# Zertifizierungsreport

**Bundesamt für Sicherheit in der Informationstechnik**

## BSI-DSZ-CC-0405-2007

zu

## Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06

der

## Fujitsu Siemens Computers GmbH

BSI- Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49(0)3018 9582-0, Telefax +49(0)3018 9582-5455, Infoline +49(0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

**BSI-DSZ-CC-0405-2007**

# Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06

der

## Fujitsu Siemens Computers GmbH

Common Criteria Arrangement
für Komponenten bis EAL4

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

**Prüfergebnis:**

Funktionalität: **Produktspezifische Sicherheitsvorgaben**
**Common Criteria Teil 2 konform**

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

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

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

Die auf der Rückseite aufgeführten Anmerkungen sind Bestandteil dieses Zertifikates.

Bonn, den 16. Januar 2007

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik

IT Security Certified
SOGIS - MRA

Dr. Helmbrecht L.S.

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

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

# Vorbemerkung

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

Teil A: Zertifizierung

Teil B: Zertifizierungsbericht

Teil C: Auszüge aus den technischen Regelwerken

# A Zertifizierung

## 1 Grundlagen des Zertifizierungsverfahrens

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

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

---

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

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

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

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

# 2 Anerkennungsvereinbarungen

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

## 2.1 ITSEC/CC - Zertifikate

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

## 2.2 CC - Zertifikate

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

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

# 3 Durchführung der Evaluierung und Zertifizierung

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

Das Produkt Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06 hat das Zertifizierungsverfahren beim BSI durchlaufen. Es handelt sich um eine Re-Zertifizierung basierend auf BSI-DSZ-CC-0280-2004.

Die Evaluation des Produkts Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06 wurde von TÜV Informationstechnik GmbH durchgeführt. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Antragsteller, Hersteller und Vertreiber ist

Fujitsu Siemens Computers GmbH
Bürgermeister-Ulrich-Strasse 100
86199 Augsburg, Deutschland .

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 16. Januar 2007 vom BSI abgeschlossen.

Das bestätigte Vertrauenswürdigkeitspaket gilt nur unter der Voraussetzung, daß

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

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

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

[6] Information Technology Security Evaluation Facility

# 4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-16.

Das Produkt Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

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

[7] Fujitsu Siemens Computers GmbH
Bürgermeister-Ulrich-Strasse 100
86199 Augsburg, Deutschland

# B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

# Gliederung des Zertifizierungsberichtes


| | | |
|---|---|---|
| 1 | Zusammenfassung | 3 |
| 2 | Identifikation des EVG | 7 |
| 3 | Sicherheitspolitik | 8 |
| 4 | Annahmen und Klärung des Einsatzbereiches | 8 |
| 5 | Informationen zur Architektur | 9 |
| 6 | Dokumentation | 9 |
| 7 | Testverfahren | 9 |
| 8 | Evaluierte Konfiguration | 11 |
| 9 | Ergebnisse der Evaluierung | 11 |
| 10 | Kommentare und Empfehlungen | 13 |
| 11 | Anhänge | 13 |
| 12 | Sicherheitsvorgaben | 13 |
| 13 | Definitionen | 13 |
| 14 | Literaturangaben | 15 |

# 1 Zusammenfassung

Der EVG besteht aus der Tastatur mit integriertem Kartenleser und stellt neben der normalen Tastaturfunktionalität die Möglichkeit zur Verfügung, kontaktbehaftete Speicher- und Prozessorchipkarten zu verarbeiten. Die PIN wird über den Nummernblock des TOE eingegeben, wobei die sichere PIN-Eingabe vom TOE nur für Prozessorchipkarten unterstützt wird. Die Prozessorkarten müssen den Spezifikationen ISO 7816[11] bzw. EMV [13] genügen und die Übertragungsprotokolle T=0 und T=1 unterstützen. Bei synchronen Chipkarten basiert das Übertragungsprotokoll auf den herstellerspezifischen Spezifikationen.

Der TOE kann an jedem USB-fähigen PC-System betrieben werden und ist für den Einsatz im nichtöffentlichen oder privaten Bereich vorgesehen. Hierzu zählt auch die normale Büroumgebung mit geregelten Zugriffsmöglichkeiten. Die Schnittstelle zwischen Host (i. A. ein PC) und dem EVG basiert auf dem Funktionsumfang des CCID-Standards [12]. Ziel ist es das Kartenterminal u.a. für die Applikation „digitale Signatur“ nach dem deutschen Signaturgesetz [14] einzusetzen.

Der EVG bietet die Möglichkeit, die PIN über den Nummernblock (numerisch) einzugeben. Bei der Eingabe über den Nummernblock hat das alphanumerische Feld keine Funktion.

Um die sichere PIN-Eingabe zu starten, wird von der Applikation das PIN-Eingabekommando an den EVG gesendet, welcher anschließend in den PIN-Eingabemodus umschaltet. Optisch wird dies dem Nutzer über die rot blinkende LED angezeigt. Der Eingabefortschritt wird bei der PIN-Eingabe mittels der Übertragung von Dummycodes [*] dem System mitgeteilt. Nach erfolgreicher Eingabe der PIN wird diese direkt zur Chipkarte gesendet und anschließend wieder in die Tastaturfunktion zurückgekehrt. Der EVG stellt sicher, dass die PIN nur zur Chipkarte hin übertragen wird.

Um sicherheitstechnische Veränderungen am Kartenterminal erkennbar zu machen, werden am Produkt über die Trennkante zwischen Gehäuseober- und Unterteil authentische und fälschungssichere Siegel aufgebracht. Diese gewährleisten, daß ein Öffnen des Gehäuses ohne Beschädigung der Siegel nicht möglich ist. Um den Nutzer auf die Unversehrtheit aufmerksam zu machen, wird er in der Bedienungsanleitung explizit darauf hingewiesen. Dem Nutzer werden dort das Aussehen, die Beschaffenheit und die Position der Siegel beschrieben.

Die Kommunikation des Kartenterminals basiert auf dem von Microsoft spezifizierten PC/SC-Standard, welcher Bestandteil der meisten heute am Markt verfügbaren Betriebssysteme (wie z.B. Windows XP / 2000, Linux-Derivate) ist. Die Treibersoftware gehört nicht zum Evaluationsumfang.

Die Evaluation des Produkts Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06 wurde von TÜV Informationstechnik GmbH durchgeführt und am 16. November 2006 abgeschlossen. Das Prüflabor TÜV Informationstechnik GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[8].

[8] Information Technology Security Evaluation Facility

Antragsteller, Hersteller und Vertreiber ist

Fujitsu Siemens Computers GmbH
Bürgermeister-Ulrich-Strasse 100
86199 Augsburg, Deutschland

## 1.1 Vertrauenswürdigkeitspaket

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

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

Tabelle 1: Vertrauenswürdigkeitskomponenten und EAL-Zusätze

## 1.2 Funktionalität

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

| Sicherheitsanforderungen | Thema |
|---|---|
| **FDP** | **Schutz der Benutzerdaten** |
| FDP_ACC.1 | Teilweise Zugriffskontrolle |
| FDP_ACF.1 | Zugriffskontrolle basierend auf Sicherheitsattributen |
| FDP_RIP.2 | Vollständiger Schutz bei erhalten gebliebenen Informationen |
| **FPT** | **Schutz der TSF** |
| FPT_PHP.1 | Passive Erkennung materieller Angriffe |
| **FTA** | **EVG-Zugriff** |
| FTA_TAB.1 | Vorgegebene EVG Zugriffswarnmeldung |

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

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

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

| Sicherheitsfunktion | Beschreibung |
|---|---|
| Speicherwiederaufbereitung (SF.1) | Die Kommunikation zwischen PC-System und Chipkarte basiert gemäß CCID [12] auf den sogenannten APDU's. Wird eine APDU über die USB-Schnittstelle im Kartenterminal empfangen, so wird sie zuerst zwischengespeichert, um anschließend zur Chipkarte gesendet zu werden. Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos bzw. dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet, um sicherzustellen, daß keine persönlichen Identifikationsdaten bzw. Datenfragmente im Kartenterminal erhalten bleiben. Außerdem wird die LED zur Anzeige der sicheren PIN-Eingabe ausgeschaltet. |
| Schutz der PIN (SF.2) | Das Umschalten des Nummernblocks im Kartenterminal in den sicheren PIN-Eingabemodus wird durch ein explizites CT-Kommando nach CCID [12] durchgeführt. Dieses CT-Kommando enthält die PIN-Handlingsvereinbarungen und das Chipkartenkommando, in welches die PIN an die spezifizierte Stelle integriert wird. Anhand des Instructionbytes des Chipkartenkommandos wird überprüft, ob es sich um ein PIN-Kommando handelt, welches explizit eine PIN-Eingabe erwartet. Im folgenden sind die zugelassenen Instructionbytes aufgeführt:<br>• VERIFY (ISO/IEC 7816-4): INS=0x20<br>• CHANGE REFERENCE DATA (ISO/IEC 7816-8): INS=0x24<br>• ENABLE VERIFICATION REQUIR EMENT (ISO/IEC 7816-8): INS=0x28<br>• DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26<br>• RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C<br>Durch Umschalten des Nummernblocks in den PIN-Eingabemodus wird die Eingabe der persönlichen Identifikationsdaten im RAM zwischengespeichert, um sie nach Beendigung der Eingabe direkt mit dem PIN-Kommando zur Chipkarte zu senden. Der PIN-Eingabemodus wird optisch durch ein rotes Blinken der SPE-LED angezeigt bis die Vollständigkeit der PIN erreicht ist, beziehungsweise der Vorgang abgebrochen wird. Zum Abbruch des Vorgangs zählen das Ziehen der Karte, das Betätigen der Abbruchtaste und das Überschreiten der vorgegebenen Eingabezeit.<br>Der Eingabefortschritt wird mittels der Übertragung von Dummycodes [*] dem System mitgeteilt. |

Tabelle 3: Sicherheitsfunktionen des EVG

| Sicherheitsmaßname | Beschreibung |
|---|---|
| Versiegelung (SM.1) | Anhand authentischer und fälschungssicherer Sicherheitssiegeln, welche über die Trennkante zwischen Gehäuseunter- und Oberteil geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden. Dies wird dadurch sichergestellt, dass ein Öffnen nicht ohne Beschädigung des Siegels möglich ist.<br>Die Beschaffenheit (Zerstöreigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann. Das eingesetzte Siegel ist fälschungssicher, weist Authentizitätsmerkmale auf und erfüllt die Sicherheitsstufe 2 entsprechend der BSI 7500 Druckschrift „Produkte für die materielle Sicherheit“ [10]. |

Tabelle 4: Sicherheitsfunktionen und –maßnahmen des EVG

## 1.3 Stärke der Funktionen

Für den TOE gelten keine funktionalen Sicherheitsanforderungen, die für eine Betrachtung der Stärke (SOF) in Frage kommen. Für Details siehe Kap. 9 dieses Berichtes.

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

Zu schützen sind die PIN als Identifikationsmerkmal des Chipkarteninhabers, sowie die Firmware und Hardware des TOE.

Als Bedrohungen für den TOE durch einen Angreifer gelten das Ausspähen der Identifikationsdaten und die sicherheitstechnische Veränderung am TOE. Im Einzelnen werden im Security Target die folgenden Bedrohungen aufgeführt:

| Bedrohungen | Beschreibung |
|---|---|
| T.1 | Ein Angreifer könnte versuchen, durch Einsatz von Sniffertools (Hardware oder Software) die über den TOE eingegebene PIN auszuspähen. |
| T.2 | Ein Angreifer könnte versuchen, eine PIN-Eingabe zu provozieren und damit die PIN zu erlangen. |
| T.3a | Ein Angreifer könnte versuchen, den TOE in seinen Bestandteilen (Hardware und Firmware) zu manipulieren, um die PIN zu ermitteln. |
| T.3b | Ein Angreifer könnte versuchen, die im TOE zwischengespeicherte PIN auszulesen. |
| T.4 | Ein Angreifer könnte versuchen, die PIN in einen ungeschützten Bereich der Chipkarte zu schreiben, um sie anschließend daraus auszulesen |
| T.5 | Ein Angreifer könnte versuchen, das Sicherheitssiegel zu manipulieren, um sicherheitstechnische Veränderungen am TOE zu verschleiern. |

Tabelle 5: Bedrohungen für den EVG

Organisatorische Sicherheitspolitiken sind im Security Target nicht angegeben.

## 1.5 Spezielle Konfigurationsanforderungen

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

Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06 des Herstellers Fujitsu Siemens Computers GmbH.

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

Eine Konfiguration des EVG und eine damit verbundene Beeinflussung der Sicherheitsfunktionen durch den Nutzer ist nicht möglich.

## 1.6 Annahmen über die Einsatzumgebung

Die Chipkartenleser-Tastatur KB SCR Pro ist für den Gebrauch im privaten und nicht öffentlichen Bereich vorgesehen. Hinsichtlich der Benutzung des EVG werden die folgenden Annahmen im Security Target [6, Kapitel 3.1] genannt:

| Annahmen | Beschreibung |
|---|---|
| AE.1 | Einsatz im privaten oder nichtöffentlichen Bereich |
| AE.2 | Verwendung von entsprechenden Prozessorchipkarten. |
| AE.3 | Überprüfung der Siegel. |
| AE.4 | Unbeobachtete Eingabe der PIN. |
| AE.5 | Überprüfung der LED bei der PIN-Eingabe. |
| AE.6 | Eingabe der PIN über den Nummernblock. |

Tabelle 6: Annahmen

## 1.7 Gewährleistungsausschluß

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

# 2 Identifikation des EVG

Der EVG heisst:

**Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06**

Die folgende Tabelle beschreibt den Auslieferungsumfang:

| No | Type | Identifier | Release | Form der Auslieferung |
|---|---|---|---|---|
| 1 | HW / SW | KB SCR Pro mit Firmware | Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06 | einzelverpackt in Kartonage |
| 2 | DOK | Fujitsu Siemens USB-Security-Tastaturen | A26381-K329-Z170-4-7419, Ausgabe 5 | gedruckte Form |
| 3 | Software | Treiber-CD | | CD-ROM |

Tabelle 7: Auslieferungsumfang des TOE

Der EVG wird nach der Montage an verschiedenen Standorten (siehe Kapitel 8) an die Fujitsu Siemens Computers GmbH in Augsburg geliefert. Dort erfolgt die Einzelverpackung in Kartons mit der Beilegung der Bediengungsanleitung und die Lagerung in einem geschützen Bereich. Speditionen liefern den EVG entweder an den Endkunden direkt oder an den Einzelhandel aus.

Der Benutzer kann den EVG anhand des Typschildes identifzieren, das auf der Rückseite der Tastatur sowie auf dem Verpackungskarton aufgebracht ist. Auf dem Typschild ist die

Sachnummer vermerkt, aus der gemäß der Beschreibung im Security Target auch die Firmwareversion extrahierbar ist.

# 3 Sicherheitspolitik

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

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

Die Sicherheitspolitik der Chipkartenleser-Tastatur KB SCR Pro zielt demnach auf den Schutz der PIN und der Integrität der Firmware sowie auf die zuverlässige Anzeige von sicherheitstechnischen Änderungen an der Hardware ab.

# 4 Annahmen und Klärung des Einsatzbereiches

## 4.1 Annahmen über den Einsatz

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

| Annahmen | Beschreibung |
|---|---|
| AE.2 | Es wird angenommen, daß der Benutzer ausschließlich Prozessorkarten benutzt, die den Spezifikationen ISO 7816 [11] bzw. EMV 2000 [13] genügen |
| AE.3 | Es wird angenommen, daß sich der Nutzer vor der Inbetriebnahme, und regelmäßig vor Benutzung des Gerätes durch Kontrolle der Unversehrtheit der Siegel überzeugt, ob keine sicherheits-technischen Veränderungen am Kartenterminal vorgenommen wurden. |
| AE.4 | Es wird angenommen, daß der Benutzer eine unbeobachtete Eingabe der Identifikationsdaten (PIN) gewährleistet. |
| AE.5 | Es wird angenommen, daß der Benutzer während der PIN-Eingabe über den Nummernblock den Status der LED dahingehend überprüft, ob der Modus der sicheren PIN-Eingabe aktiv ist. |
| AE.6 | Es wird angenommen, daß der Benutzer die PIN über den Nummernblock eingibt. |

Tabelle 8: Annahmen über den Einsatz des EVG

## 4.2 Angenommene Einsatzumgebung

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

| Annahmen | Beschreibung |
|---|---|
| AE.1 | Es wird angenommen, daß der TOE als Kartenterminal für die nicht öffentliche Umgebung eingesetzt wird. |

Tabelle 9: Annahmen über die Einsatzumgebung des EVG

# 5 Informationen zur Architektur

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

- Mikrocontroller (XCHIP)
- USB-Interface
- Anzeigeeinheit (Leuchtdioden)
- Tastenmatrix mit Nummernblock
- Chipkarteninterface
- Quarz

Die Firmware ist hauptsächlich für die Sicherheitsfunktionalität verantwortlich. Sie lässt sich folgendermaßen in Teilsysteme untergliedern:

- System

  Dieses Teilsystem enthält die elementaren Funktionen des Mikroprozessorsystems wie die Initialisierung der Hard- und Firmware.

- USB

  Mit diesem Teilsystem wird die Kommunikation über die USB-Schnittstelle der Tastatur geregelt.

- Chipkarte

  Dieses Teilsystem enthält die Firmware-Anteile für die Umsetzung der Chipkarten-Bedienung wie z.B. Anteile an der sicheren PIN-Eingabe.

- Keyboard

  Die Firmware-Anteile zur Initialisierung und Umsetzung der Keyboardfunktionalität sind in diesem Teilsystem enthalten. Da über den Nummernblock der Tastatur auch die PIN eingegeben wird, ist dieses Teilsystem auch maßgeblich an der Umsetzung der Sicherheitsfunktionen beteiligt.

# 6 Dokumentation

Für die Chipkartenleser-Tastatur stellt der Hersteller die folgende Bedienungsanleitung bereit:

- Fujitsu Siemens USB-Security-Tastaturen, A26381-K329-Z170-4-7419, Ausgabe 5,

# 7 Testverfahren

## 7.1 Hersteller Tests

Die Herstellertests wurden an einem Muster des EVG durchgeführt, das wie in den Sicherheitsvorgaben definiert mit der Firmware-Version 1.06 ausgestattet ist.

Für die Tests wird der EVG an einem IBM-kompatiblen PC-System mit 32-Bit Windows Betriebssystem betrieben. Gemäß der Teststrategie des Herstellers sollen die vorgesehenen funktionalen Tests am EVG die Übereinstimmung mit den in der funktionalen Spezifikation beschriebenen Sicherheitsfunktionen prüfen und zeigen. Dabei werden die Tests getrennt nach den Sicherheitsfunktionen durchgeführt und dokumen-

tiert. Für jeden Test definiert der Hersteller in seinem Testplan die Testziele, die Prozeduren zur Testdurchführung, die erwarteten Testergebnisse definiert und protokolliert die tatsächlich erzielten Ergebnisse.

Wie durch die Testabdeckungsanalyse nachgewiesen ist, hat der Hersteller den EVG systematisch auf dem Niveau der Sicherheitsfunktionalitäten aus der funktionalen Spezifikation und der Teilsysteme aus dem Entwurf auf hoher Ebene getestet.

Es wurden keine Fehler entdeckt und es traten keine Abweichungen bzgl. der beschriebenen Sicherheitsfunktionalität auf. Infolgedessen konnten alle Sicherheitsfunktionen erfolgreich getestet werden.

## 7.2 Unabhängige Tests der Prüfstelle

Vom Hersteller wurde der EVG mit der Bezeichnung KB SCR Pro: S26381-K329-V220 HOS:01 geliefert und für die unabhängigen Tests der Prüfstelle einschließlich der stichprobenhaften Wiederholung von Herstellertests als Prüfobjekt zur Verfügung gestellt. Für die Tests wird der EVG an einem IBM-kompatiblen PC-System mit 32-Bit Windows Betriebssystem betrieben.

Die Tests werden getrennt nach den Sicherheitsfunktionen durchgeführt und dokumentiert. Für jeden Test werden ein Testplan mit Testziel erstellt, die verwendete Testkonfiguration aufgeführt, das Testverfahren beschrieben, die erwarteten Testergebnisse definiert und die tatsächlich erzielten Ergebnisse dargestellt.

Der Evaluator spezifiziert zu jeder Sicherheitsfunktion unabhängige Tests, deren Ergebnisse entsprechend dem oben beschriebenen Verfahren dokumentiert sind. Die tatsächlichen Ergebnisse stimmten mit den erwarteten Ergebnissen überein.

Weiterhin hat der Evaluator aus den Herstellertests der Sicherheitsfunktionen des EVG eine Stichprobe ausgewählt und getestet. Auch hierbei stellten sich die erhaltenen Testergebnisse sich für alle durchgeführten Tests wie erwartet ein.

Es wurden keine Fehler entdeckt und es traten keine Abweichungen bzgl. der beschriebenen Sicherheitsfunktionalität auf. Infolgedessen konnten alle Sicherheitsfunktionen erfolgreich getestet werden.

## 7.3 Penetrationstests der Prüfstelle

Der Evaluator hat systematisch eine Schwachstellenanalyse auf Basis der Herstellerdokumente und Prüfberichten sowie gemäß den Anweisung aus der Evaluationsmethodologie [2] bzw. den AIS [4, AIS 34] durchgeführt. Mit den Penetrationstests zur Widerstandsfähigkeit des EVG hat der Evaluator nicht nur die vollständige und korrekte Implementierung der Sicherheitsfunktion überprüft, sondern auch nach versteckten Funktionen oder weiteren Kommandos gesucht. Die Siegeltests aus der Basis-Evaluation wurden vom Evaluator nicht wiederholt, da sich das EVG-Gehäuse, die Orte der Siegelanbringung und das Siegelmaterial gegenüber der Basis-Evaluation nicht verändert haben.

Der Sicherheitsfunktionen des EVG haben sich während der Penetrationstests wie spezifiziert verhalten. Schwachstellen sind in der beabsichtigten Einsatzumgebung des EVG nicht ausnutzbar.

# 8 Evaluierte Konfiguration

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

**Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06**

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

- Amper Plastik R. Dittrich GmbH & Co, Dachau, Deutschland
- Fujitsu Siemens Computers GmbH, Augsburg, Deutschland
- Omnikey AG, Linz, Österreich

# 9 Ergebnisse der Evaluierung

Der Evaluation Technical Report (ETR), [8] wurde von der Prüfstelle gemäß den Common Criteria [1], der Evaluationsmethodology [2], den Anforderungen des Schemas [3] und allen Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind.

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

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

| Vertrauenskeitsklassen und Komponenten | Kurzform | Urteil |
|---|---|---|
| Prüfung und Bewertung der Sicherheitsvorgaben | CC Klasse ASE | PASS |
| EVG Beschreibung | ASE_DES.1 | PASS |
| Sicherheitsumgebung | ASE_ENV.1 | PASS |
| ST-Einführung | ASE_INT.1 | PASS |
| Sicherheitsziele | ASE_OBJ.1 | PASS |
| PP-Postulate | ASE_PPC.1 | PASS |
| IT-Sicherheitsanforderungen | ASE_REQ.1 | PASS |
| Explizit dargelegte IT-Sicherheitsanforderungen | ASE_SRE.1 | PASS |
| EVG Übersichtsspezifikation | ASE_TSS.1 | PASS |
| Konfiguratationsmanagement | CC Klasse ACM | PASS |
| Autorisierungskontrolle | ACM_CAP.3 | PASS |
| EVG-CM-Umfang | ACM_SCP.1 | PASS |
| Auslieferung und Betrieb | CC Klasse ADO | PASS |
| Erkennung von Modifikationen | ADO_DEL.2 | PASS |
| Installations-, Generierungs- und Anlaufprozeduren | ADO_IGS.1 | PASS |

| Vertrauenskeitsklassen und Komponenten | Kurzform | Urteil |
|---|---|---|
| Entwicklung | CC Klasse ADV | PASS |
| Informelle funktionale Spezifikation | ADV_FSP.1 | PASS |
| Sicherheitsspezifischer Entwurf auf hoher Ebene | ADV_HLD.2 | PASS |
| Teilmenge der Implementierung der TSF | ADV_IMP.1 | PASS |
| Beschreibender Entwurf auf niedriger Ebene | ADV_LLD.1 | PASS |
| Informeller Nachweis der Übereinstimmung | ADV_RCR.1 | PASS |
| Handbücher | CC Klasse AGD | PASS |
| Systemverwalterhandbuch | AGD_ADM.1 | PASS |
| Benutzerhandbuch | AGD_USR.1 | PASS |
| Lebenszyklus-Unterstützung | CC Klasse ALC | PASS |
| Identification der Sicherheitsmaßnahmen | ALC_DVS.1 | PASS |
| Klar festgelegte Entwicklerwerkzeuge | ALC_TAT.1 | PASS |
| Tests | CC Klasse ATE | PASS |
| Analyse der Testabdeckung | ATE_COV.2 | PASS |
| Testen: Entwurf auf hoher Ebene | ATE_DPT.1 | PASS |
| Funktionales Testen | ATE_FUN.1 | PASS |
| Unabhängiges Testen - Stichprobenartig | ATE_IND.2 | PASS |
| Schwachstellenbewertung | CC Klasse AVA | PASS |
| Analysieren und Testen auf unsichere Zustände | AVA_MSU.3 | PASS |
| Stärke der EVG-Sicherheitsfunktionen | AVA_SOF.1 | PASS |
| Hohe Widerstandsfähigkeit | AVA_VLA.4 | PASS |

Tabelle 10: Urteil zu den Vertrauenswürdigkeitskomponenten

Bei dieser Re-Zertifizierung lag der Schwerpunkt der Arbeiten auf der Prüfung der geänderten Funktionalität der Firmware, die der Hersteller in seiner Auswirkungsanalyse [7] beschrieben hat.

Die Evaluierung hat gezeigt, dass:

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

Die Resultate der Evaluierung sind nur anwendbar auf den EVG (Name TOE und evaluierte Konfigurationen mit Bezug auf Kapitel 2 oben)

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

# 10 Kommentare und Empfehlungen

Die Bedienungsanleitung [9] und die Sicherheitsvorgaben [6] enthalten die notwendigen Informationen über den die Verwendung des EVG und alle Sicherheitshinweise sind darin enthalten.

# 11 Anhänge

Keine

# 12 Sicherheitsvorgaben

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

# 13 Definitionen

## 13.1 Abkürzungen

**BSI** Bundesamt für Sicherheit in der Informationstechnik, Bonn

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

**EAL** Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

**IT** Informationstechnik

**PIN** Persönliche Identifikationsnummer

**PP** Protection Profile - Schutzprofil

**SF** Sicherheitsfunktion

**SOF** Strength of Function - Stärke der Funktionen

**ST** Security Target - Sicherheitsvorgaben

**EVG** Evaluationsgegenstand

**TSC** TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle

**TSF** TOE Security Functions - EVG-Sicherheitsfunktionen

**TSP** TOE security policy - EVG-Sicherheitspolitik

## 13.2 Glossar

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

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

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

**Informell** - Ausgedrückt in natürlicher Sprache.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 14 Literaturangaben

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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

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

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

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

[6] Sicherheitsvorgaben BSI-DSZ-0405-2006, Version 1.30, 13.09.2006, Common-Criteria-Dokument Sicherheitsvorgaben EAL3+, Fujitsu Siemens Computers GmbH

[7] Auswirkungsanalyse, Version 1.30, 22.09.2006, Common-Criteria-Dokument Impact Analysis Report Firmware V 1.06, Fujitsu Siemens Computers GmbH (vertrauliches Dokument)

[8] Evaluierungsbericht, Version 1.02, 15.11.2006, EVALUATION TECHNICAL REPORT (ETR), TÜV Informationstechnik GmbH (vertrauliches Dokument)

[9] Fujitsu Siemens USB-Security-Tastaturen, A26381-K329-Z170-4-7419, Ausgabe 5, Fujitsu Siemens Computers GmbH

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

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

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

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

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

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

[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. Geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04. 01. 2005, BGBl. I, S. 2f, 10. 01. 2005.

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

# C Auszüge aus den technischen Regelwerken

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:

a) **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.

b) **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:

a) **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.

b) **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:

a) **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.

b) **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:

a) **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

**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.”