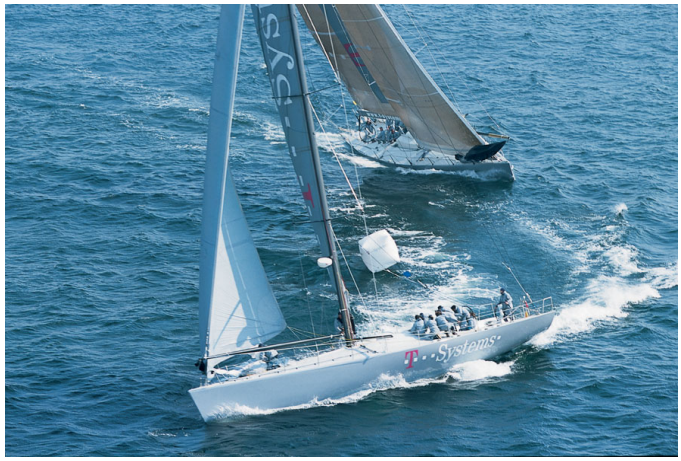
T · · Systems ·



Zertifizierungsreport

T-Systems-DSZ-CC-04181-2006

CardOS V4.3B Re_Cert with Application for Digital Signature

Siemens AG

Deutsches IT-Sicherheitszertifikat

anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

T · · Systems · · ·

CardOS V4.3B Re_Cert with Application for Digital Signature

Siemens AG

Deutscher Akkreditierungs Rat
DAR

DAT-ZE-015/98-01

Das Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle gemäß den Common Criteria Version 2.3, der Common Methodology Version 2.3 und den anzuwendenden Interpretationen des nationalen Zertifizierungsschemas evaluiert. Das Prüfergebnis lautet:

▶ Funktionalität	**Produktspezifische Sicherheitsvorgaben** **Common Criteria Teil 2 erweitert**
▶ Vertrauenswürdigkeit	**Common Criteria Teil 3 konform** **EAL4 mit Zusatz von:** AVA_MSU.3 Vulnerability Assessment: Analysis and testing for insecure states AVA_VLA.4 Vulnerability Assessment: Highly resistant

Dieses Zertifikat gilt nur für die evaluierte Version des Produkts in Verbindung mit dem vollständigen Zertifizierungsreport und den darin aufgeführten evaluierten Konfigurationen. Die Evaluierung und Zertifizierung wurden im Einklang mit den geltenden Regeln des Zertifizierungsschemas der T-Systems und den Vorgaben des BSI für das Deutsche IT-Sicherheitszertifikat durchgeführt. Die Bewertung der Stärke der zur Ver- und Entschlüsselung geeigneten kryptografischen Mechanismen ist von der Anerkennung durch das BSI ausgenommen.

Registrierungsnummer: Bonn, den 30.11.2006

T · · Systems · · ·

T-Systems-
DSZ-CC-04181-2006

Dr. Heinrich Kersten
Leiter der Zertifizierungsstelle

Akkreditiert nach DIN EN 45011 durch
DATech GmbH

Zertifizierungsstelle der T-Systems, c/o T-Systems GEI GmbH, Rabinstr.8, 53111 Bonn
☎ +49-(0)228-9841-0 , Fax: -60, Internet: www.t-systems-zert.com

Vorbemerkungen

Der vorliegende Zertifizierungsreport für den Evaluationsgegenstand (EVG) "CardOS V4.3B Re_Cert with Application for Digital Signature" dient dem Antragsteller als Nachweis der durchgeführten Evaluierung und dem Nutzer als eine Grundlage für die sichere Nutzung.

Kopien des Zertifizierungsreports sind beim Auftraggeber und - mit Zustimmung des Auftraggebers - bei der Zertifizierungsstelle erhältlich.

Die folgenden Stellen im Zertifizierungsreport enthalten wichtige Informationen:

- Abschnitt 1, Absatznummer 3: die genaue Bezeichnung des EVGs einschließlich der Versionsangabe. Der Zertifizierungsreport gilt nur für diesen EVG und diese spezielle Version.

- Abschnitt 6, Absatznummer 28: Angaben zum Auslieferungsverfahren des EVG. Andere Auslieferungsverfahren können unter Umständen nicht die für die Stufe EAL4 erforderliche Sicherheit bieten.

- Abschnitt 6, Absatznummer 29: Angaben zu evaluierten Konfigurationen des EVG. Der EVG gilt nur in diesen Konfigurationen als zertifiziert.

- Abschnitt 6, Absatznummer 30: Angaben zur evaluierten Funktionalität: Nur die hier beschriebenen Sicherheitsfunktionen sind zertifiziert.

- Abschnitt 6, Absatznummer 32: Angaben zur Vertrauenswürdigkeit im Sinne der Sicherheitskriterien.

- Abschnitt 6, Absatznummer 33: Hinweise für den sicherheitsgerechten Einsatz des EVG. Die Sicherheit bei der Anwendung des EVG kann ggf. nicht mehr gegeben sein, wenn diese Hinweise nicht beachtet werden.

In den Sicherheitsvorgaben zum EVG sind insbesondere die Informationen zur Art der Nutzung des EVG, zum Lieferumfang, zu seinen Sicherheitszielen bzw. den betrachteten Bedrohungen und zur Einsatzumgebung zu beachten. Die Sicherheitsvorgaben sind als separates Dokument erhältlich.

Die Prozesse der Evaluierung und Zertifizierung werden nach dem Stand der Technik durchgeführt, können aber keine *absolute* Garantie dafür geben, dass der EVG frei von Schwachstellen ist. Mit steigender Evaluationsstufe verringert sich allerdings die Wahrscheinlichkeit erheblich, dass *ausnutzbare* Schwachstellen unentdeckt bleiben. Dies gilt unter der Voraussetzung, dass alle Anforderungen und Hinweise aus diesem Report ein-

gehalten werden. Andernfalls gilt das Evaluationsergebnis nur noch bedingt: In einem solchen Fall ist eine ergänzende Analyse erforderlich, um festzustellen, ob und in welchem Umfang der EVG auch unter den geänderten Bedingungen noch Sicherheit bieten kann. Die Prüfstelle und die Zertifizierungsstelle können bei der Analyse unterstützen.

Bei Änderungen an dem EVG einschließlich seiner Dokumentation, seinem Auslieferungsverfahren oder seiner Einsatzumgebung ist die Zertifizierung nicht mehr gültig. Es kann jedoch eine Re-Zertifizierung erfolgen, die in einem entsprechenden technischen Anhang zu diesem Zertifizierungsreport dokumentiert wird.

Technische Anhänge werden auch bei neuen Erkenntnissen über die Sicherheit des EVG herausgegeben.

Den Web-Seiten (www.t-systems-zert.com) der Zertifizierungsstelle ist zu entnehmen, ob

- technische Anhänge zu diesem Zertifizierungsreport herausgegeben worden sind (die Anhänge werden fortlaufend nummeriert: T-Systems-DSZ-CC-04181-2006/1, .../2,...) oder
- neue Versionen des EVG sich in der Evaluierung befinden bzw. bereits zertifiziert worden sind.

Jegliche Gewährleistung für den EVG durch die T-Systems ist ausgeschlossen. Die Zertifizierung des EVG ist darüber hinaus nicht gleichzusetzen mit einer generellen Empfehlung der T-Systems für einen *beliebigen* Einsatzzweck des EVG.

Für weitere Auskünfte ist die Zertifizierungsstelle wie folgt erreichbar:

✉ Zertifizierungsstelle der T-Systems
c/o T-Systems GEI GmbH, Rabinstr.8, 53111 Bonn
☎ +49-(0)228-9841-0, FAX -60
💻 www.t-systems-zert.com

Inhaltsverzeichnis

Abkürzungen

AIS	Anwendungshinweise und Interpretationen zum Schema (Verfahren des BSI)
BGBl	Bundesgesetzblatt
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (früher: Regulierungsbehörde für Telekommunikation und Post, RegTP)
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DAR	Deutscher Akkreditierungsrat
DATech	Deutsche Akkreditierungsstelle Technik e.V.
DIN	Deutsches Institut für Normung e.V.
EAL	Evaluation Assurance Level
ETR	Evaluierungsendbericht (Evaluation Technical Report)
ETSI	European Telecommunications Standards Institute
EVG	Evaluationsgegenstand
ISO	International Organization for Standardization
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria (ITSEC)
ITSEF	IT Security Evaluation Facility: Prüflabor
ITSEM	Information Technology Security Evaluation Manual (ITSEM)
JIL	Joint Interpretation Library
PP	Protection Profile
SF	Sicherheitsfunktion
SigG	(deutsches) Signaturgesetz
SigV	(deutsche) Signaturverordnung

SOF	Stärke der Sicherheitsfunktionen (Strength of Security Function)
ST	Sicherheitsvorgaben (Security Target)
TSF	EVG-Sicherheitsfunktionen (TOE Security Functions)
ZDA	Zertifizierungsdiensteanbieter

Referenzen

/AISx/ Anwendungshinweise und Interpretationen zum Schema, Bundesamt für Sicherheit in der Informationstechnik, gültige Fassungen

/ALG/ Geeignete Kryptoalgorithmen, veröffentlicht im Bundesanzeiger durch die Bundesnetzagentur (BNetzA), gültige Fassung

/BS7799/ BS7799-1:2005 Information Technology - Code of Practice for Information Security Management (entspricht ISO/IEC 17799:2005)
BS7799-2:2002 Information Security Management Systems - Specification with Guidance for Use

/CC/ Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model, Version 2.3, August 2005, CCMB-2005-08-001
Common Criteria for Information Technology Security Evaluation – Part 2: Security Functional Requirements, Version 2.3, August 2005, CCMB-2005-08-002
Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, Version 2.3, January 2005, CCMB-2005-08-003

/CEM/ Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

/ETSI/ ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI): Policy requirements for certification authorities issuing qualified certificates, Version 1.3.1, 2005-05

/EU-DIR/ Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

/EU-REF/ Entscheidung der Kommission vom 14. Juli 2003 über die Veröffentlichung von Referenznummern

/ISO27001/ ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems. Requirements

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

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

/JIL/ ITSEC Joint Interpretation Library, Version 2.0, Nov. 1998

/SiGAK/ Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten: Arbeitsgrundlage für Entwickler / Hersteller und Prüf- / Bestätigungsstellen, Bundesnetzagentur, Version 1.4, Stand: 19.07.2005

/SigG/ Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG), zuletzt geändert durch Art. 3 (9) des Zweiten Gesetzes zur Neuregelung des Energiewirtschaftsgesetzes (EnWG) vom 07. Juli 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 42)

/SigV/ Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), zuletzt geändert durch Art. 2 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigGÄndG) vom 04. Januar 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 1)

/SigG-A/ Österreich: 190. Bundesgesetz über elektronische Signaturen, www.a-sit.at/informationen

/SigV-A/ Österreich: 30. Verordnung des Bundeskanzlers über elektronische Signaturen, www.a-sit.at/informationen

/SigG-CH/ Schweiz: Bundesgesetz über die elektronische Signatur, www.sas.ch/de/pki_isms

/SigV-CH/ Schweiz: Verordnung über die elektronische Signatur, www.sas.ch/de/pki_isms

/SigR-CH/ Schweiz: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur, www.sas.ch/de/pki_isms

/Sig-NL1/ Niederlande: Programma van Eisen (PvE), www.pki-overheid.nl

/Sig-NL2/ Niederlande: TTP-NL Guidance on ETSI TS 101.456, ECP.NL, CCvD-TTP.NL, 30.05.2002

Glossar

Das Glossar erläutert Begriffe aus dem Zertifizierungsschema der T-Systems, erhebt allerdings keinerlei Anspruch auf Vollständigkeit oder Allgemeingültigkeit. Der Begriff *Sicherheit* meint hier stets Sicherheit im Kontext der Informationstechnik.

Für kriterienspezifische Begriffe vgl. das Glossar in den jeweiligen Sicherheitskriterien.

Akkreditierung	Von einem Akkreditierungsgeber durchgeführtes Verfahren zum Nachweis, dass eine Prüfstelle [bzw. Zertifizierungsstelle] den Anforderungen der maßgebenden Norm ISO 17025 [bzw. DIN EN 45011] entspricht.
Audit	Verfahren des Sammelns objektiver Nachweise dafür, dass ein Prozess so abläuft wie vorgegeben.
Bestätigungsstelle	Stelle, die mit Anerkennung durch die Bundesnetzagentur Sicherheitsbestätigungen gemäß SigG und SigV für technische Komponenten und Zertifizierungsdiensteanbieter herausgibt.
Bestätigungsverfahren	Verfahren mit dem Ziel einer Sicherheitsbestätigung.
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 (ISO/IEC 15408) sind.
Dienstleistung	Hier: Eine von einem Unternehmen angebotene, durch Geschäftsprozesse erbrachte und durch Nutzer in Anspruch nehmbare Leistung.
Evaluation Technical Report	Schlussbericht einer Prüfstelle über den Ablauf und die Ergebnisse einer Evaluation.
Evaluationsgegenstand	Ein IT-Produkt oder IT-System, das in Verbindung mit seinen (Administrations- und Benutzer-) Handbüchern Gegenstand einer Evaluierung ist.
Evaluationsstufe	Stufe der Vertrauenswürdigkeit, die aus einer Evaluierung gewonnen wird: Höhe des Vertrauens, dass der EVG seine Sicherheitsvorgaben erfüllt (gemäß ITSEC / CC).
Evaluator	Prüfer/in in einer Prüfstelle.
Evaluierung	Prüfung eines IT-Produktes, IT-Systems oder einer IT-Dienstleistung auf der Basis von IT-Sicherheitskriterien.

Integrität	Klassisches Sicherheitsziel: Daten sollen nur von Befugten geändert werden können.
IT-Dienstleistung	Dienstleistung, die sich bei ihrer Erbringung auf IT-Systeme abstützt.
IT-Produkt	Software und / oder Hardware, die bei einem Anbieter (Hersteller, Vertreiber) erworben werden kann.
IT-Sicherheits-management	Ein Unternehmensprozess, dessen Ziel die Einrichtung und Aufrechterhaltung der (IT-)Sicherheit in einem Unternehmen ist.
IT-System	Eine in sich funktionsfähige Kombination von IT-Produkten. (ITSEC:) Eine reale Installation von IT-Produkten mit einer bekannten Einsatzumgebung.
Lizenzvereinbarung	Vereinbarung zwischen einer Prüfstelle und einer Zertifizierungsstelle - den Ablauf und die Verantwortlichkeiten bei einer Prüfung / 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, z.B. die Interpretation der Sicherheitskriterien betreffend.
Produkt-Zertifizierung	Zertifizierung von IT-Produkten.
Prozess	Abfolge vernetzter Tätigkeiten (Prozesselemente) in einer gegebenen Prozessumgebung – mit dem Gesamtziel, eine bestimmte Dienstleistung zu erbringen.
Prüfbegleitung	Verfahren der Zertifizierungsstelle, um die Ordnungsmäßigkeit (Kriterienkonformität, einheitliche Vorgehensweise und Bewertungen, etc.) einer Evaluierung zu überprüfen.
Prüfstelle	Stelle, die Evaluierungen durchführt (ITSEF).
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.
Security for Business	Programm der T-Systems mit Service-Bausteinen für die IT-Sicherheit in Unternehmen. Die Bausteine beinhalten Beratung, Schulung, Analysen, Penetrationstests, Audits sowie Verfahren der Registrierung, Siegelvergabe und Zertifizierung.
Sicherheitsbestätigung	SigG: Eine Bescheinigung, die die Erfüllung von Anforderungen des Signaturgesetzes bestätigt.
Sicherheitsfunktion	Technische Funktion bzw. Maßnahme zur Abwehr bestimmter Bedrohungen.

Sicherheitskriterien	Dokument mit Sicherheitsanforderungen an Produkte, Systeme und / oder Dienstleistungen und / oder deren Evaluierung.
Sicherheitsvorgaben	Dokument, das einen EVG spezifiziert, indem es u.a. seine Konfiguration und Einsatzumgebung, Sicherheitsziele und Bedrohungen, seine Sicherheitsfunktionen, erfüllte Sicherheitsanforderungen und entsprechende Begründungen enthält; dient als Basisdokument einer Evaluierung des EVG.
Sicherheitszertifikat	s. Zertifikat
System-Zertifizierung	Zertifizierung installierter IT-Systeme.
Trust Center	s. Zertifizierungsdiensteanbieter
Unternehmensprozess	s. Prozess
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.
Vertraulichkeit	Klassisches Sicherheitsziel: Daten sollen nur durch Befugte zur Kenntnis genommen werden können.
Zertifikat	Zusammenfassende (Kurz-)Darstellung eines Zertifizierungsergebnisses; wird durch die Zertifizierungsstelle ausgestellt.
Zertifizierer	Mitarbeiter/in einer Zertifizierungsstelle, der / die Zertifizierungen durchführt.
Zertifizierung	Unabhängige Bestätigung der Ordnungsmäßigkeit einer Evaluierung. Auch Bezeichnung für das Gesamtverfahren bestehend aus Evaluierung, Prüfbegleitung und Ausstellung von Zertifikaten und Zertifizierungsreports.
Zertifizierungsdiensteanbieter	Stelle, die die Zugehörigkeit von Signaturschlüsseln zu einer Person durch ein (elektronisches) Zertifikat bestätigt - im Signaturgesetz als „Zertifizierungsdiensteanbieter“ (ZDA) bezeichnet.
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.)

Erläuterungen zu den Sicherheitskriterien

Dieses Kapitel gibt einen Überblick über die angewendeten Sicherheitskriterien und deren Bewertungsmaßstäbe.

Sicherheitsziele für einen Evaluationsgegenstand (EVG) setzen sich in der Regel aus Forderungen nach Vertraulichkeit, Verfügbarkeit und / oder Integrität von bestimmten Datenobjekten zusammen. Solche Sicherheitsziele werden durch den Auftraggeber der Evaluierung festgelegt. Normalerweise ist dies bei einem IT-Produkt der Entwickler oder Vertreiber, bei einem IT-System der Betreiber.

Den festgelegten Sicherheitszielen stehen Bedrohungen gegenüber. Aus solchen Bedrohungen werden Angriffe, wenn Subjekte unerlaubt Datenobjekte mitlesen oder abhören, Dritten vorenthalten oder unbefugt ändern. In dem betrachteten EVG sollen (EVG-) Sicherheitsfunktionen solche Angriffe abwehren.

In den CC Teil 2 sind Anforderungen an solche Sicherheitsfunktionen in Form von "functional components" beschrieben. Die Angabe "CC Teil 2 konform" in Zertifizierungsreports meint, dass nur functional components aus den CC Teil 2 zur Beschreibung solcher Anforderungen verwendet wurden. Die Angabe "CC Teil 2 erweitert" meint, dass auch functional components verwendet wurden, die nicht aus den CC Teil 2 stammen.

Selbst dann, wenn eine EVG-Sicherheitsfunktion nicht umgangen, deaktiviert oder verfälscht werden kann, besteht dennoch die Möglichkeit, diese außer Kraft zu setzen, weil es im Konzept des ihr zugrundeliegenden Sicherheitsmechanismus eine Schwachstelle gibt. Das Sicherheitsverhalten dieser Funktionen kann mittels der Ergebnisse einer quantitativen oder statistischen Analyse des Sicherheitsverhaltens dieser Mechanismen und des zu deren Überwindung erforderlichen Aufwands charakterisiert werden. Diese Charakterisierung erfolgt in Form eines Postulats der Stärke der EVG-Sicherheitsfunktion.

Die Stärke einer Sicherheitsfunktion (SOF, Strength of Function) beschreibt den geringsten angenommenen Aufwand, der notwendig ist, um deren erwartetes Sicherheitsverhalten durch einen direkten Angriff auf die zugrundeliegenden Sicherheitsmechanismen außer Kraft zu setzen. Folgende SOF-Stufen sind in den Common Criteria (CC) festgelegt:

SOF-Niedrig: Eine Stufe der 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 Stärke von Funktionen, bei der die Analyse zeigt, daß die Funktionen einen angemessenen Schutz gegen naheliegendes oder absichtliches Bre-

chen der EVG-Sicherheit durch Angreifer bieten, die über ein mittleres Angriffspotential verfügen.

SOF-Hoch: Eine Stufe der 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.

Die Vertrauenswürdigkeit eines EVG ist nach dem Verständnis der CC dann gegeben, wenn ausreichendes Vertrauen darin besteht, dass die betrachteten Sicherheitsziele erfüllt werden. Die CC-Philosophie sagt aus, dass höhere Vertrauenswürdigkeit das Ergebnis eines höheren Evaluationsaufwandes ist, und dass das Ziel darin besteht, den geringstmöglichen Aufwand zu betreiben, der zur Erzielung des erforderlichen Grads der Vertrauenswürdigkeit notwendig ist. Der zunehmende Grad des Aufwands basiert auf

- dem Anwendungsbereich - d.h. der Aufwand ist größer, weil er einen größeren Anteil des IT-Produktes oder –Systems umfasst;

- der Testtiefe - d.h. der Aufwand ist größer, da er auf eine größere Stufe der Feinheit der Entwurfs- und Implementierungsdetails ausgelegt ist;

- der Schärfe - d.h. der Aufwand ist größer, da er auf eine stärker strukturierte, formalere Art erfolgt.

Die Tabelle gibt einen Überblick über die in den CC Teil 3 definierten Vertrauenswürdigkeitsklassen und –familien (Assurance Class / Family) sowie die abgekürzten Namen, die in Zertifizierungsreports and Zertifikaten verwendet werden.

Assurance Class	**Assurance Family**	**Abbreviated Name**
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

Assurance Class	Assurance Family	Abbreviated Name
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

Die Vertrauenswürdigkeitsfamilien sind weiter unterteilt in Vertrauenswürdigkeitskomponenten. Aus den zahlreichen Vertrauenswürdigkeitskomponenten in CC Teil 3, in denen Anforderungen an den Entwickler und den Evaluator festgelegt sind, sind insgesamt sieben Evaluationsstufen (EAL, Evaluation Assurance Level) entwickelt worden. EAL1 bezeichnet die niedrigste, EAL7 die höchste Stufe. Die Vertrauenswürdigkeit eines EVG kann somit in diesen Stufen gemessen werden. Nicht alle Vertrauenswürdigkeitskomponenten aus CC Teil 3 sind für die EAL-Stufen verwendet worden.

Die Beschreibungen charakterisieren die einzelnen EAL-Stufen.

EAL1 funktionell getestet

EAL1 ist anwendbar, wenn ein gewisses Maß an Vertrauen in einen korrekten Betrieb erforderlich ist, die Bedrohungen der Sicherheit aber nicht als ernst angesehen werden. Sie wird dort von Bedeutung sein, wo unabhängige Vertrauenswürdigkeit benötigt wird, um die Behauptung zu unterstützen, daß dem Schutz persönlicher oder vergleichbarer Informationen angemessene Aufmerksamkeit gewidmet wurde.

EAL1 stellt eine Prüfung und Bewertung des EVG, wie er an Kunden ausgeliefert wird, bereit, einschließlich unabhängigen Testens anhand einer Spezifikation und einer Überprüfung der Handbücher. Es ist beabsichtigt, daß eine EAL1-Evaluation ohne Hilfestellung durch den Entwickler des EVG erfolgreich und mit minimalen Ausgaben ausgeführt werden kann.

Eine Prüfung und Bewertung auf dieser Stufe soll nachweisen, daß der EVG in einer mit seiner Dokumentation konsistenten Weise funktioniert, und daß er einen nützlichen Schutz gegen identifizierte Bedrohungen bietet.

EAL2 strukturell getestet

EAL2 erfordert die Kooperation des Entwicklers hinsichtlich der Lieferung von Entwurfsinformationen und Testergebnissen. Dabei sollte aber der dem Entwickler abgeforderte Arbeitsaufwand das in gut geführten Betrieben übliche Maß nicht überschreiten. Das heißt, sie soll keine erheblichen finanziellen oder zeitlichen Zusatzinvestitionen erfordern.

EAL2 ist daher in den Fällen anwendbar, in denen Entwickler oder Benutzer eine niedrige bis mittlere Stufe an unabhängig geprüfter Sicherheit benötigen und die vollständigen Entwicklungsaufzeichnungen nicht verfügbar sind. Eine solche Situation kann bei der Prüfung der Sicherheit von Altanwendungen entstehen oder dann, wenn der Entwickler nur eingeschränkt zur Verfügung steht.

EAL3 methodisch getestet und überprüft

EAL3 erlaubt einem gewissenhaften Entwickler, durch positive technische Sicherheitsmaßnahmen auf der Entwicklungsstufe maximale Vertrauenswürdigkeit zu erzielen, ohne die bestehenden, stimmigen Entwicklungspraktiken wesentlich zu verändern.

EAL3 ist dann anwendbar, wenn Entwickler oder Benutzer eine mittlere Stufe an unabhängig geprüfter Sicherheit sowie eine gründliche Untersuchung des EVG und dessen Entwicklung ohne wesentliche technische Änderungen an diesem erfordern.

EAL4 methodisch entwickelt, getestet und durchgesehen

EAL4 erlaubt einem Entwickler, durch positive technische Sicherheitsmaßnahmen maximale Vertrauenswürdigkeit zu erzielen, basierend auf bewährten betrieblichen Entwicklungspraktiken, die zwar scharf sind, aber keine tiefgehenden Spezialkenntnisse, Fähigkeiten oder andere Betriebsmittel erfordern. EAL4 ist die höchste Stufe, bei der eine Nachrüstung einer Produktreihe wahrscheinlich noch wirtschaftlich durchführbar ist.

EAL4 ist daher in den Fällen anwendbar, in denen Entwickler oder Benutzer eine mittlere oder hohe Stufe unabhängig geprüfter Sicherheit für konventionelle, marktübliche EVG fordern und bereit sind, zusätzliche sicherheitsspezifische Entwicklungskosten zu tragen.

EAL5 semiformal entworfen und getestet

EAL5 erlaubt einem Entwickler, maximale Vertrauenswürdigkeit durch technische Sicherheitsmaßnahmen zu erzielen, basierend auf scharfen betrieblichen Entwicklungspraktiken, die durch begrenzten Einsatz von Sicherheits-Spezialtechniken zur Entwicklung unterstützt werden. Ein solcher EVG ist wahrscheinlich mit der Absicht

entworfen und entwickelt, die Vertrauenswürdigkeit der Stufe EAL5 zu erreichen. Es ist wahrscheinlich, daß die durch die EAL5-Anforderungen verursachten zusätzlichen Kosten, bezogen auf eine strikte Entwicklung ohne Anwendung von Spezialpraktiken, nicht erheblich sind.

EAL5 ist daher in den Fällen anwendbar, in denen Entwickler oder Benutzer für eine geplante Entwicklung einen hohen Stufe unabhängig geprüfter Sicherheit und eine scharfe Herangehensweise an die Entwicklung benötigen, ohne daß übermäßige auf Spezialtechniken zur Sicherheitsentwicklung zurückzuführende Zusatzkosten entstehen.

EAL6 semiformal verifizierter Entwurf und getestet

EAL6 erlaubt den Entwicklern, durch Anwendung von Techniken zur Sicherheitsentwicklung in einer streng kontrollierten Entwicklungsumgebung eine hohe Vertrauenswürdigkeit zu erzielen, um einen erstklassigen EVG zum Schutz hoher Werte gegen signifikante Risiken zu entwickeln.

EAL6 ist daher anwendbar für die Entwicklung von Sicherheits-EVG zum Gebrauch in Situationen mit hohem Risiko, in denen die große Bedeutung der geschützten Werte die Zusatzkosten rechtfertigt.

EAL7 formal verifizierter Entwurf und getestet

EAL7 ist anwendbar für die Entwicklung von Sicherheits-EVG zur Anwendung in Situationen mit extrem hohem Risiko und/oder in Fällen, in denen die große Bedeutung der Werte die höheren Kosten rechtfertigt. Der praktische Einsatz von EAL7 ist gegenwärtig auf EVG mit hochkonzentrierter Sicherheitsfunktionalität begrenzt, die sich für umfangreiche formale Analysen eignet.

Der folgende Tabelle aus CC Teil 3 ist zu entnehmen, aus welchen Vertrauenswürdigkeitskomponenten sich die einzelnen EAL-Stufen zusammensetzen. Die Ziffern geben die Komponentennummer innerhalb einer Familie an.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	**EAL2**	**EAL3**	**EAL4**	**EAL5**	**EAL6**	**EAL7**
ACM: Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ADO: Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
ADV: 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
AGD: Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
ALC: Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
ATE: 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**
AVA: 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

Ein höherer Grad der Vertrauenswürdigkeit, als sie von einem EAL bereitgestellt wird, kann erreicht werden durch

- Einbeziehen zusätzlicher Vertrauenswürdigkeitskomponenten (z.B. von anderen Vertrauenswürdigkeitsfamilien); oder

- Ersetzen einer Vertrauenswürdigkeitskomponente durch eine Vertrauenswürdigkeitskomponente höherer Stufe aus der gleichen Vertrauenswürdigkeitsfamilie.

Für einen speziellen EVG sind solche Erweiterungen oder Änderungen dem jeweiligen Zertifizierungsreport zu entnehmen: Die Angabe "CC Teil 3 konform" meint, dass nur Vertrauenswürdigkeitskomponenten aus den CC Teil 3 verwendet wurden. Die Angabe "CC Teil 3 erweitert" meint, dass auch Vertrauenswürdigkeitskomponenten verwendet wurden, die nicht aus den CC Teil 3 stammen.

1 Antragsteller und Evaluationsgegenstand

[1] Antragsteller der Zertifizierung ist die Siemens AG, Charles-de-Gaulle-Str. 2, 81737 München.

[2] Beantragt wurde ein Zertifikat gemäß dem Verfahren 04: „Deutsches IT-Sicherheitszertifikat“ der Zertifizierungsstelle der T-Systems.

[3] Evaluationsgegenstand (EVG) ist das Produkt „CardOS V4.3B Re_Cert with Application for Digital Signature“, im Folgenden kurz bezeichnet als: CardOS V4.3B Re_Cert.

[4] Der EVG ist eine SSEE ("Sichere Signaturerstellungseinheit").

[5] Seitens des Antragstellers sind Sicherheitsvorgaben für den EVG in englischer Sprache bereitgestellt worden. Die Sicherheitsvorgaben, letzte Version 1.0 vom 28.11.2006, sind als separates Dokument erhältlich.

[6] Die Sicherheitsvorgaben referenzieren als Prüfkriterien die Common Criteria und als Evaluationsstufe EAL4, für die Mindeststärke der EVG-Sicherheitsfunktionen (SOF) wird „SOF-hoch“ angegeben.

2 Maßgebende Prüfgrundlagen[1]

[7] Die Evaluierung des EVG erfolgte antragsgemäß gegen die

- Common Criteria: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (ISO/IEC 15408) /CC/.

[8] Für die Evaluierung und Zertifizierung waren weiterhin folgende Dokumente maßgebend:

- Common Methodology for Information Technology Security Evaluation /CEM/,
- Anwendungshinweise und Interpretationen zum Schema, Bundesamt für Sicherheit in der Informationstechnik /AIS/,
- Arbeitsanweisung „Verfahrenstyp 04: Deutsches IT-Sicherheitszertifikat“ der T-Systems GEI GmbH (gültige Fassung).

[1] Die genauen bibliografischen Angaben zu den Prüfgrundlagen finden sich im Abschnitt "Referenzen" in diesem Zertifizierungsreport.

3 Evaluierung

[9] Die Evaluierung des EVG wurde durch die Siemens AG bei der Prüfstelle für IT-Sicherheit der T-Systems GEI GmbH beauftragt.

[10] Die Prüfstelle ist nach ISO 17025 akkreditiert und besitzt eine gültige Lizenz des BSI und der Zertifizierungsstelle für das hier vorliegende Prüfgebiet.

[11] Die Evaluierung erfolgte im Zertifizierungsschema der T-Systems.

[12] Das Ergebnis der Evaluierung ist im Evaluation Technical Report (ETR) der Prüfstelle dargestellt. Der ETR trägt die Versionsnummer 1.00 und das Datum 29.11.2006.

[13] Die Evaluierung des EVG wurde am 30.11.2006 beendet.

4 Zertifizierung

[14] Das Zertifizierungsschema der T-Systems ist auf den entsprechenden Web-Seiten der Zertifizierungsstelle veröffentlicht (www.t-systems-zert.com).

[15] Die Zertifizierungsstelle der T-Systems arbeitet im Einklang mit der DIN EN 45011 und ist im Hinblick auf diese Norm bei der DATech GmbH für Prüfungen nach den ITSEC und den Common Criteria akkreditiert (DAR-Registriernummer DAT-ZE-015/98-01).

[16] Dem Zertifizierungsverfahren wurde die Registriernummer T-Systems-DSZ-CC-04181-2006 zugewiesen.

[17] Die Evaluierung bei der Prüfstelle für IT-Sicherheit der T-Systems GEI GmbH wurde durch die Zertifizierungsstelle kriteriengemäß begleitet.

[18] Die Zertifizierung des EVG erfolgt wie beantragt gemäß Verfahrenstyp 04: „Deutsches IT-Sicherheitszertifikat“.

[19] Die Zertifizierung des EVG kann die Erfüllung von Auflagen und die Beachtung von weitere Hinweisen voraussetzen. Näheres enthält der Abschnitt 6.

[20] Eine Kurzfassung der Ergebnisse enthält das Sicherheitszertifikat T-Systems-DSZ-CC-04181-2006 vom 30.11.2006 auf der Seite 2 dieses Reports.

[21] Die Tatsache der Zertifizierung wird auf den Web-Seiten (www.t-systems-zert.com) der Zertifizierungsstelle bekannt gegeben.

[22] Dieser Zertifizierungsreport wird auf den Web-Seiten (www.t-systems-zert.com) der Zertifizierungsstelle zum Download bereitgestellt.

5 Nationale und internationale Akzeptanz

[23] Das Zertifikat T-Systems-DSZ-CC-04181-2006 trägt als "Deutsches IT-Sicherheitszertifikat" das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) genehmigte Logo.

[24] Die Tatsache der Zertifizierung wird in den Broschüren BSI 7148 / 7149 des BSI referenziert.

[25] Das Zertifikat wird vom BSI als gleichwertig zu seinen eigenen Zertifikaten anerkannt.

[26] Das BSI bestätigt vertragsgemäß diese Gleichwertigkeit explizit im internationalen Kontext.

[27] Eine weitergehende internationale Akzeptanz der Zertifizierungsergebnisse wird aufgrund des Multilateralen Abkommens von EA, ILAC und IAF zur gegenseitigen Anerkennung erreicht, das von der Akkreditierungsstelle DATech GmbH unterzeichnet worden ist (vgl. www.datech.de für Details).

6 Zusammenfassung der Ergebnisse

[28] Die Auslieferung des Produkts erfolgt entsprechend den Angaben des Antragstellers nach folgendem Verfahren:

Die verschiedenen Stufen und Wege der Auslieferung des EVG und die Abläufe der Initialisierung und Personalisierung sind im Dokument "Delivery and Operation, CardOS V4.3B Re_Cert, Version 0.2, 26.10.2006 (Siemens AG)" in englischer Sprache detailliert beschrieben. Die Darstellung umfasst folgende Abschnitte: Delivery to the Chip Manufacturer, Delivery to the Trust Center, Procedure of Initialisation and Personalisation, Delivery of the signature card to the Card Holder by the Trust Center, Delivery of pre-personalised signature card to the Registration Authority by the Trust Center, Delivery to the Terminal Developer, Delivery of signature card to the Card Holder by the Registration Authority.

Die beschriebenen Auslieferungsverfahren entsprechen den Vorgaben der nationalen Zertifizierungsbehörde für die Stufe EAL4 der Common Criteria.

29 Evaluiert wurden die folgenden Konfigurationen des EVG:

1. Konfiguration 'n=1': Diese Standard-Konfiguration fordert den Nutzer zur PIN-Eingabe auf, um anschließend genau eine Signatur zu erzeugen, d. h. eine erfolgreiche Authentisierung ermöglicht die Erzeugung genau einer Signatur.

2. Konfiguration 'n>1': Diese besondere Konfiguration ermöglicht die Erzeugung von entweder n Signaturen oder von so vielen, wie die SCA (signature creation application) erlaubt. Eine beabsichtigte Begrenzung muss durch die Applikation (z. B. durch ein Zeitfenster oder einen Signaturzähler) überwacht werden. Diese Konfiguration 'n>1' darf ausschließlich in einer Umgebung (z. B. in einem Büro, einem Trust Center oder einer Registrierungsstelle) angewendet werden, die im Rahmen einer geeigneten externen Sicherheitspolitik betrieben wird, welche vom Kartenherausgeber als vertrauenswürdig angesehen wird. Diese Einsatzumgebung des EVG muss jede unbeabsichtigte und jede missbräuchliche Verwendung des EVG ausschließen.

Das Evaluierungsergebnis gilt nur für diese Konfiguration(en) des EVG.

30 Entsprechend den Sicherheitsvorgaben und dem Ergebnis der Evaluierung besitzt der EVG folgende Sicherheitsfunktionen (vgl. die Sicherheitsvorgaben für Details):

- SF1 User Identification and Authentication
- SF2 Access Control
- SF3 SCD/SVD Pair Generation
- SF4 Signature Creation
- SF5 Protection

31 Hinsichtlich der Stärke der Sicherheitsfunktionen lautet das Ergebnis (vgl. Sicherheitsvorgaben für Details):

Die Sicherheitsfunktionen SF1, SF3, SF4 des EVG besitzen die Mindest-Stärke: SOF-hoch.

32 Die Evaluierung hat ergeben:

Die Sicherheitsvorgaben erfüllen die Anforderungen der entsprechenden Klasse ASE (Security Target Evaluation) der Common Criteria.

Die funktionalen Anforderung sind CC Teil 2 erweitert.

Die Anforderungen an die Vertrauenswürdigkeit sind CC Teil 3 konform.

Der EVG genügt den Anforderungen der Evaluationsstufe EAL4 der Common Criteria. Die zu dieser Stufe gehörenden Vertrauenswürdigkeitskomponenten können den Erläuterungen zu den Kriterien in diesem Report (ab Seite 11) entnommen werden.

Die folgenden Vertrauenswürdigkeitskomponenten wurden hinzugefügt:

AVA_MSU.3 Vulnerability Assessment:
Analysis and testing for insecure states

AVA_VLA.4 Vulnerability Assessment:
Highly resistant

[33] Folgende zusätzlichen Hinweise sind für den sicherheitsgerechten Einsatz des EVG zu beachten:

1. Die Dokumentation bestehend aus "Administrator Guidance, CardOS V4.3B Re_Cert, Version 1.2, Siemens AG, 27.11.2006" und "User Guidance, CardOS V4.3B Re_Cert, Version 1.2, Siemens AG, 21.11.2006" beinhaltet alle notwendigen Informationen über den sicheren Gebrauch des EVG.

2. Der Zertifizierungsdienstanbieter (Trust Center) – in seiner Rolle als Kartenausgeber – muss sicherstellen, dass die Anzahl der im Gebrauch befindlichen EVG (Smartcards) 83 Millionen nicht überschreitet.

3. Die EVG-Konfiguration 'n>1' darf nur angewendet werden, wenn die entsprechenden EVG für die Nutzung im Rahmen einer geeigneten externen Sicherheitspolitik personalisiert werden. Die Erfüllung dieser Bedingung liegt in der Verantwortung des den EVG ausgebenden Trust Centers.

[34] Für die Gültigkeit des Zertifikats sind durch den Antragsteller folgende Auflagen zu erfüllen:

1. Der Software-Entwickler (Siemens AG) und der Chip-Hersteller (Infineon Technologies AG) sind verantwortlich dafür, die missbräuchliche Nutzung des PackageLoadKey zu verhindern; insbesondere ist seine Vertraulichkeit sicherzustellen.

2. Die Anzahl der im Gebrauch befindlichen EVGs (d. h. Smartcards) darf 83 Millionen nicht überschreiten.

Ende des Zertifizierungsreports zu T-Systems-DSZ-CC-04181-2006.

Zertifizierungsreport:
T-Systems-DSZ-CC-04181-2006

Hrsg.:	T-Systems GEI GmbH
Adresse:	Rabinstr.8, 53111 Bonn
Telefon:	+49-(0)228-9841-0
Fax:	+49-(0)228-9841-60
Web:	www.t-systems-itc.de
	www.t-systems-zert.com