Sicherheitsvorgaben (ST)

T-TeleSec Signet 1.6.0.4 mit T-TeleSec Signet Patch 1.6.0.6

Version 1.5

Dokumentenversion	**Datum**	**Autor**	**Anmerkungen**
1.5	17.05.2006	Armin Lunkeit	Anpassung Beschreibung Auslieferung

Inhaltsverzeichnis

Tabellenverzeichnis

Glossar und Abkürzungsverzeichnis

CC	Common Criteria. Bedeutet Allgemeine Kriterien, wird als Gemeinsame Kriterien für Prüfung und Bewertung der Sicherheit von Informationstechnik in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik verlegt.
CRL	Certificate Revocation List. Eine CRL ist eine Liste mit gesperrten Zertifikaten, die eine Negativprüfung von Zertifikaten ermöglicht.
CSP	Cryptographic Service Provider. Microsoft stellt einen Mechanismus zur Realisierung einer eigenen Sicherheitsinfrastruktur auf Basis der CSPs zur Verfügung. Mit diesem Mechanismus ist es Applikationen sowohl möglich, CSPs, die vom Betriebssystem zur Verfügung gestellt werden, für kryptografische Operationen zu nutzen als auch die Realisierung eigener CSPs vorzunehmen und diese dem Betriebssystem zur Verfügung zu stellen. CSPs können verschiedene Aufgaben wahrnehmen, der T-TeleSec Signet CSP wurde zur Erzeugung elektronischer Signaturen im Kontext des Betriebssystems entwickelt.
CTL	Certificate Trust List. Ist eine Zertifikatsvertrauensliste.
EVG	Evaluationsgegenstand
OCSP	Online Certificate Status Protocol. Dies ist ein Mechanismus der eine Positiv-Abfrage zu einem gegebenen Zertifikat ermöglicht.
SOF	Strength of Function – Stärke der Funktion.
SSCD	Secure Signature Creation Device. Unter einem SSCD wird ein Gerät verstanden, mit dem es möglich ist, auf sichere Art und Weise eine elektronische Signatur zu erzeugen.

1 ST-Einführung

1.1 ST-Identifikation

Titel:	Sicherheitsvorgaben (ST) T-TeleSec Signet 1.6.0.4 Maintained
Autor:	Armin Lunkeit
CC-Version:	Version 2.1, August 1999
Status:	Final

Als zusätzliches Dokument wurden die Anwendungshinweise und Interpretationen zum Schema (AIS 32, Version 1), herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik verwendet.

Stand AIS: 02.07.2001
Herausgeber: Zertifizierungstelle des BSI im Rahmen des Zertifizierungsschemas

Dieses Dokument liefert die Sicherheitsvorgaben für das Produkt T-TeleSec Signet 1.6.0.4 mit den Änderungen, die durch das Anwenden des Patches T-TeleSec Signet Patch 1.6.0.6 an dem Produkt vorgenommen werden.

1.2 ST-Übersicht

Die Applikation T-TeleSec Signet 1.6 ist eine modulare Client Applikation zur Erzeugung und Verifikation elektronischer Signaturen auf Microsoft Windows Systemen ab Windows 98. In der Sicherheitsumgebung der Applikation werden eine Smartcard und ein Kartenleser mit sicherer Pin-Eingabe benötigt, um die kryptografischen Operationen zur Signaturerzeugung und Verifikation auf sichere Art und Weise durchzuführen. Die Applikation T-TeleSec Signet 1.6 kann sowohl einfache, fortgeschrittene und qualifizierte elektronische Signaturen erzeugen. Grundlage für die qualifizierte elektronische Signatur sind das Signaturgesetz (SigG) und die Signaturverordnung (SigV).

Die Applikation selbst beschränkt sich auf die Erzeugung von kryptografischen Prüfsummen (Hashwerten) nach den Algorithmen SHA1 und RIPE MD 160 und kann somit die Integrität und Vertrauenswürdigkeit signierter Daten gemeinsam mit den Komponenten für Sperrlistenprüfung, OCSP-Abfrage und gesicherter Anzeigeeinheit für TIFF und Text Dokumente sicherstellen.

Dieses Dokument wurde auf Basis der Sicherheitsvorgaben für das nach bereits nach Common Criteria mit Prüfniveau EAL 3+ evaluierte und zertifizierte Produkt erstellt. Das vorliegende Dokument ist identisch mit den bereits erstellten Sicherheitsvorgaben, allerdings wird mit diesem Dokument das Produkt T-TeleSec Signet 1.6.0.4 nach Anwendung des Patches T-TeleSec Signet Patch 1.6.0.6 referenziert. Der Hersteller liefert einen entsprechenden Impact Analysis Report um die Änderungen zu beschreiben, die durch den Patch an dem Produkt vorgenommen werden.

1.3 Postulat der Übereinstimmung mit den CC

Der EVG T-TeleSec Signet 1.6 ist konform zu:

Teil 2 der Common Criteria 2.1, Stand August 1999

Zur Formulierung der funktionalen Anforderungen an den EVG werden funktionale Komponenten aus Teil 2 der Common Criteria genutzt. Zusätzlich wurden Erweiterungen nach den Vorgaben der CC definiert, um die funktionalen Anforderungen an den EVG vollständig zu formulieren.

Teil 3 der Common Criteria 2.1, Stand August 1999

Zur Formulierung der Anforderungen an die Vertrauenswürdigkeit des EVGs werden ausschließlich Vertrauenswürdigkeitskomponenten aus Teil 3 genutzt. Die Anforderungen an die Vertrauenswürdigkeit entsprechen der Vertrauenswürdigkeitsstufe EAL 3 mit Zusatz ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 und AVA_VLA.4.

Die Stärke der verwendeten Mechanismen ist SOF hoch.

1.4 Postulat der Übereinstimmung mit SigG und SigV

Der Hersteller postuliert, dass das Produkt T-TeleSec Signet 1.6 konform zum Signaturgesetz (SigG) §17 Absatz 2 ist. Weiterhin postuliert der Hersteller, dass das Produkt T-TeleSec Signet 1.6 konform zu §15 Absatz 2 und Absatz 4 der Signaturverordnung ist.

2 EVG-Beschreibung

Die Applikation T-TeleSec Signet 1.6 besteht aus mehreren Komponenten, die in der folgenden Auflistung aufgeführt werden:

- T-TeleSec Signet Basiskomponenten für die Erzeugung und Verifikation elektronischer Signaturen (T-TeleSec Signet Manager).
- T-TeleSec Signet Viewer zur Visualisierung von zu signierenden Dokumenten und zur Anzeige signierter Dokumente auf Text und TIFF Basis.
- T-TeleSec Crypto-Service-Provider zum Einsatz mit Microsoft Outlook und Microsoft Outlook Express.
- T-TeleSec Signet Shell Extension zur Erweiterung der Funktionen der Microsoft Explorer Kontextmenüs.
- T-TeleSec Signet Integritätscheck zur Überprüfung der Integrität der installierten Software auf dem Rechner des Anwenders.

Das Produkt T-TeleSec Signet 1.6 ist eine Anwendung, die zur Erzeugung und Verifikation elektronischer Signaturen durch den Inhaber eines Signaturzertifikates bestimmt ist. Das Produkt kann einfache, fortgeschrittene und qualifizierte elektronische Signaturen erzeugen. Der Benutzer arbeitet mit verschiedenen grafischen Schnittstellen, die als Produktbestandteile dem Benutzer den Zugang zu den Sicherheitsfunktionen des Produktes erlauben. Als Anwendungsbereich ist sowohl der Einsatz durch den Heimanwender als auch der Einsatz in größeren Infrastrukturen, z.B. im behördlichen Umfeld, anzusehen.
Durch die T-TeleSec Signet Shell Extension wird die nahtlose Integration des Produktes in den Kontext des Microsoft Explorers vorgenommen, die sichere Anzeigeeinheit (T-TeleSec Signet Viewer) stellt die Funktionen einer Betrachtung und Untersuchung der zu signierenden bzw. signierten TIFF- und Textdokumente zur Verfügung. Der T-TeleSec CSP erlaubt die Integration von Signaturmechanismen in die Umgebung eines E-Mail Clients und damit verbunden die Verwendung einer Smartcard für E-Mail Signaturen.

2.1 T-TeleSec Signet Manager

Der T-TeleSec Signet Manager ist das Kernstück der Applikation T-TeleSec Signet 1.6 und stellt die folgenden Funktionen zur Verfügung:

- Errechnung kryptografischer Prüfsummen (Hashwerte) nach den Algorithmen SHA1 und RIPE MD 160.
- Erzeugung elektronischer Signaturen auf Basis einer Smartcard und eines Kartenterminals mit sicherer Pin-Eingabe.
- Verifikation einer elektronischen Signatur, inklusive Prüfung der Zertifikatskette (Sperrlisten und OCSP sind ebenfalls enthalten).
- Bereitstellung eines API für aufsetzende Komponenten.
- Verifikation und Verwaltung von dynamischen Bibliotheken des EVGs.

Der T-TeleSec Signet Manager erzeugt PKCS#7 codierte Dokumente und erlaubt über dieses Format, dass auch andere Applikationen, welche ebenfalls das PKCS#7 Format beherrschen, mit den erzeugten Dokumenten umgehen können.
Je nach Treibermodell des Herstellers wird für die sichere PIN-Eingabe die CT-API, eine separate Secure-Pin-Entry DLL oder das PC/SC Interface[1] verwendet. Der T-TeleSec Signet Manager kann die folgenden Kartenterminals verwenden:

- Cherry SmartBoard G83-6700
- SC Microsystems SPx32/ChipDrive PinPad
- Reiner SCT CyberJack e-com Version 2.0
- Reiner SCT CyberJack pinpad Version 2.0

Die folgenden Smartcards können mit dem T-TeleSec Signet Manager verwendet werden:

- TeleSec E4Netkey Karte
- OpenLimit Karte als spezielle Konfiguration einer TeleSec E4NetKey-Karte
- TeleSec PKS Karte

[1] Unabhängig von der gewählten Methode erfolgt die Pin Eingabe am Kartenterminal. Da bisher keine einheitlichen Standards für die sichere Pin-Eingabe an einem Kartenterminal existieren, ist die gewählte Methode vom eingesetzten Kartenleser abhängig.

Bei den verwendeten peripheren Komponenten werden ausschliesslich im Sinne des SigG bestätigte Komponenten verwendet, die zugehörigen Zertifikate für diese Produkte können von den Seiten der RegTP bezogen werden (www.regtp.de).

Der T-TeleSec Signet Manager ist als ausführbare Datei realisiert und wird beim Start des Betriebssystems ebenfalls gestartet. Der T-TeleSec Signet Manager unterstützt die in den Annahmen zur Sicherheitsumgebung angegebenen Betriebssysteme.

Die Negativprüfung von Zertifikaten erfolgt in T-TeleSec Signet 1.6 über Sperrlisten. Bei jeder Verwendung einer Sperrliste wird deren Integrität an Hand ihrer Signatur und an Ihrem korrekten Aufbau überprüft. Für die Verwendung einer Sperrliste zur Prüfung einer Signatur zum Zeitpunkt der Signaturerstellung wird die geeignete Sperrliste einer Konfiguration entnommen[2]. Delta Sperrlisten werden zum jetzigen Zeitpunkt noch nicht verarbeitet. Das Modul zur Abfrage von Sperrlisten von den jeweiligen Sperrlisten Verteilungspunkten wird ebenfalls vom T-TeleSec Signet Manager verwaltet. Für den Empfang einer Sperrliste können sowohl das http Protokoll als auch das LDAP Protokoll verwendet werden. Nach Ende der Sperrlisten-Prüfung wird dem Nutzer ein eindeutiger Text angezeigt, der ihn über den Status des Zertifikats informiert.
Kann die angeforderte Sperrliste nicht heruntergeladen werden oder tritt ein anderer Fehler während des Herunterladens auf, wird der Nutzer ebenfalls informiert.

Zusätzlich zur Sperrlisten-Prüfung, die vom T-TeleSec Signet Manager immer vorgenommen wird, hat der Benutzer die Möglichkeit, den Status eines Zertifikates durch eine OCSP-Abfrage zu ermitteln. Dieser Mechanismus setzt voraus, dass in dem verwendeten Zertifikat eine Adresse für eine OCSP-Abfrage enthalten ist. Für eine OCSP-Abfrage wird das http Protokoll verwendet, wobei eine Internet Verbindung des Rechners vorausgesetzt wird.

[2] Bei der Signaturprüfung wird über das verwendete Signaturzertifikat ermittelt, ob eine direkte oder eine indirekte Sperrliste existiert. Diese Unterscheidung wird an Hand des Eintrages CRLDistributionPoint.CRLIssuer vorgenommen. Die Konfigurationsdatei für die Sperrlistenprüfung enthält den SHA1 Hashwert des Herausgeberzertifikates des Sperrlistenherausgebers und diesem zugeordnet den Namen der lokalen Sperrlistendatei. Jetzt ist die Sperrlistendatei als Name bekannt und kann syntaktisch geprüft und zur Zertifikatsprüfung verwendet werden. Die Prüfung der Sperrliste umfasst ebenfalls die Prüfung der Sperrlistensignatur.

Nach Ende der Abfrage wird dem Nutzer eine eindeutiger Text angezeigt, der ihn über den Status des Zertifikats informiert. Konnte die Abfrage nicht durchgeführt werden oder ist ein Fehler während der Abfrage aufgetreten, wird der Nutzer darüber ebenfalls informiert.

Der T-TeleSec Signet Manager realisiert eine zentrale Verwaltung aller benötigten Module für die Applikation T-TeleSec Signet 1.6. Textmeldungen, die im Zusammenhang mit der Erzeugung oder Prüfung elektronischer Signaturen im Zusammenhang stehen, werden ebenfalls direkt vom T-TeleSec Signet Manager verwaltet.

Die Abgrenzung des T-TeleSec Signet Manager in seiner Systemumwelt ist in der folgenden Liste abgebildet:

- Treiber des PC/SC Subsystems und der speziellen DLLs für die sichere Pin-Eingabe des jeweiligen Terminalherstellers (jeweilige CT-API des Herstellers).
- Funktionen des Betriebssystems für die Erzeugung grafischer Fenster und Dialoge.
- Funktionen des Betriebssystems für die TCP/IP basierte Kommunikation (Sockets).
- Funktionen des Betriebssystems für die Arbeit mit dem Dateisystem.
- Funktionen des Betriebssystems für die Arbeit mit dem öffentlichen Zertifikatsspeicher des Betriebssystems.
- COM Schnittstellen für die Kommunikation zwischen den Applikationsbestandteilen. Über eine COM-Schnittstelle wird auch das API für die Verwendung des T-TeleSec Signet Manager durch weitere Applikationsbestandteile realisiert.

Der T-TeleSec Signet Manager stellt den weiteren Applikationsbestandteilen eine einzige Schnittstelle auf Basis der Microsoft COM Mechanismen zur Verfügung. Diese Schnittstelle wird als T-TeleSec Signet Job Interface bezeichnet und stellt eine API für die Erzeugung und Verifikation elektronischer Signaturen zur Verfügung.

2.2 T-TeleSec Signet Viewer (sichere Anzeigeinheit)

Der T-TeleSec Signet Viewer ist eine gesicherte Anzeigeeinheit für die Anzeige von zu signierenden Inhalten oder bereits signierten Inhalten nach §15, Absatz 2 der SigV.

Der T-TeleSec Signet Viewer stellt Mechanismen zur Verfügung, um Dokumente im TIFF und Text Format in einer gesicherten Umgebung anzuzeigen und bei Bedarf vom T-TeleSec Signet Manager signieren oder die anhängige Signatur verifizieren zu lassen.

Zur Sicherstellung der korrekten Anzeige der Dokumente und zur Vermeidung unerwünschter Manipulationen werden TIFF oder Text Dokumente beim Öffnen durch den T-TeleSec Signet Viewer einer syntaktischen Prüfung unterzogen und der Nutzer darauf hingewiesen, wenn unbekannte Tags oder Steuerzeichen in dem Dokument enthalten sind, die von der Anzeigeeinheit nicht richtig dargestellt oder interpretiert werden können. Dieser Mechanismus stellt für den Benutzer sicher, dass keine Inhalte elektronisch signiert werden, denen der Nutzer nicht ausdrücklich vertraut.

TIFF Dokumente können als zusätzliche Option gedreht und gespiegelt dargestellt werden, wobei diese Funktionen nicht der Bildbearbeitung dienen, sondern dem Benutzer die Möglichkeit einräumen sollen, das Dokument genauer zu betrachten. Weiterhin können die Seiten verkleinert und vergrößert dargestellt werden, wobei insbesondere die Darstellung mit Originalauflösung sowie eine pixelgenaue Darstellung des Dokuments möglich ist.

Bei der Darstellung von Textdokumenten erfolgt die Textdarstellung fortlaufend und es erfolgt keine Transformation des Dokuments in bestimmte Dokumentgrößen (z.B. DIN A3 oder A4). Zur sicheren Darstellung des Dokuments wird dieses in eine Bitmap transformiert und dargestellt, wodurch die Verwendung eines leicht manipulierbaren Text-Controls vollständig entfallen kann.

Der T-TeleSec Signet Viewer bietet keine Möglichkeiten zur Bildmanipulation, es wird lediglich die Möglichkeit zur Betrachtung der Dokumente eingeräumt.

Die folgenden Schnittstellen werden für die sichere Anzeigeeinheit gegenüber seiner Systemumwelt identifiziert:

- Funktionen des Betriebssystems für die Erzeugung grafischer Fenster und Dialoge.
- Funktionen des Betriebssystems für die Erzeugung geräteunabhängiger Bitmaps.
- Funktionen des Betriebssystems für die Arbeit mit dem Dateisystem.
- COM Schnittstelle des T-TeleSec Signet Manager, um eine elektronische Signatur aus der Anzeigeinheit heraus zu verifizieren oder zu erzeugen.

2.3 T-TeleSec Signet Integritätscheck

Auf der Installations CD befindet sich ein ausführbares Programm, welches auf Anforderung des Nutzers die Integrität des EVGs nach erfolgter Installation sicherstellt. Wann und wie häufig der Benutzer die Integrität zu prüfen hat ist in der Benutzerdokumentation dargelegt. Diese Applikation überprüft, ob die Programmdateien des EVGs auf dem Rechner des Anwenders noch den Programmdateien des EVGs entsprechen, die bei der Installation auf den Rechner des Anwenders installiert wurden.

Dazu wird die Prüfung in zwei Schritten vorgenommen: Im ersten Schritt wird die Signatur der jeweiligen Programmdatei gegen den Hashwert, den das Prüfprogramm für diese Bibliothek berechnet hat, verifiziert. Kann die elektronische Signatur an der jeweiligen Programmdatei nicht verifiziert werden, wird der Anwender über diesen Zustand mit einer Textmeldung innerhalb des Prüfprogramms informiert. Weiterhin werden die auf dem Rechner des Anwenders bei der Installation abgelegten Stammzertifikate überprüft, da der EVG diesen explizit vertraut. Dabei sind der Prüfsoftware die ausgelieferten Stammzertifikate bekannt und die auf dem Rechner des Anwenders vorhandenen Zertifikate werden einem binären Vergleich mit denen, die der Prüfsoftware bekannt sind, verglichen. Schlägt der binäre Vergleich eines Zertifikates fehl, wurde dies geändert. Sind in dem Verzeichnis mehr Zertifikate vorhanden als bei der Installation ausgeliefert, wurde mindestens ein Stammzertifikat hinzugefügt, welches nicht mit dem EVG ausgeliefert und auf dem Rechner des Anwenders installiert wurde. In diesem Falle wird der Benutzer mit einer Textmeldung auf diesen Zustand hingewiesen. Die Textmeldung wird innerhalb des Programms angezeigt, es wird nicht die gesicherte Anzeigeeinheit verwendet, da diese manipuliert sein könnte.

Die folgenden Schnittstellen werden für den T-TeleSec Signet Integritätscheck gegenüber seiner Systemumwelt identifiziert:

- Funktionen des Betriebssystems für die Erzeugung grafischer Fenster und Dialoge
- Funktionen des Betriebssystems für die Arbeit mit dem Dateisystem

2.4 Shell Extension und CSP

Die beiden Komponenten T-TeleSec Signet Shell Extension und T-TeleSec Cryptographic Service Provider sind indirekte Schnittstellen auf die Sicherheitsfunktionen des T-TeleSec Signet Managers. Über eine Schnittstelle haben diese beiden Komponenten die Möglichkeit, Aufrufe zur Signaturerzeugung und Signaturverifikation an den T-TeleSec Signet Manager weiterzuleiten.

Die folgenden Schnittstellen werden für diese beiden Komponenten gegenüber ihrer Systemumwelt identifiziert::

- Funktionen des Betriebssystems für die Erzeugung grafischer Fenster und Dialoge
- Funktionen des Betriebssystems für die Arbeit mit dem Dateisystem
- Die Schnittstelle des T-TeleSec Signet Managers für den Zugang zu den Sicherheitsfunktionen
- Der CSP wird vom Microsoft Crypto API angesprochen, um für das Betriebssystem bestimmte kryptografische Funktionen zu erfüllen (Signaturerzeugung und Signaturverifikation). Daher hat diese Komponente eine Schnittstelle zu Crypto API Mechanismen des Betriebssystems.

2.5 Abgrenzung

Die folgenden Merkmale kann der EVG nicht leisten:

- Sicherstellung des privaten Schlüsselmaterials. Die Sicherstellung der Unversehrtheit und der Geheimhaltung der privaten Schlüssel obliegt der Smartcard.
- Sicherstellung der korrekten Uhrzeit auf dem Rechner des Anwenders. Der EVG enthält keine Mechanismen für die Verwendung von Zeitstempeln und kann auch keine Aussagen über die Plausibilität der eingestellten Uhrzeit.
- Sicherstellung der Integrität des Betriebssystems. Der EVG enthält keine Mechanismen, um die Integrität seiner Umgebung zu überprüfen. Der Anwender muss sicherstellen, dass er geeignete Vorkehrungen trifft, um eine Kompromittierung seines Betriebssystems zu vermeiden.
- Sicherheit der kryptografischen Operationen. Der EVG benutzt Bibliotheken zur Erzeugung elektronischer Signaturen über das RSA Public Key Verfahren. Der EVG kann die Stärke der kryptografischen Mechanismen nicht garantieren und keine Aussagen über die Stärke der kryptografischen Funktionen postulieren.

Die Leistungsmerkmale des EVGs beschränken sich auf die Erzeugung kryptografischer Prüfsummen (Hashwerte) und die Verwendung eines SSCD für die Erzeugung elektronischer Signaturen sowie die Verwendung des RSA Algorithmus für die Verifikation elektronischer Signaturen. Für den Verifikationsprozess werden Sperrlisten verwendet, OCSP Abfragen stehen als Mechanismus ebenfalls zur Verfügung. Der EVG kann Manipulationen an Zertifikatsverzeichnissen ebenso wenig abwehren wie die Protokollierung elektronischer Signaturvorgänge auf dem Rechner des Benutzers.

Evaluiert werden sollen der T-TeleSec Signet Manager mit seinen beschriebenen Funktionen sowie die gesicherte Anzeigeeinheit (T-TeleSec Signet Viewer).

2.6 Lieferumfang

Die T-Systems International GmbH beabsichtigt, den Patch für das Produkt T-TeleSec Signet sowohl per CD als auch per Download an den Endanwender auszuliefern.

Im Regelfall wird dem Endanwender durch die T-Systems eine CD bereitgestellt, die entweder durch persönliche Übergabe oder durch einen Kurierdienst überstellt wird. Soll ein Download erfolgen, wird dem Endanwender ein Nutzername sowie ein Passwort mitgeteilt, mit dem er den Patch aus dem Downloadbereich der Firma OPENLiMiT beziehen kann.

Nach dem Herunterladen des Patches muss der Anwender die Installationsroutine ausführen. Anschließend muss der Patch vom Endanwender installiert werden.

Nach der Installation des Patches muss der Anwender das bereits auf der CD befindliche Integrity Tool ausführen und durch die Ausführung dieses Tools sicherstellen, dass er den korrekten Patch erhalten hat[3].

Die ausgetauschten binären Programmbestandteile des Produktes sind mit dem selben privaten Schlüssel signiert, wie es bei der Programmversion 1.6.0.4 der Fall ist. Da der zugehörige Integritätscheck, welcher bereits auf CD-ROM beim Endanwender vorliegt, die elektronischen Signaturen der Programmbestandteile prüft, ist durch die Ausführung des Integritätschecks sichergestellt, dass der Endanwender den richtigen Patch installiert hat.

[3] Das Originalprodukt wurde an den Endanwender per CD-ROM ausgeliefert. Dieses Lieferverfahren ist in der Sicherheitsvorgabe für das Produkt T-TeleSec Signet 1.6.0.4 beschrieben.

3 EVG-Sicherheitsumgebung

3.1 Annahmen

Es werden folgende Annahmen über die Einsatzumgebung formuliert.

A.Plattform

Der Benutzer verwendet als Hardwareplattform einen Intel 586 kompatiblen Rechner, der über mindestens 64 MB RAM und 60 MB freien Festplattenplatz verfügen.

Auf dem Rechner ist eines der folgenden Betriebssysteme Microsoft Windows 98, Microsoft Windows 98 SE, Windows ME, Windows NT 4.0 mit Servicepack 6.0, Windows 2000 oder Windows XP installiert. Es sind der Internet Explorer ab Version 4.01 SP2 mit der Shell32.dll ab Version 4.0 und die Microsoft Smartcard Base Components ab Version 1.0 auf dem Rechner installiert.

Der Benutzer stellt sicher, dass alle Komponenten des Betriebssystems und alle sonstig installierte Software korrekt und vertrauenswürdig ist.

Der Benutzer verwendet eine sicheres Signaturerzeugungssystem, welches aus Kartenleser mit sicherer Pin-Eingabe und Smartcard besteht. Der Benutzer setzt eine der folgenden SigG konformen Smartcards entsprechend den Vorgaben des Herstellers ein:

- TeleSec E4Netkey-Karte
- OpenLimit Karte als spezielle Konfiguration der TeleSec E4NetKey-Karte
- TeleSec PKS Karte

Der Benutzer setzt einen der folgenden Kartenleser mit sicherer Pin-Eingabe entsprechend den Vorgaben des Herstellers ein:

- Cherry SmartBoard G83-6700
- SCMMicrosystems SPx32/ChipDrive Pin-Pad
- Reiner SCT CyberJack e-com Version 2.0
- Reiner SCT CyberJack pinpad Version 2.0

Bei den verwendeten peripheren Komponenten werden ausschliesslich im Sinne des SigG [12] bestätigte Komponenten verwendet, die zugehörigen Zertifikate für diese Produkte können von den Seiten der RegTP bezogen werden (www.regtp.de).

A.Personal

Der Benutzer, der Administrator und das Wartungspersonal sind vertrauenswürdig befolgen die Benutzerdokumentation des EVGs. Insbesondere prüft der Benutzer die Integrität des EVGs entsprechend den Anweisungen im Benutzerhandbuch.

A.Netzwerk

Der Rechner, auf dem der EVG installiert ist, kann über einen Internetzugang verfügen. In diesem Falle wird eine Firewall verwendet, die sicherstellt, dass keine Systemdienste oder Systemkomponenten durch Zugriffe aus dem Internet kompromittiert werden können. Weiterhin setzt der Benutzer einen Virenscanner ein, der in der Lage ist, sowohl klassische Virenprogramme wie Makroviren als auch Backdoor Programme zu erkennen und den Anwender im Falle eines Angriffs über diesen Zustand in Kenntnis zu setzen.
Der Rechner, auf dem der EVG installiert ist, kann über einen Intranetzugang verfügen. In diesem Falle setzt der Anwender einen Virenscanner ein, welcher in der Lage ist, sowohl klassische Virenprogramme wie Makroviren als auch Backdoor Programme zu erkennen und den Anwender im Falle eines Angriffs über diesen Zustand in Kenntnis zu versetzen.

A.Zugriff

Der Rechner des Anwenders befindet sich in einer Umgebung, in welcher der Anwender volle Kontrolle über eingelegte Datenträger und Netzwerkfreigaben hat. Der EVG ist so geschützt, dass er über eine Netzwerkfreigabe nicht erreichbar ist. Der Zugriff auf den EVG vom Rechner des Anwenders ist möglich.

3.2 Bedrohungen

Die Analyse der Bedrohungen gegen den EVG und die durch den EVG zuschützenden Objekte wurde unterstützt durch das Dokument „Maßnahmenkatalog für technische Komponenten nach dem Signaturgesetz“ [2]. Es ist anzumerken, dass dieser Maßnahmekatalog sich auf das „alte“ Signaturgesetz (vom 22.07.1997) bezieht. Die Referenzierung auf diesen Maßnahmenkatalog [2] ist dennoch zulässig, weil (nur gering eingeschränkt) die Maßnahmen auf das jetzt gültige Signaturgesetz übertragbar sind.

Alle Bedrohungen gehen von einem Angreifer mit einem hohen Angriffpotential aus.

Die zu schützenden Objekte sind: Eine Benutzerdatei, eine signierte Datei und der EVG mit seinen Daten. Bei der Benutzerdatei handelt es sich um jede Datei, die aus Sicht des Benutzers schützenswert ist. Bei der signierten Datei handelt es sich um jede Datei, die mit einer elektronischen Signatur zum Schutz vor z.B. Manipulationen versehen worden ist. Bei dem EVG handelt es sich um ein Softwareprodukt, das i.A. aus ausführbaren Dateien und aus Datendateien (z.B. Zertifikate) besteht.

T.DAT

Manipulation einer Benutzerdatei

Ein Angreifer manipuliert durch beliebige Mittel eine Benutzerdatei und die Manipulation bleibt unerkannt.

Die Bedrohung ist hier bewusst sehr allgemein gehalten worden, da sie sehr verschiedene Szenarien abdecken soll. Bei der Benutzerdatei handelt es sich um jede Datei, die aus Sicht des Benutzers schützenswert ist. Der Angreifer kann eine Datei mit Mitteln wie mit einem Editor oder mit einem Netzwerktool während der Datenübertragung usw. manipulieren. Eine Manipulation schließt gezielte und zufällige Veränderungen ein. Der Angreifer verfügt über ein hohes Angriffspotential.

T.SIG_DAT

Manipulation einer signierten Datei

Ein Angreifer manipuliert durch beliebige Mittel eine signierte Datei und die Manipulation bleibt unerkannt.

Die Bedrohung ist hier bewusst sehr allgemein gehalten worden, da sie sehr verschiedene Szenarien abdecken soll. Bei der signierten Datei handelt es sich um jede Datei, die mit einer elektronischen Signatur versehen worden ist. Der Angreifer kann den Inhalt der Datei (also einschließlich der Daten der Signatur) mit Mitteln wie mit Editor oder mit einem Netzwerktool während der Datenübertragung usw. manipulieren. Eine Manipulation schließt gezielte und zufällige Veränderungen ein. Der Angreifer verfügt über ein hohes Angriffspotential.

T. EVG

Manipulation des EVGs und seiner Daten.

Ein Angreifer manipuliert oder tauscht Teile (Module) bzw. Daten des EVGs auf dem Rechner aus und die Manipulation bleibt unerkannt.

Die Manipulation der Teile des EVGs richtet sich direkt gegen die EVG-Software. Der Angreifer mit einem hohen Angriffspotential ändert/vertauscht bei dieser Bedrohung die Programmteile mit der Absicht die Sicherheitsfunktionalität des EVG zu verändern und damit diese zu deaktivieren, umzugehen usw.

T.VOR_SIG

Manipulation der Datei vor Entscheidung zu signieren

Ein Angreifer manipuliert durch beliebige Mittel den Inhalt einer Datei, bevor der Benutzer sich entscheidet einen Signaturvorgang einzuleiten und die Manipulation bleibt unerkannt.

Bei der Datei handelt es sich um eine Datei, für die der Benutzer eine Signatur erstellen will. Die Bedrohung geht von einem Angreifer mit einem hohen Angriffpotential aus, der in der Lage ist die Datei zu verändern in dem Zeitraum zwischen der Auswahl der Datei zur Unterschrift durch den Benutzer und der Mitteilung des Benutzers an den EVG, die Datei zu signieren.

T.NACH_SIG

Erzeugung einer gefälschten elektronischen Signatur

Ein Angreifer manipuliert den Hashwert nach der Entscheidung des Benutzers, einen Signaturvorgang einzuleiten und die Manipulation bleibt unerkannt.

Die Bedrohung geht von einem Angreifer mit einem hohen Angriffpotential aus, der in der Lage ist den einer zu signierenden Datei zugeordneten Hashwert zu verändern in dem Zeitraum zwischen der Mitteilung des Benutzers an den EVG, die Datei zu signieren und der Übergabe des Hashwertes an die Signaturkarte zur Erzeugung der elektronischen Signatur. Der Angreifer kann z.B. den Hashwert auf der Übertragungsleitung zu der Signaturkarte verändern.

3.3 Organisatorische Sicherheitspolitik

Für den EVG ist keine organisatorische Sicherheitspolitik definiert.

4 Sicherheitsziele für den EVG und die Umgebung des EVG

4.1 Sicherheitsziele für den EVG

OT. DAT

Schutz einer Benutzerdatei

Der EVG muss einen Schutz gegen die Manipulation einer vom Benutzer definierten Datei durch die Errechnung eines Hashwertes über die Daten der Datei anbieten.

OT.SIG_DAT

Schutz einer signierten Datei

Der EVG muss es dem Benutzer ermöglichen, eine Manipulation einer signierten Datei zu erkennen.

OT. EVG

Schutz des EVGs

Der EVG muss es dem Benutzer ermöglichen, Manipulationen seiner Komponenten bzw. seiner Daten zu erkennen.

OT.VOR_SIG

Schutz der Datei vor Entscheidung zu signieren

Der EVG soll eine Datei dem Benutzer derart darstellen, dass der Benutzer in der Lage ist, den Inhalt der Datei eindeutig zu erkennen.

OT.NACH_SIG

Schutz vor Fälschung der Signatur

Der EVG muss es dem Benutzer ermöglichen, eine Manipulation des Hashwertes einer zu unterschreibenden Datei nach Erzeugung der Signatur, zu erkennen.

4.2 Sicherheitsziele für die Umgebung des EVGs

Die Sicherheitsziele für die Umgebung des EVGs sind aus den Annahmen der EVG-Sicherheitsumgebung und aus der Bedrohung T.DAT abgeleitet.

OE.Plattform

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass der Benutzer als Hardwareplattform einen Intel 586 kompatiblen Rechner, der über mindestens 64 MB RAM und 60 MB freien Festplattenplatz verfügt, verwendet.

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass der Benutzer auf dem Rechner eines der folgenden Betriebssysteme installiert: Microsoft Windows 98, Microsoft Windows 98 SE, Windows ME, Windows NT 4.0 mit Servicepack 6.0, Windows 2000 oder Windows XP. Des weiteren, dass der Internet Explorer ab Version 4.01 SP2 mit der Shell32.dll ab Version 4.0 und die Microsoft Smartcard Base Components ab Version 1.0 auf dem Rechner installiert ist.

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass alle Komponenten des Betriebssystems und alle sonstig installierte Software korrekt und vertrauenswürdig ist.

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass ein sicheres Signaturerzeugungssystem, welche aus Kartenleser mit sicherer Pin-Eingabe und Smartcard besteht, verwendet wird und dass eine der folgenden SigG konformen Smartcards entsprechend den Vorgaben des Herstellers eingesetzt wird:

- TeleSec E4Netkey-Karte
- OpenLimit Karte als spezielle Konfiguration einer TeleSec E4NetKey-Karte
- TeleSec PKS Karte

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass einer der folgenden Kartenleser mit sicherer Pin-Eingabe (Anmerkung: der EVG bietet keine Funktionalität zur Pin-Prüfung an) entsprechend den Vorgaben des Herstellers eingesetzt wird:

- Cherry SmartBoard G83-6700
- SCMMicrosystems SPx32/ChipDrive Pin-Pad
- Reiner SCT CyberJack e-com Version 2.0
- Reiner SCT CyberJack pinpad Version 2.0

Bei den verwendeten peripheren Komponenten werden ausschließlich im Sinne des SigG [12] bestätigte Komponenten verwendet, die zugehörigen Zertifikate für diese Produkte können von den Seiten der RegTP bezogen werden (www.regtp.de).

OE.Personal

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass der Benutzer, der Administrator und das Wartungspersonal vertrauenswürdig sind und die Benutzerdokumentation des EVGs befolgen. Insbesondere prüft der Benutzer die Integrität des EVGs entsprechend der Benutzerdokumentation.

OE.Netzwerk

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden in dem Fall, dass der Rechner an das Internet angeschlossen ist, z.B. durch die Verwendung einer Firewall , dass keine Systemdienste oder Systemkomponenten durch Zugriffe aus dem Internet kompromittiert werden können. Weiterhin, dass ein Virenscanner, der in der Lage ist, sowohl klassische Virenprogramme wie Makroviren als auch Backdoor Programme zu erkennen und den Anwender im Falle eines Angriffs über diesen Zustand in Kenntnis zu setzen, eingesetzt wird.

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden in dem Fall, dass der Rechner über einen Intranetzugang verfügt, ein Virenscanner, welcher in der Lage ist, sowohl klassische Virenprogramme wie Makroviren als auch Backdoor Programme zu erkennen und den Anwender im Falle eines Angriffs über diesen Zustand in Kenntnis zu versetzen, eingesetzt wird.

OE.Zugriff

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass der Rechner des Anwenders sich in einer Umgebung, in welcher der Anwender volle Kontrolle über eingelegte Datenträger und Netzwerkfreigaben hat, befindet. Weiterhin, dass der EVG ist so geschützt, dass er über eine Netzwerkfreigabe nicht erreichbar ist, und dass der Zugriff auf den EVG vom Rechner des Anwenders möglich ist.

OE.SIG_DAT

Schutz der Benutzerdateien

Es muss durch geeignete organisatorische Maßnahmen sichergestellt werden, dass die IT-Umgebung eine Funktionalität zur Errechnung einer elektronischen Signatur aus einem Hashwert anbietet.

5 IT-Sicherheitsanforderungen

5.1 Funktionale Sicherheitsanforderungen an den EVG

Die an dieser Stelle formulierten funktionalen Sicherheitsanforderungen sind konform zur CC Teil 2 formuliert und korrespondieren mit den vorgegebenen funktionalen Komponenten mit der Ausnahme der Komponente FDP_SVR.1, die in diesen Sicherheitsvorgaben definiert worden ist.

FCS_COP.1 (SHA)[4]

Kryptografischer Betrieb

FCS_COP.1.1

Die TSF müssen [Zuweisung: *die Berechnung von Hash-Werten*] gemäß eines spezifizierten kryptografischen Algorithmus [Zuweisung: *SHA-1*] und kryptografischer Schlüssellängen [Zuweisung: *keine*], die den folgenden [Zuweisung: *Standard FIPS 180-1*] entsprechen, durchführen.

FCS_COP.1 (160)[5]

Kryptografischer Betrieb

FCS_COP.1.1

Die TSF müssen [Zuweisung: *die Berechnung von Hash-Werten*] gemäß eines spezifizierten kryptografischen Algorithmus [Zuweisung: *RIPE MD-160*] und kryptografischer Schlüssellängen [Zuweisung: *keine*], die den folgenden [Zuweisung: *Standard ISO/IEC 10118-3*] entsprechen, durchführen.

[4] Iteration

[5] Iteration

FCS_COP.1 (RSA1)[6]

Kryptografischer Betrieb

FCS_COP.1.1

Die TSF müssen [Zuweisung: *die Überprüfung elektronischer Signaturen*] gemäß eines spezifizierten kryptografischen Algorithmus [Zuweisung: *RSA*] und kryptografischer Schlüssellängen [Zuweisung: *1024 bit*], die den folgenden [Zuweisung: *Standard PKCS#1*] entsprechen, durchführen.

FCS_COP.1 (RSA2)[7]

Kryptografischer Betrieb

FCS_COP.1.1

Die TSF müssen [Zuweisung: *die Überprüfung elektronischer Signaturen*] gemäß eines spezifizierten kryptografischen Algorithmus [Zuweisung: *RSA*] und kryptografischer Schlüssellängen [Zuweisung: *1024 bit*], die den folgenden [Zuweisung: *Standard PKCS#1*] entsprechen, durchführen.

Verfeinerung zu FCS_COP.1 (RSA2):

Teil1:

Die TSF müssen während der *Überprüfung elektronischer Signaturen* die Überprüfung der Zertifikatskette nach dem Standard ISIS-MTT Common ISIS MTT Mailtrust Specifications for Interoperable PKI Applications Version 1.02 vornehmen, wenn das Gültigkeitsmodell der CA auf dem Kettenmodell[8] basiert.

[6] Iteration

[7] Iteration

[8] Dies trifft dann zu, wenn in den Zertifikatsrichtlinien SigG-Konformität postuliert wird. Es wird eine Ausnahme formuliert: Wurde das verwendete Zertifikat von der 4RCA bis 7RCA der RegTP herausgegeben, wird nach dem Kettenmodell geprüft, auch wenn das Zertifikat keine SigG-Konformität postuliert.

Teil2:

Die TSF müssen während der *Überprüfung elektronischer Signaturen* die Überprüfung der Zertifikatskette nach dem Standard RFC 3280 vornehmen, wenn das Gültigkeitsmodell der CA nicht auf dem Kettenmodell basiert.

FDP_DAU.2

Datenauthentisierung mit Garantie der Identität

FDP_DAU.2.1

Die TSF müssen die Fähigkeit zur Generierung von Nachweisen als Gültigkeitsgarantie von [Zuweisung: *durch den Benutzer ausgewählten Dateien*] bereitstellen.

FDP_DAU.2.2

Die TSF müssen [Zuweisung: *dem Benutzer*] die Fähigkeit zur Verifizierung des Gültigkeitsnachweises der angezeigten Information und der Identität des Benutzers, der den Nachweis generiert hat, bereitstellen.

FDP_ITC.1(1)[9]

Import von Benutzerdaten ohne Sicherheitsattribute

FDP_ITC.1.1

Die TSF müssen die [Zuweisung: *keine*] beim Import von unter Kontrolle SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen.

FDP_ITC.1.2

Die TSF müssen die mit den Benutzerdaten verknüpften Sicherheitsattribute ignorieren, wenn diese von außerhalb des TSC importiert werden.

[9] Iteration

FDP_ITC.1.3

Die TSF müssen die folgenden Regeln beim Import unter Kontrolle der SFP stehender Benutzerdaten von außerhalb des TSC durchsetzen: [Zuweisung*: Regeln für die Verwendung des Zertifikates bei der Prüfung nach der Signaturerstellung*].

Erklärung:
Regeln für die Verwendung des Zertifikates bei der Prüfung nach der Signaturerstellung

Nach der Signaturerzeugung müssen die TSF mit dem öffentlichen Schlüssel des Zertifikates die Signatur nach dem RSA Verfahren wieder entschlüsseln und das Operationsergebnis mit der kryptografischen Prüfsumme (Hashwert) vergleichen, die als Ausgangsbasis für die Signaturerzeugung verwendet wurde (Vergleich auf mathematische Korrektheit der erzeugten Signatur).

FDP_ITC.1(2)
Import von Benutzerdaten ohne Sicherheitsattribute

FDP_ITC.1.1

Die TSF müssen die [Zuweisung: *keine*] beim Import von unter Kontrolle SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen.

FDP_ITC.1.2

Die TSF müssen die mit den Benutzerdaten verknüpften Sicherheitsattribute ignorieren, wenn diese von außerhalb des TSC importiert werden.

FDP_ITC.1.3

Die TSF müssen die folgenden Regeln beim Import unter Kontrolle der SFP stehender Benutzerdaten von außerhalb des TSC durchsetzen: [Zuweisung*: Regeln für die Verwendung aktueller Zertifikate vom Netz*].

Erklärung:
Regeln für die Verwendung aktueller Zertifikate vom Netz

Bei der Prüfung der elektronischen Signatur müssen die TSF die im Unterverzeichnis Data\CRLS vorhandenen Sperrlisten benutzen, um die Gültigkeit des Zertifikates zum Zeitpunkt der Signaturerzeugung zu überprüfen.

FDP_SVR.1
Sichere Anzeige

FDP_SVR.1.1

Die TSF müssen sicherstellen, dass der dem Benutzer angezeigte Inhalt eines Dokumentes entsprechend den folgenden Normen [Zuweisung: *Standards oder Regeln: TIFF Revision 6.0 Final Draft June 3, 1992, Adobe Developers Association*, *Benutzerdokumentation T-TeleSec Signet 1.6*] eindeutig ist.

FDP_SVR.1.2

Die TSF müssen sicherstellen, dass der dem Benutzer anzuzeigende Inhalt eines Dokumentes frei von aktiven oder verdeckten Inhalten ist. Die TSF muss die Darstellung solcher Dokumente verweigern und den Benutzer darüber informieren.

FDP_SVR.1.3

Die TSF müssen sicherstellen, dass der Benutzer über einen nicht darstellbaren Inhalt eines anzuzeigenden Dokumentes informiert wird.

FTP_ITC.1

Inter-TSF Vertrauenswürdiger Kanal

FTP_ITC.1.1

Die TSF müssen einen Kommunikationskanal zwischen sich und einem entfernten vertrauenswürdigen IT-Produkt bereitstellen, der logisch von den anderen Kommunikationskanälen getrennt ist und eine gesicherte Identifikation seiner Endpunkte sowie den Schutz der Daten des Kanals vor Modifizierung oder Preisgabe bereitstellt.

FTP_ITC.1.2

Die TSF müssen [Auswahl: *den TSF*] erlauben, eine Kommunikation über den vertrauenswürdigen Kanal einzuleiten.

FTP_ITC.1.3

Die TSF müssen für [Zuweisung: *Erstellung einer elektronischen Signatur*] eine Kommunikation über den vertrauenswürdigen Kanal einleiten.

5.2 Vertrauenswürdigkeitsanforderungen an den EVG

Die folgende Tabelle gibt eine Übersicht über die Dokumente, in denen dargestellt ist, wie die Anforderungen erfüllt werden. Die Anforderungen an die Vertrauenswürdigkeit des EVG sind entsprechend EAL3 (Common Criteria Teil 3) mit Zusätzen definiert worden. Alle Vertrauenswürdigkeitsanforderungen sind aus den Common Criteria Teil 3 entnommen worden.

Vertrauenswürdigkeits-klasse	**Vertrauenswürdigkeits-familie**	**Dokument**
Konfigurations-management	Autorisierungskontrolle ACM_CAP.3	Der Entwickler betreibt ein Konfigurationsmanagement, das alle Versionen für alle Konfigurationsteile verwaltet und die Sicherheitsfunktionen des Betriebssystems nutzt, um sicherzustellen, dass keine unerlaubten Modifikationen am EVG vorgenommen werden. ACM_SCP.1 EVG CM-Umfang Das eingesetzte Konfigurationskontrollsystem verfolgt die Darstellung der Implementierung, Design, Tests und Dokumentation. Die Details sind in SignCubes Konfigurationsmanagement“, das ein Teil der Herstellerdokumentation für die Evaluierung ist, dargestellt.
	EVG-CM-Umfang ACM_SCP.1	
Auslieferung und Betrieb	Auslieferungsprozeduren ADO_DEL.1	Die Auslieferungsprozeduren sind klar definiert und in „Auslieferung“, das ein Teil der Herstellerdokumentation für die Evaluierung ist , dokumentiert.
	Installations-, Generierungs- und Anlaufprozeduren ADO_IGS.1	Diese Aspekte werden im Benutzerhandbuch behandelt.
Entwicklung	Informelle funktionale Spezifikation ADV_FSP.1	Die Sicherheitsfunktionen sind informelle funktional spezifiziert.
	Sicherheitsspezifischer Entwurf auf hoher Ebene ADV_HLD.2	Entwurf auf hoher Ebene (High Level Design) ist beschreieben.

	Teilmenge der Implementierung der TSF ADV_IMP.1	Der Source-Code ist verfügbar für die Evaluierung gemacht worden.
	Beschreibender Entwurf auf niedriger Ebene ADV_LLD.1	Entwurf auf niederer Ebene (Low Level Design) ist beschreieben.
	Informeller Nachweis der Übereinstimmung ADV_RCR.1	
Handbücher	Systemverwalterhandbuch AGD_ADM.1	Das Benutzer-Handbuch ist sehr detailliert und gibt Hinweise zur sicheren Installation, Verwaltung und Nutzung des EVG.
	Benutzerhandbuch AGD_USR.1	
Lebenszyklus-unterstützung	Identifikation der Sicherheitsmaßnahmen ALC_DVS.1	Die Sicherheit der Entwicklungsumgebung wird durch materielle, personelle und andere Maßnahmen gesichert.
	Klar festgelegte Entwicklungswerkzeuge ALC_TAT.1	Es werden klar festegelegte Werkzeuge (Compiler) zur Entwicklung des EVG benutzt. Die Details sind in SignCubes Konfigurationsmanagement“, das ein Teil der Herstellerdokumentation für die Evaluierung ist, dargestellt.
Testen	Analyse der Testabdeckung ATE_COV.2	Der Entwickler setzt wohldokumentierte Testverfahren ein: • Tests gegenüber der Funktionalen Spezifikation • Tests auf der Ebene der Subsysteme • Tests aller Sicherheitsfunktionen
	Testen – Entwurf auf hoher Ebene ATE_DPT.1	
	Funktionales Testen ATE_FUN.1	

	Unabhängiges Testen – Übereinstimmung ATE_IND.2	Vom Evaluator sind eigenständige Tests durchzuführen.
Schwachstellenbewertung	Analysieren und Testen auf unsichere Zustände AVA_MSU.3	Durch einen internen Reviewprozess der Handbücher wird verhindert, dass darin widersprüchliche, irreführende, unvollständige oder übertriebene Anleitungen aufgenommen werden.
	Hohe Widerstandsfähigkeit AVA_VLA.4	Für jeden Mechanismus, der ein SOF-Postulat besitzt, wird eine Analyse durchgeführt und deren Ergebnis dokumentiert.
	Stärke der EVG-Sicherheitsfunktionen AVA_SOF.1	Es wird eine Analyse zur Identifikation von Schwachstellen durchgeführt und deren Ergebnis dokumentiert.

Tabelle 1 Übersicht über die Dokumente

5.3 Sicherheitsanforderungen an die IT-Umgebung

FCS_COP.1 (ES)

Kryptografischer Betrieb

FCS_COP.1.1

Die TSF müssen [Zuweisung: *die Erzeugung elektronischer Signaturen*] gemäß eines spezifizierten kryptografischen Algorithmus [Zuweisung: *RSA*] und kryptografischer Schlüssellängen [Zuweisung: *1024 bit*], die den folgenden [Zuweisung: *Standard PKCS#1*] entsprechen, durchführen.

6 EVG-Übersichtsspezifikation

6.1 EVG-Sicherheitsfunktionen

SF.1

Hashwertberechnung und Anstoß der Erzeugung elektronischer Signaturen mit Zertifikaten unter Verwendung eines Kartenterminals und einer Smartcard

Der EVG erzeugt Hashwerte von beliebigen Dateien nach dem SHA1 Algorithmus (wie gefordert durch FCS_COP.1 (SHA), die auch die entsprechenden zu Grunde liegenden Standards benennt). Nach Erzeugung des Hashwertes nutzt der EVG die PC/SC oder die CT-API Mechanismen, um den Hashwert von einer Smartcard in einem Smartcard Terminal mit sicherer Pin-Eingabe nach dem RSA Verfahren verschlüsseln zu lassen und so eine elektronische Signatur zu erzeugen[10]. Der EVG fügt dem verschlüsselten Hashwert das Zertifikat des unterschreibenden hinzu. Insgesamt wird durch die Verschlüsselung (Signatur) des Hashwertes der Nachweis als Gültigkeitsgarantie der Datei und durch das Zertifikat die Verifizierung des Gültigkeitsnachweises bereitgestellt.

[10] Diese Verschlüsselung ist Teil der Sicherheitsfunktionalität, die von der IT-Umgebung erbracht wird. Der Algorithmus und die verwendete Schlüssellänge ist wie in FCS_COP.1(ES) spezifiziert.

Vor der Erzeugung des Hashwertes nach dem SHA1 Algorithmus zeigt der EVG dem Benutzer mit einer eindeutigen Textmeldung an, dass eine elektronische Signatur erzeugt werden soll. Dabei ist eindeutig erkennbar, auf welche Daten sich die Signatur beziehen soll, da der T-TeleSec Signet Manager dem Nutzer mitteilt, welche Applikation welche Datei signieren will. Im gleichen Dialog ist der Aufruf der sicheren Anzeigeeinheit (SF.5) möglich, so dass der Inhalt der zu signierenden Daten hinreichend zu erkennen ist. Durch die Verwendung eines sicheren Signaturerzeugungssystems aus Kartenleser mit sicherer Pin-Eingabe und Smartcard ist sichergestellt, dass die Signatur nur durch die berechtigte Person erfolgt und die Identifikationsdaten nicht preisgegeben werden.

Die Sicherheitsfunktion SF.1 verwendet permutationelle Mechanismen. Bei allen verwendeten Mechanismen handelt es sich ausschließlich um kryptografische Algorithmen. Es wird daher keine Mechanismenstärke für diese Funktion postuliert. Die verwendeten kryptografischen Algorithmen sind in [11] als geeignet zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22.Mai 2001 in Verbindung mit Anlage 1 Abschnitt 1 Nr. 2 SigV vom 22.November 2001 Mainz, 2003 aufgeführt worden.

SF.2

Prüfung von Hashwerten und Signaturen unter Verwendung von Sperrlisten und optionaler OCSP-Abfrage

Der EVG kann die Signaturen an beliebigen Dateien überprüfen, die entweder mit dem SHA1 Algorithmus oder dem RIPE MD 160 Algorithmus erzeugt wurden. Dabei wird eindeutig erkennbar, auf welche Datei sich die elektronische Signatur bezieht. Bei der Prüfung der Signatur wird wiederum der Hashwert über die Originaldaten gebildet (wie gefordert durch FCS_COP.1 (SHA) oder FCS_COP.1(160), die auch die entsprechenden zu Grunde liegenden Standards benennen) und die eigentliche Signatur mit dem öffentlichen Schlüssel nach dem RSA Verfahren (wie gefordert durch FCS_COP.1 (RSA2), die auch den entsprechenden Standard für den kryptografischen Algorithmus benennt) entschlüsselt[11], wobei die Überprüfung der Zertifikatskette nach dem Kettenmodell bzw. entsprechend dem Standard RFC3280 (wie gefordert durch die Verfeinerung zu FCS_COP.1(RSA2), die auch die entsprechenden zu Grunde liegenden Standards benennt) vorgenommen wird. Der EVG gibt dem Nutzer eine eindeutige Meldung, ob die beiden Hashwerte identisch waren oder ob die Hashwerte differieren (Überprüfung der Signatur zur Umsetzung von FDP_DAU.2, insbesondere FDP_DAU.2.2). Dadurch wird eindeutig erkennbar, ob die Daten unverändert sind. Die Korrektheit der Signatur wird somit zuverlässig geprüft die und zutreffend angezeigt. Durch die Verwendung der sicheren Anzeigeeinheit (SF.5) wird sichergestellt, dass der Inhalt der signierten Daten hinreichend zu erkennen ist.

Bei der Signaturprüfung wird aus dem Signaturzertifikat das Herausgeberzertifikat ermittelt und auf Grund dieses Zertifikats eine entsprechende Sperrliste geladen. Innerhalb dieser Sperrliste wird überprüft, ob ein entsprechender Eintrag für das Zertifikat in der Sperrliste vorhanden ist. Ist dies der Fall, werden die Informationen aus der Sperrliste übernommen (entsprechend den Regeln wie definiert in FDP_ITC.1(2)). War das Zertifikat zum Zeitpunkt der Signaturerzeugung bereits gesperrt, wird dies dem Benutzer angezeigt.

Zusätzlich hat der Benutzer die Möglichkeit, eine OCSP-Abfrage zum Signaturzertifikat durchzuführen. Das Ergebnis der OCSP-Abfrage wird dem Benutzer mit einer eindeutigen Textmeldung angezeigt.

[11] Bei der Prüfung der Signatur wird stets der gesamte PKCS#1 Version1.5 Block überprüft. Diese Überprüfung wird mit der frei verfügbaren Bibliothek CryptoPP 5.1 vorgenommen. Als PKCS#1 Version 1.5 Blocktype wird Typ 0.1 benutzt.

Die Sicherheitsfunktion SF.2 verwendet permutationelle Mechanismen. Bei allen verwendeten Mechanismen handelt es sich ausschließlich um kryptografische Algorithmen. Es wird daher keine Mechanismenstärke für diese Funktion postuliert. Die verwendeten kryptografischen Algorithmen sind in [11] als geeignet zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22.Mai 2001 in Verbindung mit Anlage 1 Abschnitt 1 Nr. 2 SigV vom 22.November 2001 Mainz, 2003 aufgeführt worden.

SF.3

Erkennung der Manipulation von Modulen des EVGs

Der EVG wird von der Firma SignCubes mit signierten Bibliotheken und ausführbaren Dateien ausgeliefert, die ebenfalls signiert sind. Um die Erkennung der Manipulation an den installierten Dateien zu realisieren, existiert ein separater Prüfmodul, welcher als DLL realisiert ist. Alle Subsysteme[12] des Produktes T-TeleSec Signet 1.6 kennen den SHA1 Hashwert dieses Prüfmoduls. Das Prüfmodul selbst kennt den öffentlichen Schlüssel, mit dem die einzelnen Module und ausführbaren Dateien der Firma SignCubes signiert werden.
Wird der T-TeleSec Signet Manager gestartet, bildet dieser im ersten Schritt den Hashwert des vorhandenen Prüfmoduls (wie gefordert durch FCS_COP.1 (SHA), die auch die zu Grunde liegenden Standards benennt) und stellt somit die Integrität des Prüfmoduls sicher. Im Gegenzug ermittelt der Prüfmodul, von welcher Anwendung er geladen wird und überprüft die Signatur an der ihn ladenden Anwendung (FCS_COP.1 (SHA) und FCS_COP.1(RSA1) welche auch die relevanten Standards benennen und die verwendeten Schlüssellängen spezifizieren). Das Prüfmodul ist im logischen Modell der Anwendung der Hauptanwendung (T-TeleSec Signet Manager) zugeordnet, da der T-TeleSec Signet Manager ohne das Prüfmodul nicht korrekt arbeiten kann. Soll nun ein Modul[13] von einem der Subsysteme geladen werden, verwendet dieses (das Subsystem) das Prüfmodul, um eine Manipulationserkennung durchzuführen. Dazu bildet das Prüfmodul den Hashwert über das zu ladende Modul (wie gefordert durch FCS_COP.1 (SHA), die auch die zu Grunde liegenden Standards benennt) und verifiziert mit dem öffentlichen Schlüssel des Signaturzertifikates die Signatur des zu ladenden Moduls (wie gefordert in FCS_COP.1 (RSA1), die auch die relevanten Standards benennt und die Schlüssellängen spezifiziert).

Die einzelnen Subsysteme des EVGs kennen des Hashwert des Prüfmoduls. Um die Authentizität des Prüfmoduls zu überprüfen, wird der Hashwert vom Prüfmodul (FCS_COP.1(SHA), s. auch oben) gebildet und mit dem in den Subsystemen enthaltenen Hashwert verglichen. Stimmen der ermittelte Hashwert und der in den jeweiligen Subsystemen enthaltene Hashwert nicht überein, verweigern diese Module jede weitere Arbeit.

[12] Die Subsysteme der Applikation sind die sichere Anzeigeinheit, der Cryptographic Service Provider, der Signet Manager und die Shell Extension. Eine detaillierte Beschreibung der verwendeten Mechanismen erfolgt im Dokument zum Entwurf auf hoher Ebene und im Dokument zum Entwurf auf niederer Ebene.

[13] Im Sinne einer DLL.

Die Sicherheitsfunktion SF.3 verwendet permutationelle Mechanismen. Bei allen verwendeten Mechanismen handelt es sich ausschließlich um kryptografische Algorithmen. Es wird daher keine Mechanismenstärke für diese Funktion postuliert. Die verwendeten kryptografischen Algorithmen sind in [11] als geeignet zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22.Mai 2001 in Verbindung mit Anlage 1 Abschnitt 1 Nr. 2 SigV vom 22.November 2001 Mainz, 2003 aufgeführt worden.

SF.4

Sicherstellung der Unversehrtheit des EVGs

Mit der Applikation T-TeleSec Signet 1.6. wird eine Prüfsoftware ausgeliefert, die auf der CD verbleibt und nicht auf dem Rechner des Anwenders installiert wird. Wird das Testprogramm gestartet, überprüft es die Integrität der Installation, indem es die Hashwerte der installierten Module bildet (wie gefordert durch FCS_COP.1 (SHA), die auch die entsprechenden zu Grunde liegenden Standards benannt) und über den RSA Algorithmus (wie gefordert in FCS_COP.1 (RSA1), die auch den relevanten Standard benennt und die Schlüssellängen spezifiziert) die vorhandenen Modulsignaturen entschlüsselt (der öffentliche Schlüssel zur Signaturprüfung ist fester Bestandteil der Hauptanwendung) und das Operationsergebnis mit den errechneten Hashwerten vergleicht. Wurden die Module verändert, weist das Prüfprogramm den Anwender auf diesen Zustand hin.
Das Prüfprogramm enthält die ausgelieferten Zertifikatsvertrauenslisten (CTLs) und Stammzertifikate, die im Unterverzeichnis Data/CTLs bei der Installation abgelegt werden. Der Pfad für die Ablage kann vom Benutzer mit Administrationsrechten geändert werden, das Prüfprogramm erkennt den geänderten Ablagepfad an Hand der abgelegten Optionen in der Registry. Wurde der Ablagepfad geändert, weist das Prüfprogramm den Benutzer darauf hin, dies wird jedoch nicht als Fehler gewertet, da der Benutzer die Pfade konfigurieren kann. Das Prüfprogramm nimmt einen binären Vergleich der vorhandenen und der ausgelieferten Stammzertifikate und Zertifikatsvertrauenslisten vor und weist den Nutzer mit einer Statusmeldung darauf hin, wenn die Dateien nicht binär identisch sind.
Wurden Stammzertifikate in dem Verzeichnis hinzugefügt, wird der Benutzer ebenfalls durch eine Statusmeldung auf diesen Zustand hingewiesen.

Die Prüfsoftware nimmt keine Überprüfung der vorhandenen Registry Einträge vor.

Die Sicherheitsfunktion SF.4 verwendet permutationelle Mechanismen. Bei allen verwendeten Mechanismen handelt es sich ausschließlich um kryptografische Algorithmen. Es wird daher keine Mechanismenstärke für diese Funktion postuliert. Die verwendeten kryptografischen Algorithmen sind in [11] als geeignet zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22.Mai 2001 in Verbindung mit Anlage 1 Abschnitt 1 Nr. 2 SigV vom 22.November 2001 Mainz, 2003 aufgeführt worden.

SF.5

Sichere Anzeige der zu signierenden Daten

Der EVG stellt mit der sicheren Anzeigeeinheit sicher, dass der Benutzer die Inhalte, die angezeigt werden sollen, eindeutig interpretieren kann und die angezeigte Datei frei von verdeckten oder aktiven Inhalten ist (wie gefordert durch FDP_SVR.1.1). Weiterhin wird mit der sicheren Anzeigeeinheit erreicht, dass der Benutzer informiert wird, falls aktive Inhalte oder nicht darstellbare Inhalte in der Datei enthalten sind (wie gefordert durch FDP_SVR.1.2 und FDP_SVR.1.3).

Bei der sicheren Anzeige der Datei werden die folgenden Arbeitsschritte vorgenommen: Bei der Datei handelt es sich entweder um eine Textdatei oder um eine TIFF Datei. Dies wird über einen entsprechenden Dokumentenparser ermittelt. Handelt es sich um ein unbekanntes Format, wird eine entsprechende Fehlermeldung ausgegeben, die den Hinweis enthält, dass diese Datei nicht dargestellt werden kann (wie gefordert durch FDP_SVR.1). Nachdem festgestellt wurde, um welchen Dateityp es sich handelt, werden die in der Datei enthaltenen Tags und Steuerzeichen untersucht. Enthält die Datei Steuerzeichen, die der Anzeigeeinheit unbekannt sind, wird der Benutzer darauf hingewiesen, dass in der Datei nicht beabsichtigte Inhalte enthalten sein können (wie gefordert durch FDP_SVR.1.2). Werden aktive oder verdeckte Inhalte in der Datei erkannt, wird der Benutzer ebenfalls mit einer eindeutigen Textmeldung auf diesen Zustand hingewiesen (wie gefordert durch FDP_SVR.1.2 und FDP_SVR.1.3). Will der Benutzer die Datei signieren, wird er mit einer eindeutigen Textmeldung darauf hingewiesen, dass verdeckte oder aktive Inhalte in dem Dokument enthalten sind, die von der sicheren Anzeigeeinheit nicht dargestellt werden.

Die Sicherheitsfunktion SF.5 verwendet keine permutationelle oder probabilistischen Mechanismen. Es wird daher keine Mechanismenstärke für diese Funktion postuliert.

SF.6
Schutz vor Hashwertverfälschung

Vor dem Signaturvorgang wird der Hashwert nach dem SHA1 Algorithmus (wie gefordert durch FCS_COP.1 (SHA), die auch die entsprechenden zu Grunde liegenden Standards benennt) über die zu signiereden Daten gebildet. Nach dem Signaturvorgang überprüft der EVG die erzeugte Signatur, indem er die Signatur mit dem öffentlichen Schlüssel (entsprechend den Regeln wie definiert in FDP_ITC.1 (1)) des verwendeten Zertifikats entschlüsselt (wie gefordert in FCS_COP.1 (RSA1), die auch den relevanten Standard benennt und die Schlüssellängen spezifiziert) und das Operationsergebnis mit dem vor dem Signaturvorgang berechneten Hashwert vergleicht (und setzt damit die Forderung FTP_ITC.1 um). Abschließend wird dem Benutzer eine Textmeldung angezeigt, ob der von ihm beabsichtigte Hashwert signiert wurde.

Die Sicherheitsfunktion SF.6 verwendet permutationelle Mechanismen. Bei allen verwendeten Mechanismen handelt es sich ausschließlich um kryptografische Algorithmen. Es wird daher keine Mechanismenstärke für diese Funktion postuliert. Die verwendeten kryptografischen Algorithmen sind in [11] als geeignet zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22.Mai 2001 in Verbindung mit Anlage 1 Abschnitt 1 Nr. 2 SigV vom 22.November 2001 Mainz, 2003 aufgeführt worden.

6.2 Maßnahmen zur Vertrauenswürdigkeit

In der Tabelle im Kapitel 5.2. werden bereits die Dokumente aufgelistet, welche die entsprechenden Maßnahmen beschreiben.

7 PP-Postulate

Für den EVG wird kein PP-Postulat abgegeben.

7.1 PP-Verweis

N/A

7.2 PP-Anpassung

N/A

7.3 PP-Ergänzungen

N/A

8 Erklärungen

8.1 Erklärungen der Sicherheitsziele

Bedrohungen, Annahmen vs. Sicherheitsziele	OT.DAT	OT.SIG_DAT	OT.EVG	OT.VOR_SIG	OT.NACH_SI	OE.Plattform	OE.Personal	OE.Netzwerk	OE.Zugriff	OE.SIG_DAT
T.DAT	x	x								x
T.SIG_DAT		x								
T.EVG			x							
T.VOR_SIG				x						
T.NACH_SIG					x					
A.Plattform						x				
A.Personal							x			
A.Netzwerk								x		
A.Zugriff									x	

Tabelle 2 Bedrohungen und Annahmen vs. Sicherheitsziele

A.Personal stellt sicher, dass der Benutzer und das Wartungspersonal vertrauenswürdig sind. Ferner stellt diese Annahme sicher, dass der Benutzer die Integrität des EVGs prüft. Das Sicherheitsziel OE.Personal formuliert genau dieselben Anforderungen. Es stellt damit explizit die Erfüllung der Annahme sicher.

A.Plattform stellt sicher, dass das Betriebssystem den Vorgaben entspricht und alle Komponenten des Betriebssystems und die sonstige installierte Software vertrauenswürdig ist. Das Sicherheitsziel OE.Plattform formuliert genau die gleichen Anforderungen und stellt damit explizit die Erfüllung dieser Annahme sicher.

A.Netzwerk stellt sicher, dass keine Systemdienste oder Systemkomponenten durch Zugriffe aus dem Internet kompromittiert werden können und somit die Vertrauenswürdigkeit der Umgebung sichergestellt ist. OE.Netzwerk formuliert genau die gleichen Anforderungen und stellt damit explizit die Erfüllung dieser Annahme sicher.

A.Zugriff stellt sicher, dass der Anwender volle Kontrolle über eingelegte Datenträger und Netzwerkfreigaben hat und somit die Vertrauenswürdigkeit der Umgebung sichergestellt ist. OE.Zugriff formuliert genau die gleichen Anforderungen und stellt somit explizit die Erfüllung dieser Annahme sicher.

T.DAT formuliert die Bedrohung, dass ein Angreifer mit hohem Angriffspotential mit beliebigen Mitteln eine Benutzerdatei manipuliert und die Manipulation bleibt unerkannt. OT.DAT formuliert als Sicherheitsziel die Errechnung eines Hashwertes über die Daten einer vom Benutzer definierten Datei. OE.SIG_DAT stellt sicher, dass eine elektronische Signatur über diesem Hashwert errechnet werden kann, und so eine signierte Datei (Datei + Signatur) erzeugt wird. OT.SIG_DAT formuliert dann das Sicherheitsziel, dass der EVG dem Benutzer ermöglichen muss, die Manipulation einer signierten Datei zu erkennen. Insgesamt kann der Benutzer eine Manipulation des Inhalts einer Datei mit Hilfe des EVG feststellen (der Benutzer muss die Funktionalität anfordern). Die Kombination dieser drei Sicherheitsziele wehrt die Bedrohung vollständig ab.

T.SIG_DAT formuliert die Bedrohung, dass einem Angreifer mit hohem Angriffspotential gelingt, eine signierte Datei zu manipulieren und die Manipulation bleibt unerkannt. OT.SIG_DAT formuliert das Sicherheitsziel, dass der EVG dem Benutzer ermöglichen muss, die Manipulation einer signierten Datei zu erkennen. Die Bedrohung wird somit vollständig abgewehrt.

T.EVG formuliert die Bedrohung, dass ein Angreifer mit hohem Angriffspotential Module bzw. Daten des EVGs austauscht oder manipuliert und die Manipulation bleibt unerkannt. OT.EVG formuliert das Sicherheitsziel, dass der EVG dem Benutzer ermöglicht, Manipulationen der Daten bzw. der Module des EVGs zu erkennen und wehrt damit die Bedrohung vollständig ab.

T.VOR_SIG formuliert die Bedrohung, dass ein Angreifer mit hohem Angriffspotential den Inhalt einer Datei manipuliert, bevor der Benutzer sich entscheidet, diese zu signieren und die Manipulation bleibt unerkannt. OT.VOR_SIG stellt sicher, dass eine Datei vom EVG derart dargestellt wird, dass der Benutzer den Inhalt der Datei eindeutig erkennen kann und wehrt die Bedrohung damit vollständig ab.

T.NACH_SIG formuliert die Bedrohung, dass ein Angreifer mit hohem Angriffspotential den Hashwert manipuliert, nachdem der Benutzer sich entschieden hat, den Signaturvorgang einzuleiten und die Manipulation bleibt unerkannt. OT.NACH_SIG stellt sicher, dass der EVG es dem Benutzer ermöglicht, die Manipulation einer zu unterschreibenden Datei nach der Entscheidung des Benutzers, einen Signaturvorgang einzuleiten, zu erkennen. Die Bedrohung wird somit vollständig abgewehrt.

8.2 Erklärungen der Sicherheitsanforderungen

Sicherheitsziele vs. Sicherheitsanforderungen	FCS_COP.1(SHA)	FCS_COP.1(160)	FCS_COP.1(RSA	FCS_COP.1(RSA	FDP_DAU.2	FDP_ITC.1(1)	FDP_ITC.1(2)	FDP_SVR.1	FTP_ITC.1	FCS_COP.1 (ES)
OT.DAT	x				x					
OT.SIG_DAT	x	x		x	x		x			
OT.EVG	x		x							
OT.VOR_SIG								x		
OT.NACH_SIG	x		x			x			x	
OE.SIG_DAT										x

Tabelle 3 Sicherheitsziele vs. Sicherheitsanforderungen

OE.SIG_DAT stellt sicher, dass die IT-Umgebung eine Funktionalität zur Verschlüsselung von kryptografischen Prüfsummen (Hashwerten) verfügbar macht. Diese geforderte Verschlüsselung wird durch FCS_COP.1 (ES) spezifiziert.

OT.DAT stellt sicher, dass der EVG Schutz gegen die Manipulation einer vom Benutzer definierten Datei durch die Errechnung eines Hashwertes über die Daten der Datei bietet. Der geforderte Schutz wird durch FDP_DAU.2 spezifiziert. FCS_COP.1(SHA) stellt die Forderung nach den unterstützenden kryptografischen Funktionen auf: Realisierung des Schutzes durch die Hashwertbildung (die Verschlüsselung des Hashwertes erfolgt in der Umgebung).

OT.SIG_DAT stellt sicher, dass es dem Benutzer möglich ist, eine Manipulation einer signierten Datei zu erkennen. Dies wird durch die Sicherheitsanforderung FDP_DAU.2 (insbesondere FDP_DAU.2.2) gefordert. FCS_COP.1(SHA), FCS_COP.1(160), FCS_COP.1(RSA2) und FDP_ITC.1(2) stellen die Forderungen für die unterstützenden kryptografischen Funktionen auf: Konkrete Realisierung durch die Hashwertberechnung und die Entschlüsselung mit einem importierten Schlüssel.

OT.EVG stellt sicher, dass es dem Benutzer möglich ist, Manipulationen der Komponenten bzw. der Daten des EVG zu erkennen. Dies wird durch die Sicherheitsanforderungen FCS_COP.1(SHA1) und FCS_COP.1(RSA1) sichergestellt.

OT.VOR_SIG stellt sicher, dass der EVG dem Benutzer eine zu unterschreibende Datei derart darstellen kann, dass der Benutzer in der Lage ist, den Inhalt der Datei eindeutig zu erkennen. Dies wird durch die Sicherheitsanforderungen FDP_SVR.1 sichergestellt.

OT.NACH_SIG stellt sicher, dass der EVG dem Benutzer ermöglicht, eine Manipulation des Hashwertes einer zu unterschreibenden Datei nach Erzeugung der Signatur, zu erkennen. Dies wird durch die Sicherheitsforderung FTP_ITC.1 sichergestellt. FCS_COP.1(SHA), FCS_COP.1(RSA1) und FDP_ITC.1(1) stellen die Forderungen für die unterstützenden kryptografischen Operationen auf.

8.2.1 Erklärung der Abhängigkeiten

Die Anforderungen an die Vertrauenswürdigkeit des EVG sind entsprechend EAL3 mit den Zusätzen AVA_MSU.3 und AVA_VLA.4 definiert worden.

Die Abhängigkeiten von AVA_MSU.3 werden durch die Komponenten ADO_IGS.1, ADV_FSP.1, AGD_ADM.1 und AGD_USR.1 aufgelöst. Die Abhängigkeiten von AVA_VLA.4 werden durch die Komponenten ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1 und AGD_ADM.1 aufgelöst. Die Abhängigkeit von ADV_IMP.1 wird durch die Komponente ALC_TAT.1 aufgelöst.

Die Abhängigkeiten der Sicherheitsanforderungen an den EVG und an die Umgebung sind nicht vollständig erfüllt. Die folgende Tabelle gibt einen Überblick über die Abhängigkeiten und zeigt wie diese erfüllt worden sind.

Anforderung	Abhängigkeit	Erfüllt
FCS_COP.1(SHA)	[FDP_ITC.1 oder FCS_CKM.1], FCS_CKM.4 und FMT_MSA.2	nein, siehe Erklärung unten
FCS_COP.1(160)	[FDP_ITC.1 oder FCS_CKM.1], FCS_CKM.4 und FMT_MSA.2	nein, siehe Erklärung unten
FCS_COP.1(RSA1)	[FDP_ITC.1 oder FCS_CKM.1], FCS_CKM.4 und FMT_MSA.2	nein, siehe Erklärung unten
FCS_COP.1(RSA2)	[FDP_ITC.1 oder FCS_CKM.1], FCS_CKM.4 und FMT_MSA.2	nein, siehe Erklärung unten
FCS_COP.1(ES)	[FDP_ITC.1 oder FCS_CKM.1], FCS_CKM.4 und FMT_MSA.2	nein, siehe Erklärung unten
FDP_DAU.2	FIA_UID.1	nein, siehe Erklärung unten
FDP_ITC.1(1)	[FDP_ACC.1 oder FDP_IFC.1], FMT_MSA.1	nein, siehe Erklärung unten
FDP_ITC.1(2)	[FDP_ACC.1 oder FDP_IFC.1], FMT_MSA.1	nein, siehe Erklärung unten
FDP_SVR.1	keine	ja, implizit
FTP_ITC.1	keine	ja, implizit

Tabelle 4 Abhängigkeiten der Sicherheitsanforderungen

FCS_COP.1(SHA) und FCS_COP.1(160) fordern einen kryptografischen Betrieb von schlüssellosen Hash-Algorithmen. In diesem Zusammenhang ist der Import bzw. Generierung/Zerstörung von Schlüsseln nicht anwendbar.

FCS_COP.1(RSA1) und FCS_COP.1(RSA2) beziehen sich auf einen kryptografischen Betrieb mit importierten öffentlichen Schlüsseln. Die Abhängigkeit vom Import (FDP_ITC.1) ist durch FDP_ITC.1(1) bzw. FDP_ITC.1(2) aufgelöst worden. Die Zerstörung des Schlüssels (FCS_CKM.4) und die sicheren Sicherheitsattribute (FDP_MSA.2) sind wegen der Verwendung eines öffentlichen Schlüssels nicht anwendbar im Kontext des EVG. Bei der Prüfung der Signatur über die EVG-Bestandteile FCS_COP.1(RSA1) wird überdies ein festcodierter öffentlicher Schlüssel verwendet, der nicht importiert wird. In diesem Fall ist zusätzlich die Abhängigkeit von FDP_ITC.1 nicht anwendbar.

FCS_COP.1(ES) bezieht sich auf die RSA Verschlüsselung, die in der Umgebung (Signaturkarte) geleistet wird. Die Art der Realisierung der Abhängigkeiten wird in der Umgebung entschieden und ist daher nicht weiter spezifiziert werden.

FDP_DAU.2 bezieht sich auf die Authentisierung der Daten. Der Nachweis der Identität des Benutzers wird durch die Information im Zertifikat bereitgestellt. Das Zertifikat wird mit dem Benutzer in der Umgebung durch geeignete Mittel hergestellt (siehe auch A.Plattform). Die Komponente FIA_UID.1 (Zeitpunkt der Identifikation) ist im Kontext des EVGs nicht anwendbar.

FDP_ITC.1(1) bzw. FDP_ITC.1(2) beziehen sich auf den Import öffentlicher Schlüssel für die Signaturprüfung (FCS_COP.1(RSA1) bzw. FCS_COP.1 (RSA2)). Die öffentlichen Schlüssel bedürfen keins Schutzes durch den EVG. Insbesondere wird weder eine Zugriffskontrolle (FDP_ACC.1) noch Informationsflusskontrolle (FDP_IFC.1) zur Erreichung der Sicherheitsziele des EVGs benötigt. Der Import erfolgt ohne Attribute und es werden nach dem Import keine Sicherheitsattribute initialisiert (FMT_MSA.3).

8.2.2 Erklärung der gegenseitigen Unterstützung

FCS_COP.1(SHA) und FCS_COP.1(ES) unterstützen sich gegenseitig bei der Erstellung elektronischer Signatur über eine Datei. FCS_COP.1(SHA) errechnet den Hashwert und FCS_COP.1(ES) verschlüsselt diesen. Beide Anforderungen tragen als konkrete Realisierung zur Erfüllung von FDP_DAU.2 bei. FDP_SVR sorgt für eine eindeutige Darstellung der Daten für den Benutzer. FTP_ITC.1 sorgt für die Übereinstimmung des zur Verschlüsselung gesendetes Hashwertes mit dem Wert der über eine vorher angezeigte Datei errechnet durch FCS_COP.1(SHA) errechnet wurde.

FCS_COP.1(SHA) und FCS_COP.1(RSA1) unterstützen sich gegenseitig bei der Prüfung einer Signatur. Beide Anforderungen tragen als konkrete Realisierung zur Erfüllung von FDP_DAU.2 (insbesondere FDP_DAU.2.2) bei. FCS_COP.1(SHA) berechnet den Hashwert und FCS_COP.1(RSA1) entschlüsselt den Hashwert aus der Signatur für einen Vergleich. Der Schlüssel wird durch FDP_ITC.1(1) bereitgestellt. Der Inhalt des zu der Signatur gehörendes Dokumentes wird eindeutig durch FDP_SVR dem Benutzer angezeigt.

FCS_COP.1(SHA) bzw. FCS_COP.1(160) und FCS_COP.1(RSA2) unterstützen sich gegenseitig bei der Prüfung einer Signatur. FCS_COP.1(SHA) bzw. FCS_COP.1(160) berechnet den Hashwert und FCS_COP.1(RSA2) entschlüsselt den Hashwert aus der Signatur für einen Vergleich. Der Schlüssel wird durch FDP_ITC.1(2) bereitgestellt.

8.3 Erklärung der Vertrauenswürdigkeitsanforderungen, EAL 3+ und SOF-hoch

Die vorgestellte Applikation ist ein Signaturanwendungskomponente nach §17 Abs. 2 des Signaturgesetzes. Um eine solche Komponente nach Common Criteria zu evaluieren wird mindestens die Vertrauenswürdigkeitsstufe EAL 3 mit Zusätzen benötigt. Die SigV fordert für solche Komponenten AVA_VLA.4 was eine Stärke der Funktionen (SOF) der Stärke „hoch“ benötigt. Weiterhin wird von der SigV gefordert, dass eine vollständige Missbrauchsanalyse durchgeführt wird, was die Wahl der Komponente AVA_MSU.3 begründet. Die zusätzlichen Komponenten ADV_IMP.1, ADV_LLD.1 und ALC_TAT.1 sind aufgenommen worden um die Abhängigkeiten (siehe Common Criteria Teil 3) der Komponenten AVA_VLA.4 und AVA_MSU.3 aufzulösen.

Die EAL 3 stellt einen bedeutenden Zuwachs an Vertrauenswürdigkeit gegenüber EAL2 dar, da sie ein vollständige Testabdeckung der Sicherheitsfunktionen, Mechanismen und/oder Prozeduren erfordert, die ein gewisses Vertrauen schaffen, dass der EVG während der Entwicklung nicht manipuliert wird.

8.4 Erklärungen der EVG Übersichtsspezifikation

Die Übersichtspezifikation verweist bei der Beschreibung der Sicherheitsfunktionen auf die entsprechenden Sicherheitsanforderungen, womit eine Erklärung gegeben worden ist. Die Nachfolgende Tabelle gibt zusätzlich dazu eine Übersicht über die Zuordnung der Sicherheitsfunktionen zu den Sicherheitsanforderungen.

Sicherheitsanforderungen vs. Sicherheitsfunktionen	**FCS_COP.1(SHA)**	**FCS_COP.1(160)**	**FCS_COP.1(RSA**	**FCS_COP.1(RSA**	**FDP_DAU.2**	**FDP_ITC.1(1)**	**FDP_ITC.1(2)**	**FDP_SVR.1**	**FTP_ITC.1**
SF1	x								
SF2	x	x		x	x		x		
SF3	x		x						
SF4	x		x						
SF5								x	
SF6	x		x			x			x

Tabelle 5 Sicherheitsanforderungen vs. Sicherheitsfunktionen

9 Definition der Familie FDP_SVR

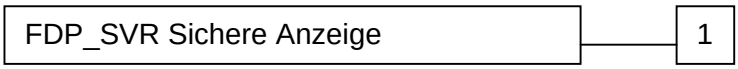
Um die funktionalen IT Sicherheitsanforderungen an den EVG zu definieren wird hier eine zusätzliche Familie (FDP_SVR) der Klasse FDP (Schutz der Benutzerdaten) definiert. Diese Familie beschreibt die funktionalen Anforderungen an eine sichere Anzeige im Umfeld elektronischer Signaturen.

FDP_SVR Sichere Anzeige

Familienverhalten

Diese Familie definiert Anforderungen an eine sichere Anzeige im Umfeld elektronischer Signaturen. In diesem Umfeld ist es erforderlich, dass der Benutzer den Inhalt des zu unterschreibenden Dokumentes eindeutig, ohne verdeckte bzw. aktive Inhalte informiert wird. Der Benutzer muss auf die nicht darstellbaren Inhalte hingewiesen werden.

Komponentenabstufung



FDP_SVR.1 Sichere Anzeige erfordert von den TSF die Fähigkeit zu einer eindeutigen Anzeige der Inhalte, die frei von verdeckten oder aktiven Inhalten ist, und zur Information des Benutzers über nicht darstellbare Inhalte.

Management: FDP_SVR.1

Für diese Komponente sind keine Management-Aktivitäten vorgesehen.

Protokollierung: FDP_SVR.1

Es sind keine Ereignisse identifiziert, die protokollierbar sein sollen, wenn FAU_GEN Generierung der Sicherheitsprotokolldaten Bestandteil des PP/ der ST ist.

FDP_SVR.1 Sichere Anzeige

Ist hierarchisch zu: Keinen anderen Komponenten

FDP_SVR.1.1 Die TSF müssen sicherstellen, dass der dem Benutzer angezeigte Inhalt eines Dokumentes entsprechend den folgenden Normen [Zuweisung: Normen für die Darstellung eines Inhalts] eindeutig ist.

FDP_SVR.1.2 Die TSF müssen sicherstellen, dass der dem Benutzer anzuzeigende Inhalt eines Dokumentes frei von aktiven oder verdeckten Inhalten ist. Die TSF müssen sicherstellen, dass der Benutzer darüber informiert wird.

FDP_SVR.1.3 Die TSF müssen sicherstellen, dass der Benutzer über einen nicht darstellbaren Inhalt eines anzuzeigenden Dokumentes informiert wird.

Abhängigkeiten: Keine Abhängigkeiten

10 Literaturverweise

[1] IT SICHERHEIT AUF BASIS DER COMMON CRITERIA, Hrsg. BSI – Bundesamt für Sicherheit in der Informationstechnik

[2] MAßNAHMENKATALOG FÜR TECHNISCHE KOMPONENTEN NACH DEM SIGNATURGESETZ STAND 15. JULI 1998, HRSG. REGTP

[3] VERORDNUNG ZUR ELEKTRONISCHEN SIGNATUR (SIGNATURVERORDNUNG – SIGV) VOM 16.11.2001, verordnet durch die Bundesregierung

[4] BEKANNTMACHUNG ZUR ELEKTRONISCHEN SIGNATUR NACH DEM SIGNATURGESETZ UND DER SIGNATURVERORDNUNG, Veröffentlicht im Bundesanzeiger Nr.48 – S.4202-4203 vom 11. März 2003

[5] DAS NEUE RECHT DER ELEKTRONISCHEN SIGNATUREN – KOMMENTIERENDE DARSTELLUNG VON SIGNATURGESETZ UND SIGNATURVERORDNUNG, BUNDESANZEIGER VERLAG, ISBN 3-89817-045-4

[6] EINHEITLICHE SPEZIFIZIERUNG DER EINSATZBEDINGUNGEN FÜR SIGNATURANWENDUNGSKOMPONENTEN VERSION 1.0, STAND 30.01.2002

[7] TIFF REVISION 6.0 FINAL DRAFT JUNE 3, 1992, ADOBE DEVELOPERS ASSOCIATION, HRSG.: ADOBE SYSTEMS INCORPORATED, 2585 CHARLESTON ROAD, P.O. BOX 7900, MOUNTAIN VIEW, CA 94039-7900

[8] BETRIEBSSYSTEM FÜR CHIPKARTEN TCOS V2.0 RELEASE 3, STAND JANUAR 2001, VERSION 1.07 HRSG: DEUTSCHE TELEKOM AG

[9] RFC 3447 – PUBLIC KEY CRYPTOGRAPHY STANDARDS (PKCS) #1: RSA CRYPTOGRAPHY SPECIFICATIONS VERSION 2.1, HRSG.:THE INTERNET SOCIETY (2003)

[10] HANDBUCH IM LIEFERUMFANG DES PRODUKTES

[11] GEEIGNETE ALGORITHMEN ZUR ERFÜLLUNG DER ANFORDERUNGEN NACH §17 ABS. 1 BIS 3 SIGG VOM 22.MAI 2001 IN VERBINDUNG MIT ANLAGE 1 ABSCHNITT 1 NR. 2 SIGV VOM 22.NOVEMBER 2001 MAINZ, 2003

[12] GESETZ ÜBER RAHMENBEDINGUNGEN FÜR ELEKTRONISCHE SIGNATUREN UND ZUR ÄNDERUNG WEITERER VORSCHRIFTEN (SIGG) VOM 16.05.2001 (BGB1.IS.876)

[13] VERORDNUNG ZUR ELEKTRONISCHEN SIGNATUR (SIGNATURVERORDNUNG – SIGV), 16.11.2001, VERORDNUNG DER BUNDESREGIERUNG