T · · Systems · · ·

Zertifizierungsreport

T-Systems-DSZ-ITSEC-04097-2003

AVA-Sign Version 2.1

ventasoft GmbH

Zertifizierungsreport T-Systems-DSZ-ITSEC-04097-2003

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

AVA-Sign Version 2.1

der

ventasoft GmbH
Prenzlauer Allee 36, D-10405 Berlin

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:	**Signaturprüfung, Unterstützung der Signaturerstellung, Entschlüsseln, Verschlüsseln, Sichere Anzeige, Umgebungskontrolle**
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. Die Bewertung der Stärke der zur Ver- und Entschlüsselung geeigneten kryptographischen Mechanismen ist von der Anerkennung durch das BSI ausgenommen. Kopien des Zertifikats und des Zertifizierungsreports sind beim Auftraggeber und bei der Zertifizierungsstelle erhältlich.

Registrierungsnummer:
T-Systems-
DSZ-ITSEC-04097-2003

Bonn, den 20.10.2003

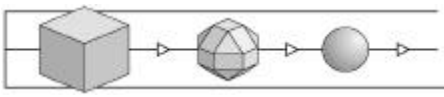
T · · Systems · · ·

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

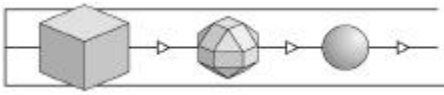
/ITSEC/ Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Version 1.2 (1991), Bundesanzeiger-Verlag Köln, ISBN 92-826-3003-X

/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.)

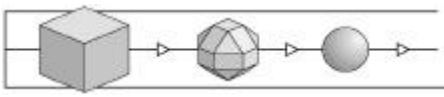


Glossar

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 (Adminstrations- und Benützer-) 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?

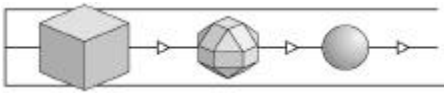
Vertrauen in die Erfüllung der Sicherheitsziele kann man dann haben, wenn *Korrektheit* und *Wirksamkeit* geprüft (*evaluiert*) worden sind.

- 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.

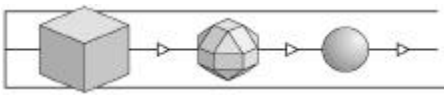
Die Widerstandskraft eines Sicherheitsmechanismus gegenüber direkten Angriffen wird als *Stärke* des Mechanismus bezeichnet.

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 Hersteller und Evaluationsgegenstand

1 Hersteller ist die ventasoft GmbH, Prenzlauer Allee 36, D-10405 Berlin.

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

3 Evaluationsgegenstand (EVG) war „AVA-Sign Version 2.1“.

4 Der EVG ist eine Signaturanwendungskomponente zur Verwendung im Zusammenhang mit der Vergabe-Plattform AVA-Online.

5 Seitens des Herstellers sind Sicherheitsvorgaben für den EVG in deutscher Sprache bereitgestellt worden. Die Sicherheitsvorgaben, letzte Version 1.15 vom 15.10.2003 , werden im Anhang wiedergegeben.

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

7 Dem Zertifizierungsverfahren wurde die Registriernummer T-Systems-DSZ-ITSEC-04097-2003 zugewiesen.

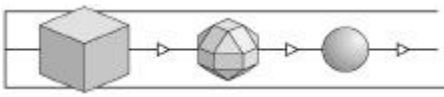
2 Maßgebende Prüfgrundlagen

8 Die Evaluierung des EVG erfolgte antragsgemäß gegen die

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

9 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

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

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

12 Die Evaluierung erfolgte im Zertifizierungsschema der T-Systems.

13 Die Evaluierung wurde durch die Zertifizierungsstelle kriteriengemäß begleitet.

14 Das Ergebnis der Evaluierung ist im Evaluation Technical Report (ETR) der Prüfstelle dargestellt. Der ETR trägt die Versionsnummer 1.0 und das Datum 20.10.2003.

15 Die Evaluierung des EVG wurde am 20.10.2003 beendet.

4 Zertifizierung

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

17 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).

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

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

20 Eine Kurzfassung der Ergebnisse enthält das Sicherheitszertifikat mit der Kennung T-Systems-DSZ-ITSEC-04097-2003 vom 20.10.2003 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 im internationalen Kontext.

22 Das Zertifikat und der Zertifizierungsreport sind auf den Web-Seiten (www.t-systems-zert.com) der Zertifizierungsstelle veröffentlicht und wer-

den in den Broschüren BSI 7148 / 7149 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) referenziert.

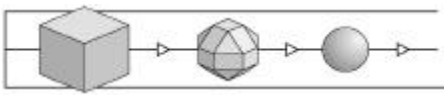
23 Hiermit wird bestätigt, daß

- 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.

Dr. Heinrich Kersten

(Leiter der Zertifizierungsstelle)



(Diese Seite ist beabsichtigterweise leer.)

5 Zusammenfassung der Ergebnisse

24 Evaluiert wurde die folgende Konfiguration des EVG:

Bei der Installation von AVA-Sign gibt es die Möglichkeit, zwischen drei Installationsarten zu wählen: „Standard“, „Vollständig“ und „Benutzerdefiniert“. Die sich hierbei ergebenden Unterschiede in der Installation betreffen lediglich Parameter außerhalb des EVG (Installation von Musterdateien und Erstellung einer Verknüpfung zu „crlloader.exe“ im Autostart–Verzeichnis des Betriebssystems) und beeinflussen in keiner Form die Sicherheit des EVG. Aus Sicht der Sicherheit besitzt der EVG deshalb nur eine (allen Installationsarten gemeinsame) Konfiguration.

AVA-Sign Version 2.1 wurde mit allen in den Sicherheitsvorgaben angegebenen Kartenlesern sowie Chipkarten getestet, und zwar unter Windows 2000 und Windows XP auf Standard-PC.

Der EVG ist lauffähig unter Microsoft Windows Betriebssystemen ab Windows 98; unter die Zertifizierung fällt jedoch **nur** der Betrieb mit Windows 2000 oder Windows XP.

Laut Herstellerangaben konnten die D-TRUST und STARCOS Signaturkarten mit dem „Kobil Kaan Standard Plus“ Kartenleser nicht unter Windows 2000 getestet werden. Daher fallen diese Kombinationen **nicht** unter die Zertifizierung.

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

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

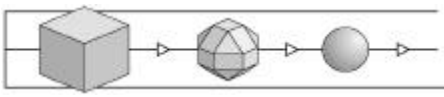
- Signaturprüfung, Unterstützung der Signaturerstellung, Entschlüsseln, Verschlüsseln, Sichere Anzeige, Umgebungskontrolle

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: Jede Sicherheitsfunktionen enthält mindestens einen kritischen Teilmechanismus.

Die folgenden Mechanismen sind vom Typ A und haben eine Mindeststärke gemäß der Stufe hoch: Die Sicherheitsfunktionen Signaturprüfung, Unterstützung der Signaturerstellung, Entschlüsseln und Verschlüsseln enthalten jeweils mindestens einen Teilmechanismus vom Typ A.

Die folgenden Mechanismen sind vom Typ B: Die Sicherheitsfunktionen Sichere Anzeige und Umgebungskontrolle enthalten nur Mechanismen vom Typ B.
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 nach folgendem Verfahren:

Die Auslieferung des EVG kann auf zwei verschiedene Weisen erfolgen:

- Download aus dem Internet von der folgenden Web-Seite des Herstellers:

  www.ventanet.de/produkte/auswahl.html

- Auslieferung auf CD direkt vom Hersteller[1].

In **beiden** Fällen hat der Benutzer durch Prüfung der Signatur der Installationsdatei sicherzustellen, daß es sich um das zertifizierte Produkt handelt und keine Änderungen auf dem Transportweg erfolgt sind:

Das für die Signatur der Installationsdatei maßgebliche Zertifikat ist auf der Website des Herstellers unter

https://www.ventanet.de/produkte/check_ava-sign.html

hinterlegt. Der öffentliche Schlüssel des Zertifikats des Herstellers lautet:

```
3081 8902 8181 00C0 8609 47DC 55C6 C19E BDD6 3B2D E108 E118 2847
78EC 3D40 F24A EA52 3F7D 92F5 49BD E7ED FC32 73AC 65D1 D281 9390
675A 570E 1D6E 3F89 A8F1 4420 2C52 77D6 1C79 808B 803E 790B 8FAD
C3D0 88E3 3502 738B CB07 85A9 CEEE 3344 6B75 FD12 EFAF 7398 5CE7
616A C049 20D4 1F28 4333 1616 7AEE 21B7 44A2 96B6 0CB4 2A96 F666
23E9 8CF8 0702 0301 0001
```

Der zugehörige Fingerabdruck lautet:

```
DDB2 A999 7192 D009 8E09 5D1D 9329 5175 D2E0 2B93
```

Die Prozeduren zur Überprüfung und sicheren Installation von AVA-Sign sind detailliert in dem Anwenderhandbuch (Online-Hilfe) beschrieben.

Die zuvor beschriebenen Auslieferungsverfahren entsprechen den Vorgaben der nationalen Zertifizierungsbehörde für die Stufe E2 der ITSEC.

31 Folgende Auflagen sind durch den Hersteller zu erfüllen:

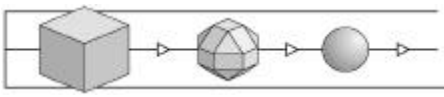
Die kryptographischen Algorithmen RSA-1024 bzw. SHA-1 und RIPEMD160, die vom EVG verwendet werden, sind im Zusammenhang mit dem deutschen Signaturgesetz zeitlich begrenzt zugelassen, nämlich bis Ende 2007 bzw. Ende 2008. Spätestens dann muß eine neue Bewertung der Stärke dieser Mechanismen vorgenommen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

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

1. AVA-Sign unterstützt auch Terminals ohne sichere PIN-Eingabe. Der Benutzer wird darauf hingewiesen, daß der Betrieb mit solchen Terminals

---

[1] In diesem Fall wird der EVG als Teil AVA-Sign Pakets mit dem Bietermodul, einem Chipkartenterminal und einer Chipkarte ausgeliefert – diese Komponenten gehören jedoch nicht zum EVG.



insbesondere der Annahme A3.1 in den Sicherheitsvorgaben (s. Anhang) widerspricht und somit **nicht** als „zertifiziert“ betrachtet werden kann.

2. Für Anwendungen im Bereich der elektronischen Signatur ist auf folgendes zu achten: Bezieht der Nutzer den Kartenleser nicht über den Hersteller ventasoft als Teil des AVA-Sign Pakets, muß sichergestellt werden, daß der Kartenleser entsprechend SigG sicherheitsbestätigt ist; in Zweifelsfällen ist der Hersteller zu kontaktieren; beim verschiedentlich angebotenen Firmware-Update für Kartenleser ist darauf zu achten, daß nur auf solche Firmware-Versionen aktualisiert wird, die unter die entsprechende Sicherheitsbestätigung fallen.

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 Hersteller 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 numeriert: T-Systems-DSZ-ITSEC-04097-2003/1, .../2,...),
- neue Versionen des EVG sich in der Evaluierung befinden bzw. bereits zertifiziert worden sind.

Ende des Zertifizierungsreports zu T-Systems-DSZ-ITSEC-04097-2003.

(Diese Seite ist beabsichtigterweise leer.)

Anhang: Sicherheitsvorgaben

zu „AVA-Sign Version 2.1“

(Diese Seite ist beabsichtigterweise leer.)

Evaluierung von AVA-Sign in der Version 2.1

Nach ITSEC E2 hoch

Sicherheitsvorgaben[2]

Version 1.15

vom

15.10.2003

venta*soft* GmbH

Prenzlauer Allee 36
10405 Berlin

Tel.: 030 – 44 33 11 0

Fax.: 030 – 44 33 11 15

---

[2] Die vom Hersteller gelieferten Sicherheitsvorgaben wurden von der Zertifizierungsstelle redaktionell hinsichtlich der Benennung und der Beschreibung der Sicherheitsfunktion F2 überarbeitet, ohne dass der Inhalt geändert wurde.

Inhalt:

1 Zu zertifizierendes Objekt

1.1 Genaue Bezeichnung

Der EVG ist das Produkt AVA-Sign Version 2.1 der Firma Ventasoft GmbH.

1.2 Auflistung der Hard- und Software-Komponenten

Nr	Typ	Bezeichnung	Release	Datum	Auslieferungs-name	Übergabe-form
1	SW	AVA-Sign	2.1	12.10.2003	AVA-Sign	CD, Online
2	DK	Benutzerhandbuch	1.18	12.10.2003	avasign_help.pdf	Pdf, Papierform

SW = Software, DK = Dokumentation

2 Art der Nutzung

2.1 Produktbeschreibung

Das AVA-Sign Paket, dessen Teil der EVG AVA-Sign ist, ermöglicht eine digitale Bearbeitung der Vergabeunterlagen und eine rechtsverbindliche Abgabe von Angeboten in digitaler Form einschließlich qualifizierter elektronischer Signatur und Verschlüsselung bei öffentlichen Ausschreibungen nach VOB/A, VOL/A und VOF. Es arbeitet mit AVA-Online der Firma Ventasoft GmbH auf einem Server in der Vergabestelle und AVA-Sign Paketen anderer Bieter zusammen. Der Bieter kann die Ausschreibungsunterlagen auf seinen lokalen Computerarbeitsplatz laden. AVA-Sign ermöglicht die Entschlüsselung und die Signaturprüfung der Ausschreibungsunterlagen sowie deren Bearbeitung zu den Angebotsunterlagen. Die Angebotsunterlagen können für die Übermittlung an AVA-Online-Server und die Speicherung auf dem AVA-Online-Server mit AVA-Sign signiert und verschlüsselt werden.

Das AVA-Sign Paket besteht aus

(1) der AVA-Sign Software (EVG),

(2) dem Bietermodul,

(3) dem Chipkartenterminal,

(4) der Chipkarte.

Der AVA-Sign EVG hat die Aufgabe

(a) die Ausschreibungsunterlagen und die Angebotsunterlagen darzustellen,

(b) die Bearbeitungswerkzeuge für die Angebotsunterlagen bereitzustellen,

(c) als Signaturanwendung für die Erstellung und die Prüfung qualifizierter elektronischer Unterschriften zu dienen,

(d) eine verschlüsselte Kommunikation mit der Vergabestelle zu ermöglichen, mindestens die Ausschreibungsunterlagen zu entschlüsseln und die Angebotsunterlagen zu verschlüsseln.

Der AVA-Sign EVG besteht aus folgenden Komponenten:

(1) der Software und

(2) der Benutzerdokumentation.

Die AVA-Sign Software stellt die Sicherheitsfunktionalität des EVG zur Verfügung.

Das Bietermodul ist ein selbständiges Programm zur Darstellung und Bearbeitung von Leistungsverzeichnissen und Angeboten in den durch den Gemeinsamen Ausschuss Elektronik im Bauwesen (GEAB) definierten Formaten GAEB-D83 und GAEB-D84.

Das Bietermodul stellt keine Sicherheitsfunktionen zur Verfügung.

Das Chipkartenterminal hat die Aufgabe,

(a) die Kommunikationsschnittstelle zwischen dem Personalcomputer und der Chipkarte bereitzustellen, insbesondere zur Übergabe der zu signierenden Daten vom Personalcomputer an die Chipkarte und der digitalen Signatur von der Chipkarte an den Personalcomputer,

(b) als Eingabeschnittstelle des Benutzers die Authentisierungsdaten (PIN) entgegenzunehmen und an die Chipkarte weiterzuleiten.

AVA-Sign verwendet folgende nach SigG als Signaturkomponenten bestätigte Chipkartenterminals

- Cherry G83-6700LPZxx/00, G83-6700LQZxx/00,
- Kobil Kaan Standard Plus,
- Kobil Kaan Professional,
- Orga HML 5010 und 5020
- Reiner SCT CyberJack e-com,
- Reiner SCT CyberJack pinpad,
- Reiner SCT CyberJack,
- SCM Microsystems SPR532

Das Terminal ist nicht Gegenstand der Evaluation. Die Evaluation stützt sich auf die zertifizierte Funktionalität des Chipkartenterminals.

Die Chipkarte hat als sichere Signaturerstellungseinheit die Aufgabe

(1) die Signaturerstellungsdaten (privater Schlüssel) zu speichern,

(2) digitale Signaturen zu den vom Chipkartenterminal übergebenen Daten zu erzeugen und an das Chipkartenterminal zu übergeben,

(3) die Authentisierungsdaten des Kartenhalters zu prüfen und die dafür benötigten Referenzdaten zu speichern und zu wechseln.

AVA-Sign Software verwendet folgende als Signaturerstellungseinheiten nach SigG bestätigte Chipkarten

- DATEV e:secure,
- D-TRUST-CARD, Version 1.0,
- Signtrust SEA – Karte, Version 2.0
- STARCOS SPK2.3 with Digital Signature Application StarCert
- T-Telesec PKS – Card, Version 2.0, 3.0,
- T-Telesec E4Netkey – Karte.

Die Chipkarte ist nicht Gegenstand der Evaluation. Die Evaluation stützt sich auf die zertifizierte Funktionalität der Chipkarte zur Signaturerstellung. AVA-Sign Software nutzt weiterhin die nicht notwendig zertifizierte RSA – Entschlüsselungsfunktion der Chipkarte.

Ebenfalls nicht Gegenstand der Evaluation sind die Vergabeplattform AVA-Online und die dort ablaufenden Prozesse. Für diese Evaluierung wird davon ausgegangen, dass die Ausschreibungsunterlagen (siehe unten, Abschnitt 3.1) korrekt erzeugt, signiert und auf dem AVA-Online-Server eingestellt werden; Angriffe gegen den AVA-Online-Server und durch Innentäter der Vergabestelle werden hier nicht betrachtet.

2.2 Annahmen über die Einsatzumgebung

Der EVG wird als Signaturanwendungskomponente in einem geschützten Einsatzbereich gemäß [4] eingesetzt (siehe Glossar).

Die Anforderungen A1, A2 und A3 sind als Auflagen für den Einsatz zu verstehen.

A1 Voraussetzungen für die qualifizierte elektronische Unterschrift

(A1.1) Die Chipkarte ist als sichere Signaturerstellungseinheit für den Kartenhalter personalisiert.

(A1.2) Der Kartenhalter verfügt über ein gültiges qualifiziertes Signaturzertifikat zu dem öffentlichen Signaturschlüssel, der zu dem privaten Signaturschlüssel in der Chipkarte als sichere Signaturerstellungseinheit gehört.

(A1.3) Der Bearbeiter verfügt über eine Liste der autorisierten Absender der Ausschreibungsunterlagen (Mitarbeiter der Vergabestelle)

(A1.4) Die Absender der Ausschreibungsunterlagen (Vergabestelle) verfügen über gültige qualifizierte Signaturzertifikate.

(A1.5) Die qualifizierten Signaturzertifikate der Bieter und der Absender der Ausschreibungsunterlagen (Vergabestelle) sind in online verfügbaren Verzeichnisdiensten abrufbar.

(A1.6) Der Absender der Ausschreibungsunterlagen (Vergabestelle) als Ersteller der Signatur und der Empfänger der Ausschreibungsunterlagen als Signaturprüfer unterstützen das S/MIME-Format innerhalb der Zip-Datei.

A2 Voraussetzungen für die verschlüsselte Kommunikation

(A2.1) Der Kartenhalter verfügt über ein gültiges Verschlüsselungszertifikat zu dem öffentlichen Verschlüsselungsschlüssel, der zu dem privaten Verschlüsselungsschlüssel in der Chipkarte des Kartenhalters gehört. Die Chipkarte unterstützt das Entschlüsseln von Datenschlüsseln mit dem privaten Verschlüsselungsschlüssel des Kartenhalters.

(A2.2) Die Absender der Angebotsunterlagen (Bieter) und die Absender der Ausschreibungsunterlagen (Vergabestelle) verfügen über eine Liste der autorisierten Empfänger und deren gültige Verschlüsselungszertifikate.

(A2.3) Der Absender und der Empfänger der Ausschreibungsunterlagen unterstützen das PKCS#7-Format des AVA-Datencontainers.

A3 Geschützter Einsatzbereich

(A3.1) Die Eingabe der Authentisierungsdaten (PIN) des Kartenhalters an die Chipkarte erfolgt nur über die Eingabeschnittstelle des Chipkartenterminals. Der Personalcomputer erhält keine Informationen zu den Authentisierungsdaten, sondern übernimmt nur die Benutzerführung (Aufforderung zur PIN-Eingabe über das Chipkartenterminal und Entgegennahme des Returncodes der Chipkarte).

(A3.2) Der Personalcomputer, auf dem das AVA-Sign Paket eingesetzt wird, läuft unter Microsoft Windows 2000 oder Windows XP. Er ist vor unbefugten Zugriffen aus dem und auf das Internet und ein ggf. angeschlossenes Intranet durch geeignete Massnahmen wie Firewall zu schützen. Die AVA-Sign Software ist auf dem Personalcomputer vor manuellen Zugriffen und Datenaustausch per Datenträger durch Unbefugte zu schützen. Während des Signaturvorganges sollte der Personalcomputer nicht mit dem Inter-/Intranet verbunden sein. Als Einsatzumgebung ist eine geschützte Einsatzumgebung nach Punkt 4.2 gemäß [4] auf einem System mit Microsoft Windows 2000 oder Windows XP vorgesehen.

Der Benutzer hat dafür Sorge zu tragen, dass der Personalcomputer vor unberechtigten Zugriffen Dritter geschützt ist. Das bedeutet, dass mindestens ein Virenscanner mit aktuellen Virensignaturen sowie eine Personal Firewall auf dem Personalcomputer aktiv ist. Der Personalcomputer ist durch Benutzernamen in Verbindung mit einem Passwort ohne Administratorrechte im Normalbetrieb zu schützen. Die in der Benutzer-

dokumentation von AVA-Sign beschriebenen Sicherheitsvorkehrungen werden eingehalten.

(A3.3) Das verwendete Chipkartenterminal muss die sichere PIN–Eingabe über seine Tastatur für die Benutzerauthenisierung und den PIN-Wechsel unterstützen.

(A3.4) Für die Arbeit von AVA-Sign ist zu ermöglichen:

(i) ein Empfang der Ausschreibungsunterlagen,
(ii) ein Senden der Angebotsunterlagen,
(iii) eine Online-Abfrage des Verzeichnisdienstes für die qualifizierten Signaturzertifikate.

3 Sicherheitseigenschaften

3.1 Subjekte / Objekte, Zugriffsarten

Für die Formulierung der Sicherheitseigenschaften des EVG werden folgende Objekte, Subjekte und Zugriffsarten beschrieben.

Objekte

Die vom EVG zu schützenden Objekte umfassen:

- Vergabeunterlagen,
- Vertragsunterlagen und
- Bietererklärungen sowie ggfs. Nebenangebote.

Vergabeunterlagen, Vertragsunterlagen und Bietererklärungen werden von der Vergabestelle an die Bieter gesendet. Diese Objekte werden unter dem Begriff Ausschreibungsunterlagen zusammengefasst (vgl. auch Glossar). Wenn nicht anders erwähnt, meint Ausschreibungsunterlagen insbesondere die Unterlagen, die von der Vergabestelle an den Bieter übermittelt werden.

Die Integrität der Ausschreibungsunterlagen ist vom EVG zu sichern, gegebenenfalls ist zusätzlich die Vertraulichkeit der Daten oder Teile dieser Daten (z.B. der Vergabeunterlagen) zu sichern. Der EVG muss dazu in der Lage sein, gesichert übertragene Daten zu prüfen (Signaturprüfung) und entschlüsseln zu können.

Die Vergabeunterlagen enthalten verbindliche Vertragsbedingungen und können nicht editiert werden. Die Vertragsunterlagen werden vom Bieter bearbeitet und an die Vergabestelle zurückgesendet. Optional können Bieter untereinander Bietererklärungen abgeben und Nebenangebote an die Vergabestelle senden. Für die Evaluierung ist wesentlich, dass solche Daten optional ebenfalls zu schützen sind; das Verfahren ist dabei analog zu den Vertragsunterlagen. Nachdem die Vertragsunterlagen vom Bieter bearbeitet worden sind, werden diese Daten an die Vergabestelle zurückgesendet. Auf dem Übertragungsweg sind diese Daten zu schützen.

Vertragsunterlagen und Bietererklärungen sowie ggfs. Nebenangebote werden unter dem Begriff Angebotsunterlagen zusammengefasst. Wenn nicht anders erwähnt, meint Angebotsunterlagen insbesondere die vom Bieter bearbeiteten und ausgefüllten Unterlagen, die vom Bieter zurück an die Vergabestelle übermittelt werden.

Die Integrität und Vertraulichkeit der Angebotsunterlagen ist vom EVG zu sichern. Der EVG muss dazu in der Lage sein, gesichert zu übertragende Daten zu signieren und zu verschlüsseln. Anmerkung: Eine Signatur kann auch dazu verwendet werden, lokal auf dem PC gespeicherte Daten vor Manipulation zu schützen.

Der EVG verwendet für die Sicherheitsfunktionen zusätzlich folgende Objekte, auf die die unten definierten Subjekte zugreifen können:

Qualifizierte Signaturzertifikate des Kartenhalters und der Absender der Ausschreibungsunterlagen,

Verschlüsselungszertifikate des Kartenhalters und der Empfänger der Ausschreibungsunterlagen.

Subjekte

Für die Formulierung der Sicherheitseigenschaften des EVG werden folgende Subjekte definiert:

(S1) Bearbeiter: eingewiesener Benutzer des EVG, der Angebotsunterlagen aus den Ausschreibungsunterlagen erstellt.

(S2) Kartenhalter: eingewiesener Benutzer des EVG, der durch Kenntnis der Authentisierungsdaten für die Chipkarte zum Signieren der Angebotsunterlagen und zum Entschlüsseln der Ausschreibungsunterlagen autorisiert ist.

Sowohl (S1) als auch (S2) können Signaturen prüfen und Angebotsunterlagen verschlüsseln.

(S3) Absender der Ausschreibungsunterlagen: zum Bereitstellen der Ausschreibungsunterlagen auf dem AVA-Online-Server berechtigter Mitarbeiter der Vergabestelle.

(S4) Empfänger der Angebotsunterlagen: zum Lesen der Angebotsunterlagen auf dem AVA-Online-Server berechtigter Mitarbeiter der Vergabestelle.

(S5) Externer Angreifer: Unbefugter, der versucht, lesenden oder schreibenden Zugang zu den Ausschreibungsunterlagen bzw. Angebotsunterlagen auf dem Übertragungskanal zwischen AVA-Online-Server und AVA-Sign zu erlangen.

(S6) Lokaler Angreifer: Unbefugter, der versucht, auf dem Personalcomputer lesenden oder schreibenden Zugang auf Daten (insbesondere Angebotsunterlagen bzw. Ausschreibungsunterlagen) zu erlangen oder Programme auszuführen.

Zugriffsarten

(ZA1) Eingabe der Authentisierungsdaten zur Benutzung des privaten Signaturschlüssels der Chipkarte (SPIN)

(ZA2) Eingabe der Authentisierungsdaten zur Benutzung des privaten Verschlüsselungsschlüssel der Chipkarte (VPIN)

(ZA3) Prüfen qualifizierter elektronischer Signaturen über den Ausschreibungsunterlagen

(ZA4) Erstellen qualifizierter elektronischer Signaturen über die Angebotsunterlagen

(ZA5) Entschlüsseln der Ausschreibungsunterlagen

(ZA6) Verschlüsseln der Angebotsunterlagen

(ZA7) Bearbeiten der Angebotsunterlagen

3.2 Bedrohungen und Sicherheitsziele

Bedrohungen

B1 Ausschreibungsunterlagen werden auf dem Übertragungskanal vom Auftraggeber zum Bieter durch einen externen Angreifer manipuliert

B2 Vertrauliche Ausschreibungsunterlagen werden auf dem Übertragungskanal vom Auftraggeber zum Bieter durch einen externen Angreifer offenbart

B3 Ausschreibungsunterlagen werden auf dem Personalcomputer durch einen lokalen Angreifer manipuliert

B4 Angebotsunterlagen werden auf dem Personalcomputer durch einen lokalen Angreifer manipuliert

B5 Angebotsunterlagen werden auf dem Übertragungskanal vom Bieter zum Auftraggeber durch einen externen Angreifer manipuliert

B6 Angebotsunterlagen werden auf dem Übertragungskanal vom Bieter zum Auftraggeber für einen externen Angreifer offenbart

B7 die Chipkarte wird nach Authentisierung des Kartenhalters für die Erstellung qualifizierter Signaturen anderer Daten durch einen lokalen Angreifer missbraucht

Sicherheitsziele

Z1 Verfälschungen der Ausschreibungsunterlagen erkennen (Signaturprüfung)
Der EVG ermöglicht es dem Bearbeiter, Verfälschungen der Ausschreibungsunterlagen durch einen externen Angreifer oder einen lokalen Angreifer zu erkennen und unverfälschte Ausschreibungsunterlagen einem Absender zu zuordnen.

Z2 Vertrauliche Ausschreibungsunterlagen lesbar machen (Entschlüsselung)
Der EVG ermöglicht es dem Kartenhalter, vertrauliche Ausschreibungsunterlagen, die vom Absender der Ausschreibungsunterlagen mit AVA-Online verschlüsselt an ihn übersandt wurden, zu entschlüsseln.

Z3 Authentizität der Angebotsunterlagen schützen (Signaturerzeugung)
Der EVG ermöglicht es als Signaturanwendungskomponente, Verfälschungen der durch den Bieter erstellten und für eine Einreichung vorgsehenen Angebotsunterlagen durch eine qualifizierte elektronische Signatur erkennbar zu machen.

Z4 Vertraulichkeit der Angebotsunterlagen vor externen Angreifern schützen (Verschlüsselung)
Der EVG ermöglicht es dem Bearbeiter, die Vertraulichkeit der Angebotsunterlagen vor externen Angreifern zu schützen. Nur der Kartenhalter und die vorgesehenen Empfänger der Angebotsunterlagen sollen die an den AVA-Online-Server versandten Angebotsunterlagen lesen können.

Z5 Schutz vor Mißbrauch
Der EVG verhindert Mißbrauch der Chipkarte nach Authentisierung des Kartenhalters für die Erstellung qualifizierter Signaturen anderer Daten durch einen lokalen Angreifer.

Die angenommenen Bedrohungen korrespondieren mit den Sicherheitszielen des EVG und den Annahmen über die Einsatzumgebung:

	B1	B2	B3	B4	B5	B6	B7
Z1	X		X				
Z2		X					
Z3				X	X		
Z4						X	
Z5							X
A1	(X)		(X)	(X)	(X)		
A2		(X)				(X)	
A3			(X)	(X)			(X)

Tabelle 1: Zusammenhang von Bedrohungen, Sicherheitszielen und Annahmen zur Einsatzumgebung

Legende:

X zeigt in der Tabelle an, dass die Bedrohung durch das Sicherheitsziel des EVG abgewehrt wird,

(X) zeigt in der Tabelle an, dass das Sicherheitsziel des EVG von Sicherheitsvorkehrungen abhängig ist, die in den Annahmen zur Einsatzumgebung dokumentiert sind.

3.3 Sicherheitsfunktionen zur Abwehr der Bedrohungen

Der EVG benutzt für die Ausschreibungsunterlagen und die Angebotsunterlagen ein spezielles Format eines AVA-Datencontainers. Ein AVA-Datencontainer ist eine PKCS#7-codierte Datei mit

(1) einer Liste der vorgesehenen Empfänger und den für sie verschlüsselten Datenschlüsseln,

(2) einer Zip-Datei, die Ausschreibungsunterlagen enthält und verschlüsselt ist.

Die Zip-Datei besteht aus

(1) einer Beschreibungsdatei *content.xml*, die XML-codiert eine Beschreibung der Ausschreibung und des Inhalts der Ausschreibungsunterlagen enthält,

(2) den Dateien der Ausschreibungsunterlagen,

(3) einer oder mehreren digitalen Signaturen eines oder mehrerer Bieter in einem herstellerspezifischen Format als AVA-Multipart-Message über eine Auswahl von Dateien der Ausschreibungsunterlagen.

Die digitale Signatur einer AVA-Multipart-Message kann im S/MIME-Format exportiert werden.

F1 Signaturprüfung

Die SSF F1 Signaturprüfung prüft qualifizierte elektronische Signaturen über die AVA-Multipart-Message innerhalb der Zip-Datei. Die SSF F1 Signaturprüfung umfasst für jede Signaturprüfung die Anzeige,

(1) auf welche Dateien innerhalb der Zip-Datei sich die Signatur der AVA-Multipart-Message bezieht,

(2) ob die Dateien der AVA-Multipart-Message insgesamt unverändert sind,

(3) welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,

(4) der Inhalte des qualifizierten Zertifikats, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate,

(5) ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren,

(6) ob die Signaturprüfung korrekt durchgeführt werden konnte.

Der öffentliche Schlüssel der RegTP, der als höchste Stelle für Prüfung der digitalen Signaturen nach dem Kettenmodell verwendet wird, ist im EVG fest kodiert.

Eine Online-Prüfung der Zertifikate in den Verzeichnisdiensten erfolgt auf Anforderung des Benutzers.

Im Rahmen der Signaturprüfung werden die Hashfunktionen SHA-1 und RIPEMD160 unterstützt.

Der Inhalt der signierten Dateien im Textformat kann durch die SSF F5 Sichere Anzeige angezeigt werden.

F2 Unterstützung der Signaturerstellung

Die SSF F2 Unterstützung der Signaturerstellung unterstützt die Erstellung qualifizierter elektronischer Signaturen über die AVA-Multipart-Message innerhalb der Zip-Datei. Die SSF F2 Unterstützung der Signaturerstellung umfasst für jede Signaturerstellung

(1) die Zusammenstellung der AVA-Multipart-Message aus Dateien der Zip-Datei und damit die Anzeige auf welche Dateien sich die zu erstellende Signatur bezieht,

(2) die Berechnung des Hashwerts,

(3) die eindeutige Anzeige der Erzeugung der Signatur durch die Chipkarte,

(4) die Aufforderung zur Authentisierung des Kartenhalters gegenüber der Chipkarte über das Chipkartenterminal,

(5) die Kodierung der AVA-Multipart-Message mit der qualifizierten elektronischen Signatur in der Zip-Datei.

Die SSF F2 Unterstützung der Signaturerstellung berechnet den Hashwert über die in der AVA-Multipart-Message referenzierten Dateien der Zip-Datei gemäß der Hasfunktion SHA-1. Sie selektiert den Signaturschlüssel des Kartenhalters auf der Chipkarte, übergibt den Hashwert an die Chipkarte und erhält die digitale Signatur von der Chipkarte zurück. Sie codiert die AVA-Multipart-Message mit der Signaturinformation mit dem Zertifikat des unterzeichnenden Kartenhalters und der digitalen Signatur im S/MIME-Format.

Die Erzeugung der digitalen Signatur durch die Chipkarte erfordert die erfolgreiche Authentisierung des Kartenhalters gegenüber der Chipkarte über das Chipkartenterminal sowie die Verwendung des privaten Signaturschlüssels zur Erstellung der digitalen Signatur. Diese Funktionen der sicherheitsbestätigten Signaturkomponenten in der IT-Umgebung des EVG werden durch SSF F2 Unterstützung der Signaturerstellung genutzt.

Der Inhalt der zu signierenden Dateien im Textformat kann durch die SSF F5 Sichere Anzeige angezeigt werden.

F3 Entschlüsseln

Die SSF F3 Entschlüsseln entschlüsselt die Zip-Datei innerhalb des AVA-Datencontainer in folgenden Schritten:

(1) der AVA-Datencontainer wird entsprechend dem PKCS#7-Format decodiert,

(2) der Datenschlüssel in der Empfängerliste des AVA-Datencontainer wird mit dem privaten Verschlüsselungsschlüssel in der Chipkarte des Kartenhalters entschlüsselt,

(3) die Zip-Datei des AVA-Datencontainers wird mit 3-Schlüssel-Triple-DES im CBC-Mode entschlüsselt,

(4) der erhaltene Klartext der Zip-Datei wird lokal gespeichert.

Die Entschlüsselung des Datenschlüssels durch die Chipkarte erfordert die erfolgreiche Authentisierung des Kartenhalters gegenüber der Chipkarte über das Chipkartenterminal sowie die Verwendung des privaten Verschlüsselungsschlüssels zur Entschlüsselung. Diese Funktionen der Chipkarte und des Chipkartenterminals in der IT-Umgebung des EVG werden durch SSF F3 Entschlüsseln genutzt.

F4 Verschlüsseln

Die SSF F4 Verschlüsseln verschlüsselt die Zip-Datei innerhalb des AVA-Datencontainer in folgenden Schritten:

(1) Bildung eines Datenschlüssels mit 168 Bit für die Verschlüsselung mit 3-Schlüssel-Triple-DES CBC und eines Initialisierungsvektors mit einem Zufallsgenerator,

(2) Generierung der Liste berechtigter Empfänger durch manuelle Auswahl bzw. Übernahme aus den Vergabeunterlagen mit den Geheimtexten des Datenschlüssels, der mit den öffentlichen Verschlüsselungsschlüsseln aus den Verschlüsselungs-Zertifikaten der berechtigten Empfänger verschlüsselt wird,

(3) Verschlüsselung der Zip-Datei mit dem Datenschlüssel mit 3-Schlüssel-Triple-DES im CBC-Mode,

(4) Kodierung des AVA-Datencontainer im PKCS#7 Format.

F5 Sichere Anzeige

Die SSF F5 Sichere Anzeige interpretiert Dateien mit Text-Erweiterung entsprechend ISO8859-1 und zeigt diese vollständig und eindeutig an. Diese Anzeige schließt verdeckten Text oder die Anzeige in Abhängigkeit von den Einstellungen des Darstellungsprogramms (d. h. aktive Inhalte) aus, d.h., es gibt keinen verdeckten Text; sämtlicher Text wird eindeutig angezeigt. Damit kann der Unterzeichner diese Daten als Teil der zu unterzeichnenden Daten zweifelsfrei erkennen.

F6 Umgebungskontrolle

Die Sicherheitsvorkehrungen der SSF F6 Umgebungskontrolle sollen in der Kombination mit Sicherheitsvorkehrungen der Einsatzumgebung potentielle Angriffe auf den EVG mit hoher Sicherheit abwehren (vgl. auch A3: Geschützter Einsatzbereich). Diese Sicherheits-vorkehrungen umfassen

(1) eine Prüfung der Integrität des EVG bei Inbetriebnahme und Programmstart,

(2) die Feststellung von Manipulationen am Hashwert bei der Übertragung an die Chipkarte.

3.4 Sicherheitsmechanismen

M1 Hashwertberechnung

Der Sicherheitsmechanismus M1 implementiert die Hashfunktion SHA-1 gemäß FIPS 180-2 [7] oder RIPEMD-160. Er wird für die Sicherheitsfunktionen F1 Signaturprüfung und die F2 Unterstützung der Signaturerstellung benutzt.

M2 Prüfung digitaler Signatur

Der Sicherheitsmechanismus M2 prüft digitale Signaturen gemäß PKCS#1 v1.5 [9][3], Abschnitt 8.2.2.

M3 Pseudozufallsgenerator

Der Sicherheitsmechanismus M3 implementiert einen deterministischen Zufallsgenerator.

M4 Triple-DES

Der Sicherheitsmechanismus M4 implementiert den 3-Schlüssel-Triple-DES gemäß [8].

M5 Anzeige

Der Sicherheitsmechanismus M5

(a) ermöglicht eine Auswahl einer Datei mit TXT-Dateierweiterung im AVA-Datencontainer,

(b) zeigt in einem gesonderten Fenster den Dateiort, den Dateinamen und die enthaltenen Daten nach ISO8859-1 an.

3.5 Zweckmäßigkeit der Sicherheitsfunktionen/-mechanismen

Das Ergebnis der Zweckmäßigkeitsuntersuchung ist in der folgenden Tabelle dargestellt. In jeder Tabellenzelle kennzeichnet ein Kreuz „X“ die den Bedrohungen entgegenwirkenden Funktionen. Die Abwehr der Bedrohung erfolgt im Sinne der Sicherheitsziele des EVG.

[3] Hinweis: Das Dokument [9] spezifiziert sowohl die Version 2.1 des Standards (relevante Teile dazu finden sich in Abschnitt 8.1) als auch die ältere Version 1.5 (vgl. Abschnitt 8.2).

	F1 Signatur-prüfung	F2 Unterstüt-zung der Signatur-erstellung	F3 Entschlüs-seln	F4 Verschlüs-seln	F5 Sichere Anzeige	F6 Umgebungs-kontrolle
B1	X					
B2			X			
B3	X					
B4	X	X				
B5		X				
B6				X		
B7					X	X

Tabelle 2: Wirksamkeit der Sicherheitsfunktionen zur Abwehr der Bedrohungen

Die Bedrohung **B1** (Manipulation der Ausschreibungsunterlagen auf dem Übertragungsweg) wird durch die Prüfung der elektronischen Signatur über den Ausschreibungsunterlagen durch die Sicherheitsfunktion F1 Signaturprüfung erkannt. Dadurch wird die Integrität der empfangenen Ausschreibungsunterlagen im Sinne des Sicherheitsziels Z1 erkannt.

Hinweis: Unter der Annahme A2 unterstützt auch die verschlüsselte Übertragung der Ausschreibungsunterlagen die Abwehr der Bedrohung B1, da eine zielgerichtete Manipulation im CBC-Mode verschlüsselter Daten zusätzlich erschwert ist. In diesem Fall muss die Verschlüsselung durch die Umgebung geleistet werden.

Die Bedrohung **B2** (Offenbarung der Ausschreibungsunterlagen auf dem Übertragungsweg) wird durch die verschlüsselte Übertragung zwischen dem Absender (unter der Annahme A2) und dem Empfänger unter Nutzung der Sicherheitsfunktion F3 Entschlüsseln gewährleistet. Die Sicherheitsfunktion F3 Entschlüsseln macht die verschlüsselten Ausschreibungsunterlagen dem Bieter entsprechend Sicherheitsziel Z2 lesbar.

Die Bedrohung **B3** (Manipulation der Ausschreibungsunterlagen auf dem lokalen Rechner) kann ebenso wie die Bedrohung B1 mit Hilfe der Prüfung der elektronischen Signatur über den Ausschreibungsunterlagen durch die Sicherheitsfunktion F1 Signaturprüfung erkannt werden.

Die Bedrohung **B4** (Manipulation der Angebotsunterlagen auf dem lokalen Rechner) kann mit Hilfe der Prüfung der (mittels F2) selbst erstellten elektronischen Signatur über den Angebotsunterlagen durch die Sicherheitsfunktion F1 Signaturprüfung erkannt werden.

Hinweis: Die Sicherheitsfunktion F5 Sichere Anzeige ermöglicht dem Bieter seine TXT-Dateien visuell vor und nach der Signaturerstellung zu prüfen. Die Sicherheitsfunktion F6 Umgebungskontrolle kontrolliert den Transport des Hashwerts der zu signierenden Daten auf dem Weg von AVA-Sign zur Chipkarte im Signierprozess der Sicherheitsfunktion F2 Unterstützung der Signaturerstellung. Beide Funktionen wirken zwar auch hier unterstützend, werden aber im Zusammenhang mit Bedrohung B7 diskutiert.

Die Bedrohung **B5** (Manipulation der Angebotsunterlagen auf dem Übertragungskanal) wird mit Hilfe der Prüfung (durch den Empfänger) der elektronischen Signatur über die Angebotsunterlagen durch die Sicherheitsfunktion F2 Unterstützung der Signaturerstellung abgewehrt, da Manipulationen für den Empfänger gemäß Annahme A1 erkannt werden können.

Die Bedrohung **B6** (Offenbarung der Angebotsunterlagen auf dem Übertragungskanal) wird durch die Verschlüsselung der Angebotsunterlagen mit der Sicherheitsfunktion F4 Verschlüsseln in Verbindung mit der Annahme A2 ausgeschlossen.

Die Sicherheitsfunktion F6 Umgebungskontrolle stellt Manipulationen am Hashwert bei der Übertragung an die Chipkarte fest. In Verbindung mit der Annahme A3 verhindert sie so eine Erstellung qualifizierter Signaturen über andere als vom Kartenhalter gewollte Daten durch einen lokalen Angreifer (Bedrohung **B7**). Die Sicherheitsfunktion F5 Sichere Anzeige verhindert, dass Daten falsch angezeigt werden, so dass der Kartenhalter fälschlicherweise einer Signaturerstellung zustimmt (möglicherweise wird er über den Inhalt des von ihm zu signierenden Textes getäuscht).

Den sicherheitsspezifischen Funktionen F1 bis F6 sind folgende Mechanismen M1 bis M5 zugeordnet:

	M1 Hashwert-berechnung	M2 Prüfung digitaler Signatur	M3 Pseudo-zufalls-generator	M4 Triple-DES	M5 Anzeige
F1 Signaturprüfung	x	x			
F2 Unterstützung der Signaturerstellung	x				
F3 Entschlüsseln				x	
F4 Verschlüsseln			x	x	
F5 Sichere Anzeige					x
F6 Umgebungs-kontrolle	x	x			

Tabelle 3: Zuordnung Sicherheitsfunktionen und Sicherheitsmechanisemn

Diese Zuordnung begründet sich wie folgt. Die SSF F1 benötigt für die korrekte Umsetzung die Mechanismen M1 und M2. Für die SSF F2 wird nur der Mechanismus M1 benötigt, die weitere Umsetzung erfolgt durch externe Sicherheitsmassnahmen der Chipkarte. SSF F3 wird durch M4 realisiert, die weitere Umsetzung erfolgt durch externe Sicherheitsmassnahmen der Chipkarte. Die Umsetzung der SSF F4 erfolgt durch die Mechanismen M3 und M4. Der Mechanismus M5 ermöglicht die SSF F5. SSF F6 wird durch die Mechanismen M1 und M2 sichergestellt.

4 Evaluationsstufe und die Mechanismenstärke

Die angestrebte Evaluierungsstufe ist E2.

Die Stärke der Mechanismen vom ITSEM-Typ A soll mindestens „hoch“ sein.

5 Anhang

5.1 Glossar

Ausschreibungsunterlagen	Oberbegriff für Angebotsunterlagen und Vergabeunterlagen; wenn nicht anders erwähnt, meint Ausschreibungsunterlagen insbesondere die Unterlagen, die von der Vergabestelle an den Bieter übermittelt werden.
Angebotsunterlagen	Oberbegriff für vom Bieter zu bearbeitete Bietererklärungen und Vertragsunterlagen, deren Vertraulichkeit und Integrität zu schützen sind; wenn nicht anders erwähnt, meint Angebotsunterlagen insbesondere die vom Bieter bearbeiteten und ausgefüllten Unterlagen, die vom Bieter zurück an die Vergabestelle übermittelt werden.
Vergabeunterlagen	Werden von der Vergabestelle herausgegeben. Auf Grund der Vergabeunterlagen wird das / werden die Angebote in Form von Vertragunterlagen erstellt.
Vertragsunterlagen	Dies sind Daten, die der Bieter als Angebot bei der Vergabestelle einreicht. Vertragsunterlagen setzen rechtlich und inhaltlich auf den Vergabeunterlagen auf.
Geschützter Einsatzbereich	Einsatzumgebung für die Signaturanwendungskomponente gemäß [4], bei der potentielle Bedrohungen über das Internet, ein angeschlossenes Intranet, einen manuellen Zugriff Unbefugter und Datenaustausch per Datenträger durch eine Kombination von Sicherheitsvorkehrungen in der Signaturanwendungskomponente selbst und der Einsatzumgebung mit hoher Sicherheit abgewehrt werden. Die EVG-spezifischen Anforderungen an die Anwendungsumgebung des geschützten Bereichs sind Abschnitt AR 5.1.1 definiert.
Isolierter Einsatzbereich	Die Signaturanwendungskomponente wird in einer „Signatur-Arbeitsstation“ eingesetzt, bei der gegenüber den potentiellen Bedrohungen folgender Schutz besteht: Es erfolgt *zu keinem Zeitpunkt* eine *Anbindung an* ein *Kommunikationsnetz* und in der *Einsatzumgebung* sind *Sicherheitsvorkehrungen* vorhanden, die potentielle Angriffe über manuellen

	Zugriff Unbefugter/Datenaustausch per Datenträger mit hoher Sicherheit abwehren. Die EVG-spezifischen Anforderungen an die Anwendungsumgebung des isolierten Bereichs sind Abschnitt 5.3 Pkt. 4 definiert.
Terminal Klasse 1	Physikalische Schnittstelle bereitstellen
Terminal Klasse 2	Physikalische Schnittstelle bereitstellen + Tastatur
Terminal Klasse 3	Physikalische Schnittstelle bereitstellen + Tastatur + Anzeige
Bedienerführung	Aufforderung zu Benutzeraktivitäten
Benutzereingabe-schnittstelle	Tastatur für PIN-Eingabe
GAEB - Datei	„Gemeinsamer Ausschuss für Elektronik im Bauwesen“ Standardformat für Leistungsverzeichnisse

Die Begriffe „Auftraggeber“ und „Vergabestelle“ werden synonym verwendet und bezeichnen den Betreiber des AVA-Online-Servers. Die Begriffe „Bearbeiter“ und „Bieter“ werden ebenfalls synonym verwendet und bezeichnen den Nutzer des AVA-Sign-Pakets.

5.2 Abkürzungen

AR	Architekturentwurf
FE	Feinentwurf
SIK	Sicherheitsirrelevante Komponente (AR, FE: „andere Komponente“)
SPIN	Authentisierungsdaten für den privaten Signaturschlüssel auf der Chipkarte
SRF	Sicherheitsrelevante Funktion
SRK	Sicherheitsrelevante Komponente
SSF	Sicherheitsspezifische Funktion
SSK	Sicherheitsspezifische Komponente
SV	Sicherheitsvorgaben
TE	Implementierung, Test
VPIN	Authentisierungsdaten für den privaten Verschlüsselungsschlüssel auf der Chipkarte

5.3 Literatur

[1] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC). Vorläufige Form der harmonisierten Kriterien. Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, Juni 1991

[2] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz SigG), Artikel 1 in „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“, 16. Mai 2001, Bundesgesetzblatt vom 21. Mai 2001

[3] Verordnung zur digitalen Signatur (Signaturverordnung - SigV) in der Fassung des Beschlusses der Bundesregierung vom 16. November 2001

[4] Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten - Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen, RegTP Version 1.0, Stand: 30.01.2002

[5] Geeignete Kryptoalgorithmen 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, Regulierungsbehörde für Telekommunikation und Post (RegTP), 21.01.2003

[6] Anwendungshinweise und Interpretationen zum Schema, AIS20, Version 1, 2.12.1999, Bundesamt für Sicherheit in der Informationstechnik

[7] Federal Information Processing Standards Publication 180-2 Secure Hash Standard, NIST, 2002 August 1

[8] FIPS PUB 46-3 Federal Information Processing Standards Publication Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. Department Of Commerce/National Institute of Standards and Technology

[9] PKCS #1 v2.1: RSA Cryptographic Standard, 14.6.2002.

Ende der Sicherheitsvorgaben zu
„AVA-Sign Version 2.1“.

(Diese Seite ist beabsichtigterweise leer.)

Zertifizierungsreport T-Systems-DSZ-ITSEC-04097-2003

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