicherheitsmechanismus gegenüber Angriffen wird als *Stärke* des Mechanismus bezeichnet.

42 In den ITSEM werden zwei Arten von Mechanismen unterschieden: Typ B und Typ A.

Typ B „Ein Mechanismus vom Typ B ist ein Sicherheitsmechanismus, der bei perfekter Konzipierung und Implementierung keine Schwächen aufweist. Ein Mechanismus vom Typ B kann als nicht durch einen direkten Angriff überwindbar betrachtet werden, gleichgültig, wie groß der Aufwand an Ressourcen, Fachkenntnissen und entsprechenden Gelegenheiten ist. Ein mögliches Beispiel für einen Mechanismus vom Typ B wäre die Zugangskontrolle auf der Basis von Zugangskontrollisten: Bei perfekter Konzipierung und Implementierung kann dieser Mechanismus vom Typ B nicht durch einen direkten Angriff überwunden werden. Mechanismen vom Typ B können jedoch durch indirekte Angriffe überwunden werden, mit denen sich andere Wirksamkeitsanalysen befassen."

Typ B Mechanismen sind in diesem Sinne unüberwindbar.

Typ A „Ein Mechanismus vom Typ A ist ein Sicherheitsmechanismus mit einer potentiellen Schwachstelle in seinem Algorithmus, seinen Prinzipien oder seinen Eigenschaften, aufgrund derer er durch Einsatz ausreichender Ressourcen, Fachkenntnisse und entsprechender Gelegenheiten mit einem direkten Angriff überwunden werden kann. Ein Beispiel für einen Mechanismus vom Typ A ist ein Authentisierungsprogramm, bei dem ein Paßwort verwendet wird; wenn das Paßwort erraten werden kann, indem nacheinander alle möglichen Paßwörter ausprobiert werden, handelt es sich um einen Authentisierungsmechanismus vom Typ A. Mechanismen vom Typ A bedienen sich häufig eines "Geheimnisses" wie etwa eines Paßwortes oder eines kryptographischen Schlüssels.

„Alle Mechanismen vom Typ A ... haben eine Stärke, die dem Aufwand an Ressourcen, Fachkenntnissen und Gelegenheiten, zur Gefährdung der Sicherheit durch einen direkten Angriff auf den Mechanismus entspricht.“

43 Wie wird nun bei Typ A Mechanismen die Stärke definiert?

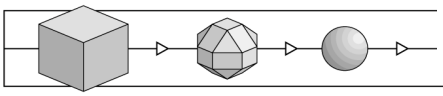
„Alle kritischen Sicherheitsmechanismen (d.h. diejenigen, deren Versagen eine Sicherheitslücke hervorrufen würde), werden hinsichtlich ihrer Fähigkeit be-

wertet, einem direkten Angriff zu widerstehen. Die Mindeststärke jedes kritischen Mechanismus wird entweder als niedrig, mittel oder hoch bewertet.

niedrig „Damit die Mindeststärke eines kritischen Mechanismus als niedrig eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen zufälliges unbeabsichtigtes Eindringen bietet, während er durch sachkundige Angreifer überwunden werden kann.“

mittel „Damit die Mindeststärke eines kritischen Mechanismus als mittel eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln bietet.“

hoch „Damit die Mindeststärke eines kritischen Mechanismus als hoch eingestuft werden kann, muß erkennbar sein, daß er nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird."



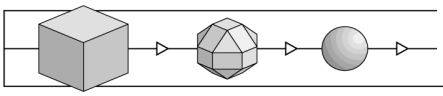
6 Anhänge

6.1 Glossar

Das Glossar erläutert die in dieser Broschüre verwendeten Begriffe, erhebt allerdings keinerlei Anspruch auf Vollständigkeit oder Allgemeingültigkeit. Der Begriff *Sicherheit* meint hier stets Sicherheit im Kontext der Informationstechnik.

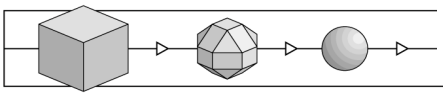
Akkreditierung	– Prozeß mit dem Ziel der Bestätigung, daß eine Prüfstelle den Anforderungen der Norm DIN EN 45001 entspricht. Eine Akkreditierung wird durch eine *Akkreditierungsstelle* durchgeführt. Allgemein anerkannt sind Akkreditierungen von Akkreditierungsstellen, die im Deutschen Akkreditierungsrat (DAR) vertreten sind. – Ergebnis eines Akkreditierungsverfahrens
Anerkennung	Ausdruck und Bestätigung der Gleichwertigkeit (von Zertifikaten und Lizenzen).
Auftraggeber	Eine natürliche oder juristische Person, die einen Auftrag (hier:) zur Zertifizierung oder Evaluierung erteilt; sie muß eine ausreichende Verfügungsberechtigung über das zu zertifizierende Objekt besitzen.
Common Criteria	Sicherheitskriterien, die aus dem amerikanischen Orange Book / den Federal Criteria, den europäischen ITSEC und den kanadischen CTCPEC hervorgegangen sind und ein weltweit akzeptierter Sicherheitsstandard werden sollen.
Bestätigungsstelle	Stelle, die im Einklang mit SigG und SigV Sicherheitsbestätigungen für technische Komponenten und für die Umsetzung von Sicherheitskonzepten bei Trust Centern herausgibt.
DebisZERT	Name des Zertifizierungsschemas von debis IT Security Services.
Dienstleistungsbereich	Bezeichnung für einen bestimmten Typ von Verfahren innerhalb von debisZERT.
DIN EN 45000	Normen-Reihe, die einschlägige Standards insbesondere für Prüf- und Zertifizierungsstellen enthält.
Einzelbericht	Bericht einer Prüfstelle zu einzelnen Prüfaspekten bei einer Evaluierung

Erst-Zertifizierung	Erstmalige Zertifizierung eines Produkts, Systems oder einer Dienstleistung.
Evaluationsstufen	s. Sicherheitsstufen.
Evaluator	Prüfer / in in einer Prüfstelle.
Evaluierung	Prüfung eines Produktes, Systems oder einer Dienstleistung auf der Basis von Sicherheitskriterien oder einer Sicherheitsnorm.
Evaluierungsbericht	Abschlußbericht einer Prüfstelle über Ablauf und Ergebnis einer Evaluierung. (Name „ETR“ im ITSEC-Kontext)
Hersteller-Laboratorium	Bei dem Hersteller eines Produkts / Systems oder bei dem Anbieter von Dienstleistungen angesiedelte Organisationseinheit, die Evaluierungen durchführt.
Integrität	Klassisches Sicherheitsziel: Daten sollen nur von Befugten geändert werden können.
IT-Dienstleistung	Dienstleistung, die sich bei ihrer Erbringung auf IT-Produkte und IT-Systeme abstützt.
IT-Komponente	Abgrenzbarer Teil eines IT-Produkts oder eines IT-Systems.
IT-Produkt	Software und / oder Hardware, die bei einem Anbieter (Hersteller, Vertreiber) erworben werden kann.
ITSEC	Information Technology Security Evaluation Criteria: Europäischer de facto Standard für die Evaluierung von IT-Produkten und IT-Systemen.
ITSEM	Information Technology Security Evaluation Manual: Handbuch zu den ITSEC, das vor allem die Durchführung von Evaluierungen betrifft.
IT-System	– Eine in sich funktionsfähige Kombination von IT-Produkten. – (ITSEC:) Eine reale Installation von IT-Produkten mit einer bekannten Einsatzumgebung.
Lizenz (persönliche)	Bestätigung einer persönlichen Qualifikation (hier im Kontext von debisZERT).
Lizenzvereinbarung	Vereinbarung zwischen einer Prüfstelle und einer Zertifizierungsstelle - den Ablauf und die Verantwortlichkeiten bei einer Evaluierung und Zertifizierung betreffend.
Meilensteinplan	Projekt- / Terminplan für die Durchführung einer Evaluierung und Zertifizierung
Problembericht	Bericht einer Prüfstelle an die Zertifizierungsstelle über besondere Probleme bei einer Evaluierung



Prüfbegleiter	Mitarbeiter / in der Zertifizierungsstelle, führt die Prüfbegleitung durch.
Prüfbegleitung	Verfahren der Zertifizierungsstelle, um die Ordnungsmäßigkeit (Kriterienkonformität, einheitliche Vorgehensweise und Bewertungen, etc.) einer Evaluierung zu überprüfen.
Prüfbericht	Einzelbericht oder Evaluierungsbericht
Prüfstelle	Stelle, die Evaluierungen durchführt.
Regulierungsbehörde	die nach §66 Telekommunikationsgesetz (TKG) zuständige Regulierungsbehörde für Telekommunikation und Post
Re-Zertifizierung	Nach Änderungen am zertifizierten Objekt notwendig werdende Zertifizierung der geänderten Version; kann auch bei Wechsel von Werkzeugen, Produktions- und Auslieferungsprozessen, Sicherheitskriterien erforderlich werden.
Sicherheitsbestätigung	In debisZERT eine juristisch verbindliche Bestätigung von Sicherheitseigenschaften; z.B. eine Bescheinigung, die die Erfüllung der Anforderungen des Signaturgesetzes bestätigt.
Sicherheitsfunktion	Funktionen eines IT-Produktes oder IT-Systems zur Abwehr bestimmter Bedrohungen.
Sicherheitskriterien	Dokument, das technische Anforderungen an Produkte, Systeme und / oder Dienstleistungen enthalten kann, zumindest aber die Evaluierung solcher Anforderungen beschreibt.
Sicherheitsnorm	Anforderungen an Produkte, Systeme oder Dienstleistungen die Sicherheit betreffend.
Sicherheitsstandard	Zusammenfassender Begriff für Sicherheitskriterien und Sicherheitsnormen.
Sicherheitsstufen	In manchen Kriterienwerken (z.B. ITSEC, CC) definierte Stufen, die aufgrund unterschiedlicher Anforderungen an das zu zertifizierende Objekt und an die Tiefe der Prüfung eine unterschiedlich hohe Sicherheit ausdrücken.
Sicherheitszertifikat	s. Zertifikat
Signaturgesetz - SigG	§3 des Informations- und Kommunikationsdienstegesetzes (IuKDG), in Deutschland gültig seit 1.8.1997.
Signaturverordnung - SigV	Amtliche Ausführungsbestimmungen zum Signaturgesetz.

System-Akkreditierung	Freigabe eines IT-Systems oder einer IT-Dienstleistung zur Nutzung (hier unter dem Blickwinkel ausreichender Sicherheit).
Trust Center	Stelle, die die Zugehörigkeit von Signaturschlüsseln zu einer Person durch ein (elektronisches) Zertifikat bestätigt - im Signaturgesetz als „Zertifizierungsstelle“ bezeichnet.
Verfahrenskennung	Code-Bezeichnung für ein Bestätigungsverfahren
Verfügbarkeit	Klassisches Sicherheitsziel: Daten sollen Befugten stets zur Verfügung stehen, d.h. nicht von Unbefugten vorenthalten werden können oder aufgrund technischer Defekte nicht verfügbar sein.
Verfügungsberechtigung	hier: Berechtigung, alle mit einer Evaluierung und Zertifizierung verbundenen Inspektionen an einem Produkt, System oder einer Dienstleistung zulassen zu können.
Vertraulichkeit	Klassisches Sicherheitsziel: Daten sollen nur durch Befugte zur Kenntnis genommen werden können.
Vor-Zertifizierung	Bestätigung der Ergebnisse einer Voruntersuchung einer produkt- bzw. prozeßspezifischen Sicherheitsnorm oder eines sicherheitsrelevanten Werkzeugs (im Hinblick auf spätere Zertifizierungen).
Zertifikat	Zusammenfassende (Kurz-)Darstellung eines Zertifizierungsergebnisses; wird durch die Zertifizierungsstelle ausgestellt.
Zertifizierer	Mitarbeiter / in einer Zertifizierungsstelle, die eine Zertifizierung durchführt.
Zertifizierung	Unabhängige Bestätigung der Ordnungsmäßigkeit einer Evaluierung. Auch Bezeichnung für das Gesamtverfahren bestehend aus Evaluierung, Prüfbegleitung und Ausstellung von Zertifikaten und Zertifizierungsreports.
Zertifizierungskennung	Code-Bezeichnung für ein Zertifizierungsverfahren.
Zertifizierungsreport	Bericht über Gegenstand, Ablauf und Ergebnis eines Zertifizierungsverfahrens; wird durch die Zertifizierungsstelle ausgestellt.
Zertifizierungsschema	Zusammenfassung aller Grundsätze, Regeln und Verfahren einer Zertifizierungsstelle.
Zertifizierungsstelle	Stelle, die Zertifizierungen durchführt. (s. auch *Trust Center* für eine zweite Bedeutung.)
ZKA-Kriterien	Sicherheitskriterien des Zentralen Kreditausschusses.



6.2 Referenzen

/ BSIG / Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz - BSIG), BGBl. I. vom 17. Dezember 1990, Seite 2834 ff.

/ CC / Common Criteria for Information Technology Security Evaluation, Version 1.0, 31. Januar 1996; Version 2.0 Draft, 19.12.97

/ EBA / Kriterien für die sicherheitstechnische Bewertung und Konstruktion von CIR-Netzkomponenten, Eisenbahn-Bundesamt, Version 1.0 vom 8.2.94

/ ITSEC / Information Technology Security Evaluation Criteria (ITSEC), Version 1.2 (1991), ISBN 92-826-3004-8

(deutsche Übersetzung:) Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Version 1.2 (1991), Bundesanzeiger-Verlag Köln, ISBN 92-826-3003-X

(französische Übersetzung:) Critères d'Évaluation de la Sécurité des Systèmes Informatiques (ITSEC), Version 1.2 (1991), ISBN 92-826-3005-6

/ ITSEM / Information Technology Security Evaluation Manual (ITSEM), Version 1.0 (1993), ISBN 92-826-7087-2

(deutsche Übersetzung:) Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik, Version 1.0 (1993), Bundesanzeiger Verlag Köln, ISBN 92-826-7078-2

/ IuKDG / Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG), BGBl. I. vom 28. Juli 1997, Seite 1870 ff.

/ JIL / Joint Interpretation Library, Version 1.04, Dez 97

/ Mkat12 / Maßnahmenkatalog nach §12 Abs. 2, RegTP, http: / / www.RegTp.de / Fachinfo / Digitale%20Signatur / start.htm

/ Mkat16 / Maßnahmenkatalog nach §16 Abs. 6, RegTP, http: / / www.RegTp.de / Fachinfo / Digitale%20Signatur / start.htm

/ SigG / Artikel 3 von / IuKDG /

/SIGV/ Verordnung zur digitalen Signatur (Signaturverordnung - SigV), BGBl. I. vom 27.10.1997, Seite 2498 ff.

/TKG/ Telekommunikationsgesetz (TKG), BGBl. I. vom 25.7.1996, Seite 1120

/V01/ Zertifikate gemäß ITSEC/CC, Dienstleistungsbereich 1, debisZERT, Version 1.0, 6.4.98

/V02/ Bestätigungen für Produkte gemäß Signaturgesetz, Dienstleistungsbereich 2, debisZERT, Version 1.0, 6.4.98

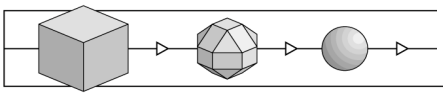
/V04/ Zertifikate mit Anerkennung durch das BSI, Dienstleistungsbereich 4, debisZERT, Version 1.2, 6.4.98

/Z01/ Zertifizierungsschema, debis IT Security Services, Version 1.2, 6.4.98

/Z02/ Zertifizierte IT-Produkte, IT- Systeme und IT-Dienstleistungen, debisZERT, Version 1.0, 6.4.98

6.3 Abkürzungen

AA	Arbeitsanweisungen
AIS	Anforderung einer Interpretation von Sicherheitskriterien
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Errichtungsgesetz
CC	Common Criteria
CTCPEC	Canadian Trusted Computer Products Evaluation Criteria
DAR	Deutscher Akkreditierungsrat
DBAG	Deutsche Bahn AG
debisZERT	Zertifizierungsschema der debis IT Security Services
DLB	Dienstleistungsbereich
EBA	Eisenbahn-Bundesamt
ETR	Evaluation Technical Report (Evaluierungsbericht)
EVG	Evaluationsgegenstand
IT	Informationstechnik
ITSEC	IT Security Evaluation Criteria



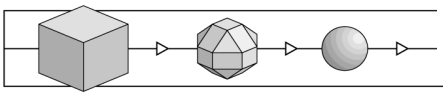
ITSEM	IT Security Evaluation Manual
IuKDG	Informations- und Kommunikationsdienstegesetz
LG	Lenkungsgremium
SigG	Signaturgesetz
SigV	Signaturverordnung
TKG	Telekommunikationsgesetz
ZKA	Zentraler Kreditausschuß
ZL	Leiter der Zertifizierungsstelle
ZZ	(für ein Verfahren) zuständiger Zertifizierer

7 Re-Zertifizierungen und technische Anhänge

Bei Änderungen an dem zertifizierten Objekt kann nach Maßgabe der Verfahrensregeln von debisZERT eine Re-Zertifizierung erfolgen. Die hier in zeitlicher Reihenfolge erscheinenden Anhänge beschreiben die Art der Änderungen, die neue Produktversion und den Zertifizierungsstatus.

Bei neuen Erkenntnissen über die Sicherheit des zertifizierten Objektes kann ein technischer Anhang zum Zertifizierungsreport herausgegeben werden.

Re-Zertifizierungen und neue technische Anhänge werden in der Druckschrift /Z02/ und über WWW angekündigt.



Ende der Erstausgabe des Zertifizierungsreports.