T · · Systems · · ·

Zertifizierungsreport

T-Systems-DSZ-ITSEC-04090-2003

ArtSignComponent V1.0

Deutsche Post Signtrust GmbH

Zertifizierungsreport T-Systems-DSZ-ITSEC-04090-2003

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

✉ Zertifizierungsstelle der T-Systems
c/o T-Systems GEI GmbH
BU ITC Security
Rabinstr.8, 53111 Bonn

☎ 0228/9841-0, Fax: 0228/9841-60

💻 www.t-systems-zert.com

Deutsches IT-Sicherheitszertifikat

anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

T · · Systems · · ·

Die Zertifizierungsstelle der T-Systems

bestätigt hiermit, daß

ArtSignComponent V1.0

der

Deutsche Post Signtrust GmbH
Tulpenfeld 9, 53113 Bonn

nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) und dem Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) gegen spezifische Sicherheitsvorgaben evaluiert wurde und folgendes Prüfergebnis erzielte:

Sicherheitsfunktionen:	**Funktionsbibliothek: Unterstützung der Signaturerstellung, Wiederaufbereitung, Verifikation einer digitalen Signatur**
Vertrauenswürdigkeitsstufe:	**E2**
Mindeststärke der Sicherheitsmechanismen:	**hoch**

Dieses Zertifikat erfüllt die Bedingungen der Vereinbarung über die gegenseitige Anerkennung von Sicherheitszertifikaten in der Informationstechnik (SOGIS-MRA) vom 03.03.1998 zwischen Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien.
Dieses Zertifikat gilt nur in Verbindung mit dem vollständigen Zertifizierungsreport zur unten angegebenen Registriernummer und für die darin aufgeführten Konfigurationen und Einsatzumgebungen. Die Empfehlungen und Hinweise im Zertifizierungsreport sind zu beachten. Die Sicherheitsvorgaben, die Basis der Evaluierung waren, sind im Zertifizierungsreport aufgeführt. Kopien des Zertifikats und des Zertifizierungsreports sind beim Auftraggeber und bei der Zertifizierungsstelle erhältlich.

Registrierungsnummer:
T-Systems-
DSZ-ITSEC-04090-2003

Bonn, den 31.10.2003

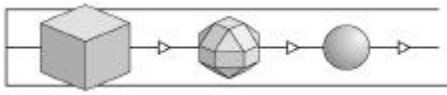
T · · Systems · · ·

Dr. Heinrich Kersten
Leiter der Zertifizierungsstelle

Zertifizierungsstelle der T-Systems
c/o T-Systems GEI GmbH, BU ITC Security, Rabinstr.8, 53111 Bonn
☎ 0228/9841-0, Fax: 0228/9841-60, Internet: www.t-systems-zert.com
Akkreditiert nach DIN EN 45011 unter DAR-Registriernummer DIT-ZE-005/98 durch DATech e.V.

(Diese Seite ist beabsichtigterweise leer.)

Inhaltsverzeichnis



Abkürzungen

AIS	Anwendungshinweise und Interpretationen zum Schema (Verfahren des BSI)
BGBl	Bundesgesetzblatt
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.
ETR	Evaluation Technical Report (Evaluierungsbericht)
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
RegTP	Regulierungsbehörde für Telekommunikation und Post
SigG	Signaturgesetz
SigV	Signaturverordnung

Referenzen

/AIS/ Anwendungshinweise und Interpretationen zum Schema, Bundesamt für Sicherheit in der Informationstechnik, gültige Fassung

/ALG/ Geeignete Kryptoalgorithmen, veröffentlicht im Bundesanzeiger durch die Regulierungsbehörde für Telekommunikation und Post, gültige Fassung

/BS7799/ BS7799-1:2000 Information technology - Code of practice for information security management (ISO/IEC 17799:2000)
BS7799-2:2002 Information security management systems - Specification with guidance for use

/CC/ Common Criteria: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (ISO 15408), August 1999
Teil1: Einführung und allgemeines Modell
Teil2: Funktionale Sicherheitsanforderungen
Teil3: Anforderungen an die Vertrauenswürdigkeit

/CEM/ Common Methodology for Information Technology Security Evaluation, Part1: Introduction and general model, Version 0.6, January 1997
Part2: Evaluation Methodology, Version 1.0, August 1999

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

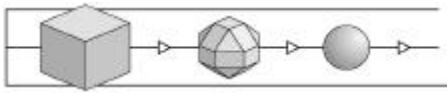
/ITSEC/ Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Version 1.2 (1991), Bundesanzeiger-Verlag Köln, ISBN 92-826-3003-X

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

/SigG/ Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I, S. 876 ff.)

/SigV/ Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I., S. 3074 ff.)

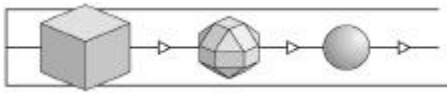


Glossar

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.

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 Regulierungsbehörde für Telekommunikation und Post und im Einklang mit SigG und SigV Sicherheitsbestätigungen für technische Komponenten und für die Umsetzung von Sicherheitskonzepten bei Trust Centern (Zertifizierungsdiensteanbietern nach SigG) 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 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; Element eines Bewertungssystems in Sicherheitskriterien ITSEC / CC; Höhe des Vertrauens, dass der EVG seine Sicherheitsvorgaben erfüllt.
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 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	Sicherheitsinitiative, die Service-Bausteine (Basissicherheit, Standardsicherheit, Professionelle Sicherheit) in puncto IT-Sicherheit für Unternehmen anbietet. Die Bausteine beinhalten Beratung, Analysen, Penetrationstests, Audits sowie nach erfolgreicher Abnahme Verfahren der Registrierung, Siegelvergabe und Zertifizierung. Details sind den Web-Seiten der Initiative zu entnehmen. (www.s4b.org)
Sicherheitsbestätigung	SigG: Eine Bescheinigung, die die Erfüllung von Anforderungen des Signaturgesetzes bestätigt.
Sicherheitsfunktion	Funktionen zur Abwehr bestimmter Bedrohungen.



Sicherheitskriterien	Dokument mit Sicherheitsanforderungen an Produkte, Systeme und / oder Dienstleistungen und / oder deren Evaluierung.
Sicherheitsvorgaben	Dokument, das einen Satz von Sicherheitsanforderungen and Spezifikationen enthält, die als Basis einer Evaluierung eines speziellen EVG dienen.
Sicherheitszertifikat	s. Zertifikat
System-Zertifizierung	Zertifizierung von installierten IT-Systemen.
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, die eine Zertifizierung durchführt.
Zertifizierung	Unabhängige Bestätigung der Ordnungsmäßigkeit einer Evaluierung. Auch Bezeichnung für das Gesamtverfahren bestehend aus Evaluierung, Prüfbegleitung und Ausstellung von Zertifikaten und Zertifizierungsreports.
Zertifizierungsdiensteanbieter	Stelle, die die Zugehörigkeit von Signaturschlüsseln zu einer Person durch ein (elektronisches) Zertifikat bestätigt - im Signaturgesetz als „Zertifizierungsdiensteanbieter“ 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.

Erläuterungen zu den Sicherheitskriterien

Dieses Kapitel gibt einen Überblick über die angewendeten Sicherheitskriterien und deren Bewertungsmaßstäbe. Textpassagen innerhalb „...“ stellen Zitate aus den ITSEC bzw. den ITSEM dar.

- Grundbegriffe

Sicherheit ist nach dem Verständnis der ITSEC dann gegeben, wenn ausreichendes Vertrauen darin besteht, dass der Evaluationsgegenstand (EVG) seine *Sicherheitsziele* erfüllt.

Sicherheitsziele 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 prinzipielle *Bedrohungen* gegenüber, nämlich der Verlust der Vertraulichkeit, der Verlust der Verfügbarkeit, der Verlust der Integrität bestimmter Datenobjekte.

Aus solchen prinzipiellen Bedrohungen werden *Angriffe*, wenn Subjekte unerlaubt Datenobjekte mitlesen oder abhören, Dritten vorenthalten oder unbefugt ändern.

Sicherheitsfunktionen des EVG sollen solche *Angriffe* abwehren.

Es stellen sich dabei zwei Grundfragen: Funktionieren die Sicherheitsfunktionen korrekt? Sind die Sicherheitsfunktionen wirksam?

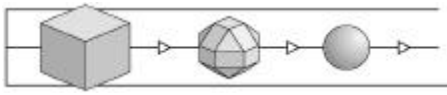
Vertrauen in die Erfüllung der Sicherheitsziele kann man dann haben, wenn *Korrektheit* und *Wirksamkeit* geprüft (*evaluiert*) worden sind.

- Evaluationsstufen

Eine Evaluierung kann nur mit begrenztem Aufwand und in begrenzter Zeit durchgeführt werden. Die mögliche Tiefe einer Evaluierung ist also stets begrenzt. Das Angemessenheitsprinzip verbietet es andererseits, bei geringem Sicherheitsbedarf eine extrem aufwändige Prüfung durchzuführen; ebenso unangemessen wäre es, bei höchstem Sicherheitsbedarf nur „oberflächlich“ zu prüfen.

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

Die Vertrauenswürdigkeit eines EVG kann also in diesen Stufen „gemessen“ werden.



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

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

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

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

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

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

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

In allen E-Stufen müssen darüber hinaus Wirksamkeitsaspekte nach folgendem Schema untersucht werden:

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

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

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

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

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

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

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

- Sicherheitsfunktionen und Sicherheitsmechanismen

Sicherheitsfunktionen in einem EVG dienen der Abwehr von Bedrohungen.

Solche Sicherheitsfunktionen können in einer typischen Kombination („Funktionalitätsklasse“) vorkommen. Beispiel: Die Funktionalitätsklasse F-C2 setzt sich aus den Funktionen *Identifikation und Authentisierung*, *Zugriffskontrolle*, *Beweissicherung*, *Protokollauswertung* und *Wiederaufbereitung* zusammen. Diese Klasse ist bei vielen kommerziellen Betriebssystemen gegeben.

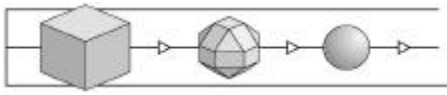
Jede Sicherheitsfunktion kann auf unterschiedlichste Weise realisiert werden. Beispiel: Die Funktion *Identifikation und Authentisierung* kann unter anderem durch ein Paßwort-Verfahren, durch Verwendung von Chipkarten mit Challenge-Response Verfahren oder durch biometrische Verfahren realisiert sein. Jede Realisierung dieser Art heißt *(Sicherheits-)Mechanismus* der Sicherheitsfunktion *Identifikation und Authentisierung*. Für andere Sicherheitsfunktionen gilt sinngemäß das gleiche.

Die Widerstandskraft eines Sicherheitsmechanismus gegenüber direkten Angriffen wird als *Stärke* des Mechanismus bezeichnet.

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

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

Typ A „Ein Mechanismus vom Typ A ist ein Sicherheitsmechanismus mit einer potentiellen Schwachstelle in seinem Algorithmus, seinen Prinzipien oder seinen Eigenschaften, aufgrund derer er durch Einsatz ausreichender Ressourcen, Fachkenntnisse und entsprechender Gelegenheiten mit einem direkten Angriff überwunden werden kann. ... Mechanismen vom Typ A bedienen sich häufig eines "Geheimnisses" wie etwa eines Paßwortes oder eines kryptographischen Schlüssels.“



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

Wie wird bei Mechanismen vom Typ A die Stärke definiert?

„Alle kritischen Sicherheitsmechanismen (d.h. diejenigen, deren Versagen eine Sicherheitslücke hervorrufen würde), werden hinsichtlich ihrer Fähigkeit bewertet, einem direkten Angriff zu widerstehen. Die Mindeststärke jedes kritischen Mechanismus wird entweder als niedrig, mittel oder hoch bewertet."

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

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

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

1 Antragsteller und Evaluationsgegenstand

1 Antragsteller der Zertifizierung war die Deutsche Post Signtrust GmbH, Tulpenfeld 9, 53113 Bonn, vertreten durch die secunet Security Networks AG.

2 Ziel der Antragstellung war ein „Deutsches IT-Sicherheitszertifikat“.

3 Evaluationsgegenstand (EVG) war „ArtSignComponent V1.0“.

4 Der EVG ist eine Funktionsbibliothek für elektronische Signatur.

5 Seitens des Auftraggebers sind Sicherheitsvorgaben für den EVG in deutscher Sprache bereitgestellt worden. Die Sicherheitsvorgaben, letzte Version 2.02 vom 21.10.2003, werden im Anhang wiedergegeben.

6 Die Sicherheitsvorgaben referenzieren als Prüfkriterien die ITSEC und als Evaluationsstufe E2, für die Mindeststärke der Sicherheitsmechanismen wird „hoch“ angegeben.

2 Maßgebende Prüfgrundlagen

7 Die Evaluierung des EVG erfolgte antragsgemäß gegen die

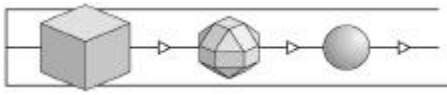
- Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) /ITSEC/.

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

- Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) /ITSEM/,
- Joint Interpretation Library /JIL/,
- Anwendungshinweise und Interpretationen zum Schema, Bundesamt für Sicherheit in der Informationstechnik /AIS/,
- Arbeitsanweisung „Deutsches IT-Sicherheitszertifikat“ der T-Systems GEI GmbH, BU ITC Security (gültige Fassung).

3 Evaluierung

9 Die Evaluierung des EVG wurde bei der Prüfstelle für IT-Sicherheit der T-Systems GEI GmbH, BU ITC Security durchgeführt.



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

11 Die Evaluierung erfolgte im Zertifizierungsschema der T-Systems.

12 Die Evaluierung wurde durch die Zertifizierungsstelle kriteriengemäß begleitet.

13 Das Ergebnis der Evaluierung ist im Evaluation Technical Report (ETR) der Prüfstelle dargestellt. Der ETR trägt die Versionsnummer 1.1 und das Datum 30.10.2003.

14 Die Evaluierung des EVG wurde am 30.10.2003 beendet.

4 Zertifizierung

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

16 Die Zertifizierungsstelle der T-Systems arbeitet im Einklang mit der DIN EN 45011 und ist im Hinblick auf diese Norm bei der DATech e.V. für Prüfungen nach den ITSEC und den Common Criteria akkreditiert (DAR-Registriernummer DIT-ZE-005/98).

17 Die Zertifizierung des EVG erfolgte wie beantragt gemäß Verfahrenstyp 04: „Deutsches IT-Sicherheitszertifikat“.

18 Dem Zertifizierungsverfahren wurde die Registriernummer T-Systems-DSZ-ITSEC-04090-2003 zugewiesen.

19 Für die Zertifizierung des EVG sind Auflagen und Empfehlungen maßgebend; näheres enthält das Kapitel 5.

20 Eine Kurzfassung der Ergebnisse enthält das Sicherheitszertifikat T-Systems-DSZ-ITSEC-04090-2003 vom 31.10.2003 auf der Seite 3 dieses Zertifizierungsreports.

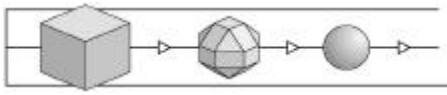
21 Das Zertifikat trägt das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) genehmigte Logo [Deutsches IT-Sicherheitszertifikat] und wird vom BSI als gleichwertig zu seinen eigenen Zertifikaten anerkannt. Das BSI bestätigt vertragsgemäß diese Gleichwertigkeit explizit im internationalen Kontext.

22 Das Zertifikat und der Zertifizierungsreport sind auf den Web-Seiten (www.t-systems-zert.com) der Zertifizierungsstelle veröffentlicht und werden in den Broschüren BSI 7148 / 7149 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) referenziert.

23 Hiermit wird bestätigt, dass

- die am Verfahren beteiligten Evaluatoren und Zertifizierer weder an der Entwicklung, dem Vertrieb noch an einer Anwendung des EVG beteiligt waren,
- alle Regeln des Zertifizierungsschemas, des speziellen Verfahrenstyps und der maßgebenden Kriterien eingehalten wurden.

Klaus-Werner Schröder	Dr. Heinrich Kersten
(Zertifizierer)	(Leiter der Zertifizierungsstelle)



5 Zusammenfassung der Ergebnisse

24 Evaluiert wurden die folgende Konfiguration des EVG:

Der EVG ist eine Software-Funktionsbibliothek; es existieren keine unterschiedlichen Konfigurationen. Der EVG ist zum Einsatz im Trust Center der Deutschen Post Signtrust GmbH bestimmt.
In den Sicherheitsvorgaben werden keine Angaben zu den Release-Ständen der im Lieferumfang enthaltenen Komponenten gemacht. Als zertifiziert gelten:

„Doku - Betriebsdokumentation [SK_Signtrust_BD]“: Release 2.0 vom 19.05.2003

“SW - Software gemäß [SK_Signtrust_KL]“ – bestehend aus folgenden Bibliotheksmodulen:

Modul	Größe/Bytes	Datum
libArtSignatureComponent.a	387.660	08.07.2003
libArtCrSmartCard.a	1.180.266	08.07.2003
libAsn1Lib.a	13.500.658	08.07.2003

25 Das Evaluierungsergebnis gilt nur für diese Konfiguration des EVG.

26 Entsprechend den Sicherheitsvorgaben und dem Ergebnis der Evaluierung besitzt der EVG folgende Sicherheitsfunktionen:

- Funktionsbibliothek: Unterstützung der Signaturerstellung, Wiederaufbereitung, Verifikation einer digitalen Signatur

27 Die Evaluierung hat ergeben, dass der EVG allen Anforderungen der Evaluationsstufe E2 der ITSEC genügt, d.h. alle Anforderungen an die Korrektheit und Wirksamkeit in dieser Stufe sind erfüllt. Dies sind:

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

Konstruktion - Entwicklungsprozeß:
Anforderungen, Architekturentwurf, Feinentwurf, Implementierung

Konstruktion - Entwicklungsumgebung:
Konfigurationskontrolle, Sicherheit beim Entwickler

Betrieb - Betriebsdokumentation:
Benutzerdokumentation, Systemverwalter-Dokumentation

Betrieb - Betriebsumgebung:
Auslieferung und Konfiguration, Anlauf und Betrieb

ITSEC 3.12 bis 3.37 für die Wirksamkeit mit den Aspekten

Wirksamkeitskriterien - Konstruktion:
Eignung der Funktionalität, Zusammenwirken der Funktionalität, Stärke der Mechanismen, Bewertung der Konstruktionsschwachstellen

Wirksamkeitskriterien - Betrieb:
Benutzerfreundlichkeit, Bewertung der operationellen Schwachstellen

29 Hinsichtlich der Sicherheitsmechanismen lautet das Ergebnis der Evaluierung:

Die folgenden Mechanismen des EVG sind **kritische** Mechanismen: M1 (PIN-Handling), M2 (RSA-Entschlüsselung), M3 (Hashwert-Berechnung).

Die folgenden Mechanismen sind vom **Typ A** und haben eine Mindeststärke gemäß der Stufe hoch: M2, M3.

Die folgenden Mechanismen sind vom **Typ B**: M1.
Für Mechanismen des Typs B ist gemäß den zugrunde liegenden Kriterien keine Mechanismenstärke anzugeben. Im Rahmen der Schwachstellenanalyse konnte jedoch festgestellt werden, daß selbst unter Zugrundelegung eines Aufwands gemäß der Stufe hoch bei den angenommenen Einsatzbedingungen keine ausnutzbare Schwachstelle erkennbar ist.

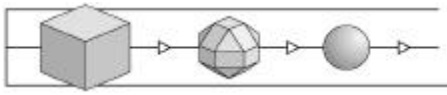
30 Die Auslieferung des Produktes erfolgt entsprechend den Angaben des Auftraggebers nach folgendem Verfahren:

Der EVG wird zusammen mit der Betriebsdokumentation auf einer Single-Session CD-ROM ausgeliefert. Die CD-ROM wird persönlich vom Entwickler an den Projektverantwortlichen der Deutschen Post Signtrust GmbH übergeben.

Dieses Auslieferungsverfahren entspricht den Vorgaben der nationalen Zertifizierungsbehörde für die Stufe E2 der ITSEC.

31 Folgende Auflagen sind durch den Auftraggeber zu erfüllen:

Die kryptographischen Algorithmen RSA-1024 bzw. SHA-1 und RIPEMD160, die vom EVG verwendet werden, sind im Zusammenhang mit dem deutschen Signaturgesetz zeitlich begrenzt zugelassen, nämlich bis Ende 2007 bzw. Ende 2008. Spätestens dann muß eine neue Bewertung der Stärke dieser Mechanismen vorgenommen werden.



32 Folgende zusätzlichen Hinweise sind für den sicherheitsgerechten Einsatz des EVG zu beachten:

Im Hinblick auf die Nutzung im Zusammenhang mit dem deutschen Signaturgesetz ist festzuhalten: Das in der Sicherheitsfunktion SF1 implementierte PIN-Handling garantiert die Nicht-Preisgabe der PIN grundsätzlich nur zwischen der Übergabe der PIN durch die steuernde Anwendung an die ArtSignComponent und der Weitergabe von der ArtSignComponent an die Schnittstelle zum Kartenterminal (ggf. einschl. Treibersoftware). Außerhalb der ArtSignComponent muss die Nicht-Preisgabe der PIN durch andere Maßnahmen in der IT-Umgebung sichergestellt werden. Hierzu kann auch das im EVG implementierte Secure Messaging beitragen; jedoch ist diese Funktionalität nicht Gegenstand der Evaluierung gewesen.

6 Anwendung der Ergebnisse

33 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.

34 Der Zertifizierungsreport dient dem Auftraggeber als Nachweis der durchgeführten Evaluierung und dem Nutzer als eine Grundlage für die sichere Nutzung des EVG.

35 Für die sichere Nutzung des EVG enthalten insbesondere die folgenden Stellen im Zertifizierungsreport wichtige Informationen:

- Kapitel 1: die genaue Produkt- und Versionsbezeichnung:
  Zertifikat und Zertifizierungsreport gelten nur für dieses Produkt und diese spezielle Version.

- Kapitel 5: Angaben zum Auslieferungsverfahren des EVG.
  Andere Auslieferungsverfahren können unter Umständen nicht die für die Stufe E2 erforderliche Sicherheit bieten.

- Kapitel 5: Angaben zu evaluierten Konfigurationen des EVG.
  Der EVG gilt nur in diesen Konfigurationen als zertifiziert.

- Kapitel 5: Hinweise für den Nutzer des EVG.
  Die Sicherheit bei der Anwendung des EVG kann ggf. nicht mehr gegeben sein, wenn diese Hinweise nicht beachtet werden.

- Anhang: Sicherheitsvorgaben zum EVG.
  Hier sind insbesondere die Informationen zur Art der Nutzung des EVG, zum Lieferumfang, zu seinen Sicherheitszielen bzw. den betrachteten Bedrohungen und zur Einsatzumgebung zu beachten.

36 Falls Anforderungen aus diesem Report nicht eingehalten werden, 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.

37 Bei Änderungen an dem EVG, an seinem Auslieferungsverfahren oder seiner Einsatzumgebung kann eine Re-Zertifizierung erfolgen. Die Ergebnisse solcher nach den Verfahrensregeln der Zertifizierungsstelle durchgeführten Re-Zertifizierungen werden in entsprechenden technischen Anhängen zu diesem Zertifizierungsreport dokumentiert.

38 Bei neuen Erkenntnissen über die Sicherheit des EVG können ebenfalls technische Anhänge zum Zertifizierungsreport herausgegeben werden.

39 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-ITSEC-04090-2003/1, .../2,...),
- neue Versionen des EVG sich in der Evaluierung befinden bzw. bereits zertifiziert worden sind.

Ende des Zertifizierungsreports zu T-Systems-DSZ-ITSEC-04090-2003.

Anhang.

Sicherheitsvorgaben zu

„ArtSignComponent V1.0“

(Diese Seite ist beabsichtigterweise leer.)

Deutsche Post Signtrust GmbH

Sicherheitsvorgaben[1] der E2-Sicherheitskomponente ArtSignComponent der Deutschen Post Signtrust GmbH

Version: 2.02
Status: Final
Datum: 21.10.2003

[1] Die vom Hersteller gelieferten Sicherheitsvorgaben wurden von der Zertifizierungsstelle redaktionell hinsichtlich der Benennung und der Beschreibung der Sicherheitsfunktion SF1 überarbeitet, ohne dass der Inhalt geändert wurde.

Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Verbesserungsvorschläge und Hinweise auf Fehler sind willkommen. Zu diesem Zweck befindet sich ein Formular am Endes dieses Handbuches. Sollte es fehlen, richten Sie bitte Ihre Anmerkungen an:

Tulpenfeld 9
53113 Bonn
Tel.: 0228-2435-510
Fax: 0228-2435-519

Inhaltsverzeichnis

1 Produktbeschreibung

Der Evaluationsgegenstand (EVG) ist eine Software-Funktionsbibliothek, die mit Hilfe von Chipkartensystemen (Chipkartenleser, Chipkartenbetriebssystem, personalisierte Chipkarte) Daten zur Wahrung deren Integrität und Authentizität mit einer digitalen Signatur im Sinne des Signaturgesetzes [SigG] versehen kann. Zusätzlich können Signaturen mathematisch verifiziert werden. Der EVG ist im Sinne der ITSEC ein Produkt mit der Bezeichnung ArtSignComponent, Version 1.0 und wird im Folgenden nur als ArtSignComponent bezeichnet.

Die im Kontext der Signatur-Erzeugung verwendeten Schlüssel müssen im Rahmen einer Personalisierung vertrauenswürdig auf die verwendete Chipkarte aufgebracht werden. Außerdem werden die Chipkarten mit einer zufälligen PIN personalisiert, welche der Benutzer mittels eines gesonderten PIN-Briefs erhält.

Zur Nutzung der ArtSignComponent muss ein Anwendungsprogrammierer eine Applikation generieren, welche die Signier- und Prüf-Funktionalität des EVG nutzt. Diese kann im signaturgesetzkonformen Trust-Center der Deutsche Post Signtrust GmbH z. B. zum Signieren von Zertifikaten, Verzeichnisdienstauskünften und Sperrlisten genutzt werden.

Der zu beschreibende Evaluationsgegenstand hat unter Berücksichtigung der Forderungen des Signaturgesetzes [SigG] und der mitgeltenden Signaturverordnung [SigV] folgende Aufgaben:

- Unterstützung der Erstellung von digitalen Signaturen über Daten unter Zuhilfenahme einer personalisierten Prozessorchipkarte. Diese Funktionalität ist notwendig für die Bereitstellung einer Sicherheitsfunktion der ArtSignComponent.
- Mathematische Prüfung einer digitalen Signatur durch die ArtSignComponent. Diese Funktionalität ist notwendig für die Bereitstellung einer Scherheitsfunktion der ArtSignComponent.
- Initialisierung von Chipkarten-Lesegeräten zur Bereitstellung der Funktionalität der verwendeten Prozessorchipkarten. Diese Funktionalität ist notwendig, um die Kommunikation zwischen der Signierkomponente und der Prozessorchipkarte zu ermöglichen.
- Bereitstellung des Signaturschlüssel-Zertifikates nach dessen Auslesen aus einer personalisierten Prozessorchipkarte.
- Bereitstellung des CA-Zertifikats nach dessen Auslesen aus einer personalisierten Prozessorchipkarte
- Bereitstellung des Root-Zertifikats der RegTP nach dessen Auslesen aus einer personalisierten Prozessorchipkarte.

1.1 Art der Nutzung

Die ArtSignComponent ist eine statische Funktionsbibliothek und wird als solche in einer entsprechenden Einsatzumgebung in Kombination mit einer Applikation betrieben.
Zur Erzeugung von digitalen Signaturen (SigG-konform) müssen folgende Eingangsdaten durch die entsprechende Applikation der ArtSignComponent zur Verfügung gestellt werden:

- PIN zur Initialisierung der Prozessorchipkarten.

Die Erfassung der PIN muss von der die ArtSignComponent nutzenden Applikation zur Verfügung gestellt werden. Weiter muß die Applikation Sorge dafür tragen, daß die PIN-Eingabe unsichtbar durch den Benutzer erfolgt und daß der Speicherbereich in dem sich die PIN befindet, nach Übergabe an die ArtSignComponent mit Nullen überschrieben wird.

- Signaturumfang (zu signierende Nutzdaten)

Zur mathematischen Verifikation elektronischer Signaturen müssen folgende Eingangsdaten durch die entsprechende Applikation der ArtSignComponent zur Verfügung gestellt werden:

- Signaturumfang
- Elektronische (digitale) Signatur über den Signaturumfang
- Zugehöriges Signaturschlüsselzertifikat bzw. öffentlicher Schlüssel

Der EVG wird folgendermaßen ausgeliefert:

Art	Beschreibung
SW	Software gemäß [SK_Signtrust_KL]
Doku	Betriebsdokumentation [SK_Signtrust_BD]

2 Sicherheitspolitik

Für den Einsatz des EVG gibt es Anforderungen sowohl an die technische als auch an die organisatorische Einsatzumgebung. Eine Beschreibung dieser Anforderungen ist Bestandteil der folgenden Kapitel.

2.1 Technische Einsatzumgebung

2.1.1 Hardware und Betriebssystem

Der EVG ist für den Einsatz unter dem Betriebssystem HP-UX Version 11.0 vorgesehen. Der EVG stellt keine besonderen Anforderungen an die Hardware. Er kann auf einer HP-Workstation mit Anschlussmöglichkeit für einen Chipkartenleser sowie CD-ROM zur Installation des EVG eingesetzt werden.

2.1.2 Chipkarten

Als Chipkarten können die E4-hoch evaluierten Telesec Signaturkarten mit dem Chipkartenbetriebssystemen TCOS 2.0 Release2 bzw. TCOS2.0 Release3 eingesetzt werden. Die Chipkartenschnittstelle erfüllt den Standard ISO 7816.
Zur Realisierung einer Übertragungssicherung muss Chipkartenseitig das *Secure Messaging* verwendet werden, welches im Vorfeld der PIN-Übertragung einen Session-Key mit der Chipkarte aushandelt. Zur Initialisierung des Secure Messaging werden 512 Bit lange RSA-Schlüsselpaare vom EVG generiert und mittels derer die symmetrischen Schlüssel mit der Karte ausgetauscht.
Das Secure Messaging wird ausschließlich als zusätzliche Servicefunktion gesehen, die die Übertragung der PIN an die Chipkarte verstärkt absichert.

2.1.3 Chipkartenterminal

Als Chipkartenterminal können Kartenleser vom Typ B1, welche die universelle Schnittstelle CT-API unterstützen, eingesetzt werden. Die Chipkartenschnittstelle muss kompatibel zu den unterstützten Chipkarten nach Kapitel 2.1.2 sein.

2.2 Organisatorische Einsatzumgebung

2.2.1 Einsatzort

Der EVG kann im zertifizierten Trust-Center der Deutsche Post Signtrust GmbH im Rahmen einer signaturgesetzkonformen Applikation eingesetzt werden.
Bei der PIN-Eingabe ist es zwingend erforderlich, dass beim Initiieren des secure messaging während der Übergabe der Parameter e und N des RSA-Verfahrens an die Chipkarte ein zuverlässiger Benutzer anwesend ist (Systemadministrator), der im Vorfeld sich von dem ordnungsgemäßen Zustand des Computers überzeugt hat, auf

dem der EVG zum Einsatz gelangt. Dieser Zustand beinhaltet, dass der Kabelweg zwischen Kartenleser und Rechner nicht manipuliert wurde und auf dem Rechner keine Programme laufen, die die PIN-Eingabe unzulässig protokollieren.

2.3 Objekte/ Subjekte/ Aktionen

Die ArtSignComponent verwaltet Objekte, bei denen berechtigte Subjekte Aktionen ausführen dürfen.

2.3.1 Subjekte

Das Produkt in Form der ArtSignComponent wird in Form einer Anwendungsschnittstelle betrieben, d. h. nur die zugehörige Applikation ist in der Lage, aktiv Daten an die ArtSignComponent zu übergeben bzw. von dieser zu übernehmen. Daher existieren nur folgende Subjekte:

S1:	**Applikation, die die ArtSignComponent nutzt.**
S2:	**Anderes, unbefugtes Subjekt (Mensch, Maschine, etc.)**

Tabelle 1: Subjekte, die auf die ArtSignComponent einwirken

Die ArtSignComponent besitzt keine Benutzerschnittstelle, über die ein anderer Benutzer als S1 die ArtSignComponent ansprechen könnte.

Die der ArtSignComponent zugeordnete Prozessorchipkarte wird nicht als Subjekt definiert, da sie nur als rein passives Rechenwerk genutzt wird.

2.3.2 Objekte

Das Produkt in Form des EVG bietet Schutz für die nachfolgend aufgeführten Objekttypen:

O1:	**Signierte Daten**
O2:	**PIN**

Tabelle 2: Objekte, die die ArtSignComponent verwaltet

Objekte vom Typ O1 stellen Daten mit definiertem Aufbau dar. Sie setzen sich zusammen aus einem *Signaturumfang*, d. h. aus den Daten, die letztendlich signiert werden (von den einzelnen Applikationen abhängig), und der *elektronischen Signatur* über den Signaturumfang.

Das Objekt vom Typ O2 stellt die PIN dar. Mit Hilfe der PIN werden die Prozessorchipkarten initialisiert. Die PIN wird von der nutzenden Applikation an die ArtSignComponent übergeben.

2.3.3 Zugriffsarten

Nachfolgende Aktionen sind für das Subjekt S1 möglich:

A1:	**Digital signieren**
A2:	**Verifikation einer Signatur**
A3:	**Übergabe**

Tabelle 3: Aktionen zu den Objekte

Eine digitale Signatur kann herangezogen werden, um sowohl den Ersteller der Signatur zu identifizieren als auch die Integrität der Daten zu wahren, über die die digitale Signatur gelegt wurde.

Für eine Aktion vom Typ A1 unterstützt die ArtSignComponent die Verwendung privater Signaturschlüssel. Innerhalb der SigG-konformen ZS sind diese jeweils einer Applikation (S1) zugeordnet. Die Zuordnung zwischen dem zugehörigen Signaturschlüssel-Zertifikat und der ZS-Applikation (S1) wurde von der zuständigen Regulierungsbehörde RegTP zertifiziert.
Der Inhalt der *Nutzdaten* ist von der jeweiligen Applikation abhängig:

Applikation	**Nutzdaten**
Verzeichnisdienst	Antwort des Verzeichnisdienst an den Kunden
Zeitstempeldienst	Antwort des Zeitstempeldienst an den Kunden
Zertifizierungskomponente	Ein zu erstellendes Signaturschlüssel-Zertifikat

Tabelle 4: Nutzdaten in Abhängigkeit der Applikation

Die Nutzdaten, die der ArtSignComponent zum Signieren übergeben werden, müssen von der jeweiligen Applikation auf vertrauenswürdige Weise zur Verfügung gestellt werden.

Eine Aktion vom Typ A2 ist die Überprüfung der mathematischen Korrektheit einer elektronischen Signatur. Alle Informationen, die zur Durchführung der Aktion A2 durch die ArtSignComponent notwendig sind, müssen durch die nutzenden Applikationen der ArtSignComponent auf vertrauenswürdige Weise zur Verfügung gestellt werden.

Eine Aktion vom Typ A3 ist die Übergabe der PIN (O2) durch die nutzende Applikation (S1) an die ArtSignComponent.

2.4 Definition der Sicherheitspolitik

Die vom EVG verfolgte Politik läßt sich direkt aus §17(1) des Signaturgesetzes wie folgt formulieren:

„Die ArtSignComponent muss Fälschungen elektronischer Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen. Für den EVG sind Sicherheitsvorkehrungen erforderlich, die gegen unberechtigte Nutzung der privaten Signaturschlüssel schützen.“

2.5 Sicherheitsziele

Die Sicherheitsziele, die die ArtSignComponent erfüllen soll, lassen sich aus deren Sicherheitspolitik ableiten und basieren auf Forderungen des Signaturgesetztes und der mitgeltenden Signaturverordnung.

SZ-1:	*Die ArtSignComponent gewährleistet, daß die an sie übergebene PIN (O2) nicht preisgegeben wird.*
SZ-2:	*Die ArtSignComponent unterstützt die Erzeugung digitaler Signaturen gemäß SigG/ SigV.*
SZ-3:	*Eine mathematische Verifikation elektronischer Signaturen wird durch die ArtSignComponent korrekt durchgeführt.*

2.6 Bedrohungen

B-1:	*Die PIN (Objekt O2) wird durch einen Angreifer aus dem Speicher ermittelt.*
B-2:	*Die signierten Daten (Objekte vom Typ O1: Signatur, die von der Chipkarte im Rahmen der Erzeugung einer digitalen Signatur erstellt wurden und die signierten Daten) werden nachträglich manipuliert, ohne das dies erkannt wird.*

3 Sicherheitsfunktionen

Die ArtSignComponent stellt folgende Sicherheitsfunktionen zur Verfügung, die den in Kapitel 2.6 festgestellten Bedrohungen entgegenwirken als auch zum Erreichen der in Kapitel 2.5 definierten Sicherheitsziele dient:

Nr.	Sicherheitsfunktion
SF1:	Unterstützung der Signaturerstellung, Wiederaufbereitung
SF2:	Mathematische Verifikation einer digitalen Signatur

Tabelle 5: Sicherheitsfunktionen der ArtSignComponent

3.1 Die Sicherheitsfunktion SF1 (Unterstützung der Signaturerstellung, Wiederaufbereitung)

Innerhalb der Sicherheitsfunktion SF1 unterstützt die ArtSignComponent die Erstellung der nachprüfbaren, eindeutigen Verbindung (digitale Signatur) zwischen dem zugehörigen Signaturschlüssel-Zertifikat und dem zu signierenden Signaturumfang mit Hilfe eines privaten Signaturschlüssels.

Über den Signaturumfang der zu signierenden Daten wird mittels einer Hash-Funktion eine Abbildung auf eine Byte-Kette definierter Länge erstellt. Der erzeugte Hash-Wert wird anschließend mittels eines privaten Signaturschlüssels unter Zuhilfenahme einer Prozessorchipkarte chiffriert[2]. Die ArtSignComponent übergibt dieses Chiffrat zurück an die aufrufende Applikation.

Die Inbetriebnahme und Initialisierung der Chipkarten in den Chipkartenlesern erfolgt durch Übergabe einer PIN an die ArtSignComponent, die diese an die Chipkarte weiterleitet. Die PIN wird durch die den EVG nutzende Applikation erfasst. Die nutzende Applikation muss dafür Sorge tragen, daß die PIN-Eingabe unsichtbar erfolgt und der Speicherbereich, in dem sich die PIN befindet, nach Übergabe an den EVG wieder aufbereitet wird.

Nach erfolgreicher Initialisierung der Chipkarten überschreibt die ArtSignComponent mit Hilfe der SF1 den Speicherbereich in dem sich die PIN befindet mit Nullen, so daß dann kein unbefugter Zugriff auf die PIN möglich ist.

3.2 Die Sicherheitsfunktion SF2 (math. Verifikation einer digitalen Signatur)

Innerhalb der Sicherheitsfunktion SF2 prüft die ArtSignComponent die mathematische Korrektheit einer digitalen Signatur eines Objektes O1.

[2] Die Prozessorchipkarte muss zuvor durch Übergabe der PIN initialisiert sein.

Die Applikationen, die den EVG nutzt, übergibt den Signaturumfang des Objektes O1 und dessen Signatur sowie das zugehörige Signaturschlüsselzertifikat oder alternativ den öffentlichen Schlüssel an den EVG. Mit Hilfe dieser Informationen kann geprüft werden, ob es zu einer Manipulation am Signaturumfang oder der Signatur oder am öffentlichen Schlüssel gekommen ist. Ein übergebenes Signaturschlüsselzertifikat wird nicht zusätzlich geprüft.

Im Schritt 1 wird die Signatur des Objektes O1 mittels des zugehörigen öffentlichen Signaturschlüssels PK_{MA} (gegebenenfalls aus dem Signaturschlüsselzertifikat entnommen) dechiffriert. Dieses Ergebnis wird in dieser Darlegung als *Vergleichswert1* bezeichnet. Man hat so die Information darüber, welchen Hashwert der Ersteller der Signatur über den Signaturumfang erzeugt hat. Der EVG führt zu keinem Zeitpunkt eine mathematische Operation mit dem privaten Schlüssel SK_{MA} aus. Die Information $Signatur=SK_{MA}(Hash[Signaturumfang])$ wurde ausschließlich vom Ersteller der Signatur erzeugt.

Im Schritt 2 wird überprüft, ob eine PKCS#1-Blockkonformität von *Vergleichswert1* vorliegt (siehe auch Kapitel 3.3, Hinweise zu SF1 und SF2). Das schrittweise Vorgehen dieser Prüfung wird im Feinentwurf zum EVG dargelegt (s.e.d., Kapitel 7.1, „Blockprüfung bei der Sicherheitsfunktion SF-2“). Wenn der *Vergleichswert1* nicht PKCS#1-kodiert ist, so ist das Ergebnis der Signaturprüfung „*mathematisch nicht korrekt*“ und die folgenden Schritte werden nicht durchgeführt. Wenn der *Vergleichswert1* PKCS#1-kodiert ist, so gehe zu Schritt 3.

Schritt 3: Identifiziere im *Vergleichswert1* die zum Signieren verwendete Hashfunktion. Wenn die Hashfunktion nicht identifizierbar ist oder nicht RIPEMD-160 oder nicht SHA-1 ist, so ist das Ergebnis der Signaturprüfung „mathematisch nicht korrekt“ und de folgenden Schritte werden nicht durchgeführt. Wenn die Hashfunktion als RIPEMD-160 oder SHA-1 identifiziert ist, so gehe zu Schritt 4.

Im Schritt 4 wird aus dem *Vergleichswert1* der HashWert extrahiert für Vergleichszwecke. In dieser Darlegung wird dieser Hashwert als *Vergleichswert2* bezeichnet.

Schritt 5: Bilde aus [Signaturumfang] mit der im Schritt 3 identifizierten Hashfunktion den Vergleichswert3 := Hash[Signaturumfang]

Im Schritt 6 werden die Werte *Vergleichswert2* und *Vergleichswert3* miteinander verglichen. Wenn Ungleichheit besteht, so ist das Ergebnis der Signaturprüfung „*mathematisch nicht korrekt*“. Wenn Gleichheit besteht, so ist das Ergebnis der Signaturprüfung „*mathematisch korrekt*“.

Math.Prüfung der Signatur:

1. Bilde: Vergleichswert1 = PK_{MA}(Signatur), wobei Signatur=SK_{MA}(Hash[Signaturumfang])(wurde vom Ersteller der Signatur erzeugt)
2. Prüfe PKCS#1-Blockkonformität vom Vergleichswert1
3. Identifiziere Hashfunktion aus Vergleichswert1
4. Vergleichswert2= extrahiere HashWert aus Vergleichswert1
5. Bilde aus Vergleichswert3=Hash[Signaturumfang]
6. Vergleiche: Vergleichswert2 == Vergleichswert3

3.3 Hinweise zu SF1 und SF2

Unterstützt werden die Hash-Algorithmen SHA-1 und RIPEMD-160 [Krypt]. Als Signaturalgorithmus wird RSA verwendet (siehe [Krypt], der öffentliche Exponent wird bei SF1 auf 2^{16}+1 fest gesetzt) unter zu Hilfenahme von Schlüssellängen von 1024Bit (Chipkarte). Die digitalen Signaturen, mit denen der EVG umgeht, sind mit einem privaten RSA-Signaturschlüssel verschlüsselte, blockformatierte Hashwerte des Signaturumfanges. Die Blockformatierung erfolgt mit der im PKCS#1-Standard spezifizierten Kodierung EMSA-PKCS1-v1_5-ENCODE. Dabei wird die Kennung des Hash-Verfahrens zusammen mit dem Hashwert nach den Distinguished Encoding Rules (DER) in einen String *T* kodiert. Dann wird ein String *PS* aus 1024 - |*T*| - 3 Hexadezimalwerten[3] FF gebildet. Die blockformatierte Ausgabe ist dann 00 01 || *PS* || 00 || *T*.[4]

4 Zweckmäßigkeit der Funktionalität

4.1 Korrelation Sicherheitsziele/ Bedrohungen/ Sicherheitsfunktionen

Die folgende Tabelle 6 zeigt auf, durch welche Sicherheitsfunktionen das in Kapitel 2.4 angestrebte Sicherheitsziel erreicht wird:

	SZ1	SZ2	SZ3
SF1	X	X	
SF2			X

Tabelle 6: Korrelation zwischen den Sicherheitsfunktionen und dem Sicherheitsziel

[3] |*T*| bezeichnet hier die Hexadezimale Länge von *T*

[4] || bezeichnet hier die Konkatenation, d. h. das Aneinanderhängen von Bitstrings

Mit der folgenden Tabelle 7 wird der Bezug zwischen der in Kapitel 2.6 festgelegten Bedrohung und den in Kapitel 3 spezifizierten Sicherheitsfunktionen hergestellt.

	B1	**B2**
SF1	X	X
SF2		X

Tabelle 7: Korrelation zwischen den Sicherheitsfunktionen und der Bedrohung

4.2 Zweckmäßigkeit

4.2.1 Zweckmäßigkeit der Sicherheitsfunktionen in Bezug auf Sicherheitsziele

SZ-1: *(Die ArtSignComponent gewährleistet, daß die an sie übergebene PIN (O2) nicht preisgegeben wird.)*
Die Sicherheitsfunktion **SF1** gewährleistet, daß die an die ArtSignComponent übergebene PIN zur Chipkarte weitergeleitet wird. Nach erfolgreicher Initialisierung der Chipkarten überschreibt die Sicherheitsfunktion **SF1** den Speicherbereich in dem sich die PIN befindet mit Nullen, so daß dann kein Zugriff auf die PIN möglich ist.

Somit wird das Sicherheitsziel **SZ-1** durch die Sicherheitsfunktion **SF1** realisiert.

SZ-2: (*Die ArtSignComponent unterstützt die Erzeugung digitaler Signaturen gemäß SigG/ SigV.)*
Die Sicherheitsfunktion **SF1** erstellt über den Signaturumfang der zu signierenden Daten (INPUT) mittels einer Hash-Funktion eine Abbildung auf eine Byte-Kette definierter Länge.
Der erzeugte Hash-Wert wird anschließend mittels eines privaten Signaturschlüssels unter Zuhilfenahme einer Prozessorchipkarte chiffriert. Somit realisiert die **SF1** unter Zuhilfenahme einer Prozessorchipkarte mit E4-hoch evaluiertem Betriebssystem das **SZ-2**.

SZ-3: *(Eine mathematische Verifikation elektronischer Signaturen wird durch die ArtSignComponent korrekt durchgeführt.)*
Die Sicherheitsfunktion **SF2** gewährleistet die korrekte mathematische Verifikation elektronischer Signaturen.

4.2.2 Zweckmäßigkeit der Sicherheitsfunktionen in Bezug auf die Bedrohungen

SF1 wirkt der Bedrohung **B1** entgegen.

Nach erfolgter Übergabe der PIN von der Applikation an die ArtSignComponent leitet diese die PIN unter Anwendung eines unterstützenden *Secure Messaging* an die Prozessorchipkarte weiter. Nach erfolgreicher Initialisierung der Prozessorchipkarte überschreibt die Sicherheitsfunktion **SF1** den Speicherbereich, in dem sich die PIN befindet, mit Nullen, so daß dann kein Zugriff auf die PIN möglich ist.

SF1 und **SF2** wirken der Bedrohung **B2** gemeinsam entgegen.
Mit Hilfe der Sicherheitsfunktion **SF1** werden unter der integeren Einbeziehung des privaten Signaturschlüssels, der der ArtSignComponent zugeordneten Prozessorchipkarte Objekte vom Typ O1 derart erzeugt, daß eine nachträgliche Manipulation an diesem Objekt ohne Besitz der entsprechenden Prozessorchipkarte und der zugehörigen PIN nicht unbemerkt durchführbar ist.

Mit Hilfe der Sicherheitsfunktion **SF2** kann jederzeit zweifelsfrei die mathematische Korrektheit des Objektes O1 festgestellt werden.

5 Evaluationsziel

5.1 Angestrebte Evaluationsstufe

Für den EVG ArtSignComponent wird bezüglich der Korrektheit der Implementierung die ITSEC-Evaluationsstufe **E2** festgelegt.

5.2 Mindeststärke der Mechanismen

Die Mindeststärke aller verwendeten Mechanismen wird mit **hoch** postuliert.

Tabellenverzeichnis

Literaturverzeichnis

[SigG]	**Signaturgesetz**, Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, in Kraft getreten am 16.05.2001
[Krypt]	Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001
[SigV]	**Signaturverordnung,** Verordnung zur elektronischen Signatur vom 16.11.2001 (BGBL 2001 Teil I Nr.59, S. 3074-3084)
[SK_Signtrust_BD]	**Betriebsdokumentation** der E2-Sicherheitskomponente ArtSignComponent der Deutschen Post Signtrust GmbH, Version 2.0, 19.05.2003
[SK_Signtrust_KL]	**Konfigurationsliste** der E2-Sicherheitskomponente ArtSignComponent der Deutschen Post Signtrust GmbH, Version 2.0, 19.05.2003

Ende der Sicherheitsvorgaben zu
„ArtSignComponent V1.0“.

Zertifizierungsreport T-Systems-DSZ-ITSEC-04090-2003

Hrsg.:	T-Systems GEI GmbH
Adresse:	Rabinstr.8, 53111 Bonn
Telefon:	0228/9841-0
Fax:	0228/9841-60
Web:	www.t-systems-itc-security.com www.t-systems-zert.com