Zertifizierungsbericht

Zertifizierungs-Vorgang:	**TUVIT-DSZ-ITSEC-9151**
Produkt / System:	Anwenderkomponente DATEV Anwenderkomponente GERVA Version 1.31
Hersteller:	DATEV Datenverarbeitung und Dienstleistung für den steuerberatenden Beruf eG Paumgartner Straße 6-14 90329 Nürnberg
Auftraggeber:	s. o.
Prüfstelle:	TÜViT, Prüfstelle für IT-Sicherheit
Evaluierungsbericht:	Version 1.0 vom 12.01.2004 Dokument-Nummer: 20557748_60_TÜViT_001.01 Verfasser: Clemens Wanko, Stephan Di Nunzio
Formaler Ablauf:	vollständig / ordnungsgemäß durchgeführt
Ergebnis:	E2 / hoch
Evaluierungsauflagen:	keine
Prüfbegleiter:	Dr. Silke Götze
Zertifizierungsauflagen:	keine

Essen, den 12.01.2004

Dr. Christoph Sutter Dr. Silke Götze

Inhaltsverzeichnis

1 Grundlage und Gegenstand der Zertifizierung

Die Zertifizierung wurde auf Grundlage der Zertifizierungsbedingungen der Zertifizierungsstelle der TÜViT und des mit dem Bundesamt für Sicherheit in der Informationstechnik[1] abgestimmten Zertifizierungsschemas durchgeführt.

1.1 Evaluationsgegenstand (EVG) und Prüfkriterien

Die Zertifizierung der DATEV Anwenderkomponente GERVA, Version 1.31[2], ist eine Re-Zertifizierung auf der Basis der Zertifizierung TUVIT-DSZ-ITSEC-9146-2002 der Vorgängerversion GERVA, Version 1.2, die sich von dieser in den folgenden Punkten unterscheidet:

- im Windows Terminal Server (WTS)-Modus werden die Sicherheitsfunktionen zum Anstoßen einer qualifizierten elektronischen Signaturerzeugung und Prüfung einer qualifizierten elektronischen Signatur unterstützt,
- Anpassung des OCSP-Kommunikationsprotokoll zwischen dem Verzeichnisdienst und GERVA zur dynamischen Zertifikatsprüfung auf den ISIS-MTT Standard,
- Download von Verschlüsselungszertifikaten von einem LDAP Server,
- Etablierung einer Schnittstelle zum MS Cert Store für den Import von Verschlüsselungszertifikaten,
- Modifikationen innerhalb des GERVA-GUI,
- automatische Initiierung des Anmeldedialogs bei gesteckter SmartCard,
- Bugfix im Bereich PIN-Caching für fortgeschrittene elektronische Signaturen,
- Bugfix im Bereich Anzeige von Attributzertifikaten,
- Bugfix im Bereich Timing-Verhalten der SmartCard-API.

Die Zertifizierung hat die Funktionen zum Erstellen und Verifizieren qualifizierter elektronischer Signaturen nach Signaturgesetz (SigG)[3] der DATEV Anwenderkomponente GERVA, Version 1.31 der Firma DATEV Datenverarbeitung und Dienstleistung für den steuerberatenden Beruf eG, Paumgartner Straße 6-14, 90329 Nürnberg als Gegenstand und bescheinigt, dass diese auf Grundlage der *"Kriterien für die Bewertung der Sicherheit*

[1] Im folgenden kurz BSI genannt

[2] Im folgenden kurz GERVA genannt

[3] D.h. Funktionen, die dazu bestimmt sind, Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zuzuführen oder qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen

von Systemen der Informationstechnik Version 1.2 (1991)"[4] und des *„Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik Version 1.0 (1993)"*[5], gegen die produktspezifischen Sicherheitsvorgaben von der Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH[6] evaluiert wurde.

Ein Auszug aus ITSEC und ITSEM findet sich in Kapitel 4.

1.2 Durchführung der Evaluierung und Evaluierungsendbericht

Die Evaluierung wurde in der Zeit vom 27.01.2003 bis zum 12.01.2004 von Herrn Hans-Werner Blißenbach, Herrn Clemens Wanko, Herrn Stephan di Nunzio und Herrn Volker Nies durchgeführt. Die Leitung der Evaluierung wurde von Herrn Hans-Werner Blißenbach wahrgenommen und der Evaluierungsendbericht Version 1.0 vom 12.01.2004 (Nummer: 20557748_60_TÜViT_001.01) wurde von Herrn Clemens Wanko und Herrn Stephan di Nunzio erstellt.

1.3 Prüfergebnis der Evaluierung

Die Evaluierung wurde erfolgreich durchgeführt. Die Sicherheitsfunktionen werden gemäß den Sicherheitsvorgaben geleistet, was von den Prüfergebnissen bestätigt wird. Im Sinne von ITSEC handelt es sich bei dem Evaluationsgegenstand[7] um ein Produkt, welches folgende Sicherheitsfunktionalität aufweist:

- I & A Management,
- Speicherwiederaufbereitung,
- Zuführung von Daten zum Prozess der Erzeugung qualifizierter elektronischer Signaturen (unter Einsatz einer von einem Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 SigG herausgegebenen sicheren Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG),
- Prüfung einer qualifizierten elektronischen Signatur,
- Gültigkeitsprüfung von Zertifikaten,
- Übertragungssicherung.

Die angestrebte Evaluationsstufe **E2** wurde erreicht und die untersuchten Mechanismen besitzen die Mindeststärke **hoch**.

---

[4] Im folgenden kurz ITSEC genannt

[5] Im folgenden kurz ITSEM genannt

[6] Im folgenden kurz TÜViT genannt

[7] Im folgenden kurz EVG genannt

1.4 Erweiterung der Ergebnisse auf andere Konfigurationen

Der EVG ist durch die Versionsnummer (Version 1.31) eindeutig gekennzeichnet. Eine Erweiterung der Ergebnisse auf andere Konfigurationen des EVG ist nicht möglich.

Jede Änderung der Hardware/Firmware/Software seitens des EVG-Herstellers ist der Prüfstelle und der Zertifizierungsstelle anzuzeigen und zieht ggf. eine Re-Evaluation bzw. Re-Zertifizierung nach sich.

1.5 Auflagen, Hinweise und Empfehlungen aus der Evaluation

1.5.1 Auflagen, Hinweise und Empfehlungen für den Hersteller

Der Evaluierungsendbericht enthält keine Auflagen, Hinweise oder Empfehlungen für den Hersteller.

1.5.2 Hinweise, Empfehlungen und Auflagen für den Anwender

Der Evaluierungsendbericht enthält folgende Hinweise und Empfehlungen für den Anwender:

- Nur bei dem Betrieb eines bestätigten PIN-Pad Lesers im PIN-Pad Modus (Klasse 2 Leser) ist sichergestellt, dass die PIN nur zur SmartCard übertragen wird,
- die GERVA Einstellungen können durch andere Computernutzer auch ohne SmartCard Anmeldung verändert werden,
- nur die qualifizierte Signaturerzeugung über den GERVA Drucker beinhaltet eine sichere Darstellung des Dateiinhalts der zu signierenden Daten,
- für Filesignaturen aus dem Windows Explorer enthält GERVA nur dann eine Referenz auf den Dateinamen, wenn die Anzeige der Statuszeile nicht über „Ansicht – Statuszeile“ abgewählt wurde,
- die GERVA Makros sind verfügbar in Microsoft Word und Microsoft Excel und können nur ausgeführt werden, wenn die Sicherheitseinstellungen für Makros dort unter „Extras – Makros“ nicht auf „hoch“ gesetzt sind.

1.6 Zertifizierungsauflagen und Hinweise

1.6.1 Zertifizierungsauflagen

Es existieren keine Auflagen.

1.6.2 Zertifizierungshinweise für den Anwender

Es existieren keine Hinweise für den Anwender.

1.7 Unabhängigkeit des Prüfbegleiters

Der Prüfbegleiter hat innerhalb der letzten 2 Jahre für das die Zertifizierung beauftragende Unternehmen keine Beratungen oder sonstige Dienstleistungen erbracht und mit diesem Unternehmen auch keine Beziehungen gepflegt, die seine Beurteilung beeinflussen könnten.

Der Prüfbegleiter ist zu keiner Zeit an Prüfverfahren für das dem Zertifizierungsvorgang zugrunde liegende Produkt beteiligt gewesen.

2 Zusammenfassung der Sicherheitsvorgaben

2.1 Definition des EVG und Art der Nutzung

2.1.1 Definition des EVG

Der Evaluationsgegenstand besteht ausschließlich aus den GERVA-Funktionen zum Erstellen und Verifizieren qualifizierter elektronischer Signaturen nach Signaturgesetz (SigG) der Anwenderkomponente GERVA, Version 1.31. Diese Funktionen werden in einem Teil von GERVA in Software realisiert. Nur dieser Teil der Software bildet den EVG.

Der EVG besteht aus den in der folgenden Tabelle angegebenen Dateien:

Dateiname	Datum	Zeit	Dateigrösse [Bytes]
Gerva:			
TRUSTED.RTF	28.08.03	16:04	14.267
ANWENDUNG.ICO	16.06.03	13:58	766
BMP_AUSDRUCK.ICO	21.01.03	07:22	318
CERT.ICO	16.06.03	13:59	766
CERT_UEBERNEHMEN.ICO	16.06.03	13:59	766
CLSDFOLD.ICO	16.06.03	13:59	766
DISIG004.ICO	21.01.03	07:22	766
DISIG005.ICO	21.01.03	07:22	766
DISIG006.ICO	21.01.03	07:22	766
DISIG009.ICO	21.01.03	07:22	766
DISIG010.ICO	21.01.03	07:22	766
DISIG011.ICO	21.01.03	07:22	766
DISIG012.ICO	21.01.03	07:22	766

DISIG015.ICO	21.01.03	07:22	766
DISIG016.ICO	21.01.03	07:22	766
DISIG017.ICO	16.06.03	13:59	766
DISIG018.ICO	16.06.03	13:59	766
DISIG019.ICO	16.06.03	14:00	766
DISIG020.ICO	16.06.03	14:00	766
DISIG021.ICO	16.06.03	14:00	766
DISIG022.ICO	16.06.03	14:00	766
DISIG023.ICO	16.06.03	14:00	766
DISIG024.ICO	21.01.03	07:22	766
DISIG025.ICO	16.06.03	14:00	766
DOC_GERVA.ICO	16.06.03	14:01	766
GERVA.CUR	21.01.03	07:22	766
IEXPLORER.ICO	21.01.03	07:22	318
KOMVW404.ICO	21.01.03	07:22	318
KOMVW415.ICO	21.01.03	07:22	318
KOMVW416.ICO	21.01.03	07:22	318
KOMVW434.ICO	21.01.03	07:22	318
KOMVW435.ICO	21.01.03	07:22	318
OPENFOLD.ICO	16.06.03	14:01	766
STARTUP.BMP	21.01.03	07:22	97.880
STATUS_NOTOK.ICO	21.01.03	07:22	318
STATUS_OK.ICO	21.01.03	07:22	318
STATUS_UNKNOWN.ICO	21.01.03	07:22	318
UNZEITSTEMPEL.ICO	16.06.03	14:01	766
ZEITSTEMPEL3.ICO	16.06.03	14:01	766
ZERTIFIKAT.ICO	16.06.03	14:01	766
DATEVADDINGERVA.MTF	25.08.03	15:18	130.946
DATEVADDINGERVA.OCX	08.12.03	15:01	4.337.703
DATEVSHOWDOCUMENT.OCX	06.08.03	15:47	208.896
BYTEBUFFERSVR.DLL	03.07.03	14:12	143.360
OCSPSVR.DLL	04.07.03	08:55	602.112

EXCHANGENOTIFYSVR.EXE	16.08.01	07:15	180.224
EXCHANGENOTIFYSVRPS.DLL	16.08.01	07:15	36.864
GERVASHEXT.DLL	01.07.03	13:12	114.688
GERVATSS.DLL	29.08.02	14:05	151.552
CRYPTOSEALOCX.OCX	12.09.03	15:24	1.425.408
DVSigE2:			
DVCServ.EXE	15.09.03	11:03	327.680
DvckService.EXE	15.09.03	11:03	65.536
DvckServdll.DLL	15.09.03	11:03	262.144
DVCCSAckE2002.DLL	10.09.03	12:17	90.112
DVCCSAckshareE2002.DLL	10.09.03	12:16	98.304
DVCCSActapi002.DLL	21.07.03	09:20	114.688
DVCCSApE2002.DLL	10.09.03	12:16	90.112
DVCCSAsigE2Proc002.DLL	10.09.03	12:17	122.880
DVCCSADialogAddInE2001.OCX	10.09.03	12:16	159.744
DVCCSACrypto002.DLL	29.08.02	10:32	421.888
Rsa_w32E2.DLL	11.03.96	16.23	30.208
DVCCSAsigE2002.dll	24.09.03	12:21	86.016
DVCCSAWTSClientSigE2002.dll	24.09.03	12:21	81.920
SmartCard-API:			
DVCCSAAsn1002.DLL	15.09.03	11:02	139.264
DVCCSAbaseProc002.DLL	15.09.03	11:02	118.784
DVCCSAckshare002.DLL	12.12.03	14:48	135.168
DVCCSAbase002.dll	07.10.03	16:56	131.072
DVCCSAWTSClientBase002.dll	24.09.03	12:21	81.920
Komprimierung			

DUZACTX.DLL	12.09.00	10.30	229.376
DZACTX.DLL	12.09.00	10.30	249.856

Neben den in obiger Tabelle angegebenen Dateien, werden noch weitere zu GERVA gehörige Dateien, die allerdings nicht Bestandteil des EVG sind, ausgeliefert. Darüber hinaus wird noch die folgende Betriebsdokumentation ausgeliefert:

Titel	Version
Benutzerdokumentation für die signaturgesetzkonforme DATEV Anwenderkomponente GERVA der Version 1.31	3.3, 18.12.2003
Systemverwalterdokumentation für die signatur-gesetzkonforme DATEV Anwenderkomponente Gerva der Version 1.31	1.3, 12.12.2003

Der EVG führt die eigentliche Signaturerzeugung nicht selbst durch, sondern bildet nur einen Hashwert über die ihm übergebenen Daten und leitet diese an eine sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG (Signaturkarte[8]) weiter. Die Signaturerzeugung findet in der Signaturkarte statt. Funktionen zum Erzeugen der Schlüssel auf der Signaturkarte und zur Personalisierung der Signaturkarte sind nicht Bestandteil des EVG.

GERVA erlaubt auch die Nutzung nicht SigG-konformer Signaturkarten der DATEV eG für die Ausführung sogenannter Service-Funktionen (Ver- und Entschlüsseln, Komprimieren, nicht SigG-konformes Signieren oder Verifizieren von Daten). Diese Funktionalität ist nicht Gegenstand der Evaluation.

2.1.2 Art der Nutzung

GERVA kann sowohl in der Einzelplatzversion als auch in einer Windows Terminal Server (WTS)-Umgebung eingesetzt werden.

Auf einem Einzelplatzrechner können von GERVA elektronische Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zugeführt und damit mit Hilfe von Chipkartensystemen (Chipkartenleser und personalisierte Chipkarte als sichere Signaturerstellungseinheit) mit einer qualifizierten elektronischen Signatur versehen sowie erstellte Signaturen verifiziert werden.

In der WTS-Umgebung werden die selben Funktionalitäten zur Verfügung gestellt. Im Unterschied zur Einzelplatzversion prägt GERVA in der WTS-Umgebung eine Client-

[8] Bemerkung: Die Signaturkarte gehört nicht zum EVG.

Server Architektur, wobei GERVA als Anwendung auf einem Terminal- Server (WTS-Server) ausgeführt wird und ein Anwender über seinen Terminal Server Client (WTS-Client) diese Anwendung nutzen kann. Dabei werden die Bildschirmdaten vom WTS-Server zum WTS-Client übertragen. Der WTS-Client liefert Tastatureingaben wie auch Mausbewegungen an den WTS-Server zurück. Der WTS-Client präsentiert dem Anwender über ein Bildschirmfenster die gleiche grafische Windows-Benutzeroberfläche wie die der GERVA-Anwendung in der Einzelplatzversion und ermöglicht ihm die Interaktion mit der auf dem Server ausgeführten Applikation. Die Aufbereitung der zu signierenden Daten (insbes. die Hashwertbildung) erfolgt auf dem WTS-Server, die Signaturerstellung erfolgt mit dem Chipkartensystem am WTS-Client.

Vor **Erstellung einer qualifizierten elektronischen Signatur** mit einer Signaturkarte werden dem Benutzer die zu signierenden Daten visualisiert (GERVA-Drucker) oder die Dateinamen der zu signierenden Dateien dargestellt (Filesignaturen). Die Signaturerstellung auf der Signaturkarte erfolgt immer erst nach expliziter Benutzer-Bestätigung durch Eingabe der Chipkarten-PIN für die qualifizierte elektronische Signatur. Der EVG erzeugt über die zu signierenden Daten einen Hashwert mit Hilfe einer für qualifizierte elektronische Signaturen zugelassenen Hashfunktion, der dann in der Signaturkarte mit dem privaten Signaturschlüssel verschlüsselt wird. Der EVG prüft die so erstellte Signatur auf Übereinstimmung mit dem ursprünglich berechneten Hashwert und legt die signierten Daten, die Signatur, das Zertifikat des Signaturschlüssel-Inhabers, sowie das CA-Zertifikat in einen PKCS#7 Datencontainer. Der EVG erzeugt in Abhängigkeit der Konfiguration bzgl. der Anbindung eines Zeitstempeldienstes zwei mögliche Varianten des PKCS#7 Datencontainers. Ist der EVG so konfiguriert, dass er keinen Online-Zeitstempel einholt, dann enthält der PKCS#7 Datencontainer keinen Zeitstempel. Bei der Signaturprüfung wird der Verifikationszeitpunkt als Prüfzeitpunkt verwendet. Holt der EVG einen SigG-Online-Zeitstempel ein, dann enthält der PKCS#7 Datencontainer einen Zeitstempel, die Zeitangabe aus dem Zeitstempel wird bei der Prüfung der Signatur als Prüfzeitpunkt verwendet.

Zum **Verifizieren einer qualifizierten elektronischen Signatur** wird die qualifizierte elektronische Signatur selbst durch mathematische Prüfung des Hashwerts und anschließende Prüfung der Zertifikatskette bis hin zum Root-Zertifikat (Zertifikat der RegTP) aus der Signaturkarte durchgeführt. Zusätzlich kann der EVG eine Gültigkeitsprüfung (Sperrstatus) des Signaturschlüsselzertifikates eines Unterzeichners mit Hilfe einer Verzeichnisdienstanfrage an den entsprechenden Verzeichnisdienst durchführen. Bei der Signaturprüfung wird in Abhängigkeit davon, ob ein Zeitstempel vorhanden ist, der Zeitstempel oder der Verifikationszeitpunkt als Prüfzeitpunkt verwendet.

2.2 Angenommene Einsatzumgebung

Der EVG wird in einer zugangsgeschützten Umgebung eingesetzt, so dass nur autorisierte Mitarbeiter Zugang zu Arbeitsplatzrechnern bzw. Servern haben.

- Einsatz auf einem Einzelplatzrechner

  Der EVG ist auf einem Einzelplatzrechner in einer Büroumgebung installiert und wird dort lokal ausgeführt.

- Einsatz auf einem WTS-Terminal-Server

  Der EVG ist auf einem WTS-Server in einer geschützten Server-Umgebung installiert und wird von WTS-Clients auf dem WTS-Server ausgeführt. Die Netzwerkverbindung zwischen Server und Clients erfolgt über ein LAN oder ein WAN. Auf dem WTS-Server selbst kann der EVG nicht lokal ausgeführt werden.

- Einsatz auf einem WTS-Terminal-Client

  Der EVG ist auf einem WTS-Client installiert, der über ein LAN oder WAN mit einem WTS-Server verbunden ist, auf dem der EVG in einer WTS Terminal Session ausgeführt wird. Die Anzeige von Bildschirmdaten des EVG, sowie Tastatur-/Mauseingaben und Chipkartenleseranbindung erfolgen lokal auf dem WTS-Client. Daneben kann der EVG auf einem WTS-Client auch lokal wie auf einem Einzelplatzrechner ausgeführt werden.

2.2.1 Technische Einsatzumgebung

Als erforderliche Plattform für den Einsatz des EVG ist vorgesehen:

Der EVG wird lokal in einer Büroumgebung mit Zugangsschutz eingesetzt, so dass nur autorisierte Mitarbeiter Zugang zum Arbeitsplatzrechner haben, und auf einem nur lesbaren Medium zusammen mit einem speziellen Integritätsprüfprogramm zur Verifikation der ausgelieferten Bestandteile des EVG ausgeliefert. Als erforderliche HW-/SW-Plattform für den Einsatz des EVG sind vorgesehen:

- IBM-kompatibler PC lauffähig mit einem der unten genannten Windows Betriebssysteme, mit Anschlussmöglichkeiten für ein Read-Only-Memory-Laufwerk (z.B. CD-ROM) sowie für einen Chipkartenleser (serielle Schnittstelle oder PCMCIA) und mit einer Netzwerkverbindung
- Betriebssysteme (Arbeitsplatzmodus bzw. WTS-Client):
  Windows 98 Second Edition, Windows NT4 Workstation und Windows 2000, Windows XP Home Edition, Windows XP Professional
- Betriebssysteme (WTS-Server):
  Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server

- Betriebssystemzusatz (WTS-Client bzw. WTS-Server):
  Microsoft High Encryption Pack für 128 Bit Verschlüsselung der WTS-Verbindung
- Klasse 2 Chipkartenleser mit PIN-Pad, der die sichere Eingabe der PIN unterstützt. In die Zertifizierungstests wurde der Leser SCM SPR 532 pinpad einbezogen. Es werden funktional jedoch auch andere PC/SC oder CT-API Chipkartenleser an der seriellen oder USB-Schnittstelle unterstützt.
- Personalisierte DATEV Signaturkarte e:secure-Card V1.0 mit einer Schnittstelle nach ISO 7816 und Chipkartenbetriebssystem TCOS V2.0 Release 3 der Deutsche Telekom AG
- Netzwerkverbindung zum DATEV-Zertifizierungsdienst (Verzeichnisdienst und Zeitstempeldienst)

2.2.2 Administrative Einsatzumgebung

An die Einsatzumgebung beim Endanwender werden folgende Annahmen gestellt:

- Für eine vollständige Prüfung der Zertifikatskette muss zusätzlich auf anderem Wege überprüft werden, ob die verwendeten Zertifikate des Zertifzierungsdiensteanbieters im Verzeichnisdienst der RegTP vorhanden und nicht gesperrt sind.
- Die authentischen Root CA- und CA-Zertifikate müssen durch den Anwender bereitgestellt sein.
- Es wird eine vertrauenswürdige Eingabe der PIN vorausgesetzt. Der Benutzer hat dafür Sorge zu tragen, dass die Eingabe der PIN weder beobachtet wird noch dass die PIN anderen Personen bekannt gemacht wird.
- Zur Nutzung der GERVA-API dürfen nur vertrauenswürdige externe Applikationen verwandt werden.
- Die Einstellung der Systemzeit des Personalcomputers und ggf. des Servers muss korrekt sein.
- Bei Nutzung eines Terminal Server Clients muss sichergestellt sein, dass dieser über eine entsprechende Netzwerkanbindung verfügt, die es ihm ermöglicht den Server zu kontaktieren.
- Der Personalcomputer, auf dem GERVA verwendet wird, muss gegen eine unberechtigte Benutzung gesichert sein. Der Benutzer des Computers muss sich davon überzeugen, dass jede auf diesem Computer installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert wurde, um Daten auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. Insbesondere ist sicherzustellen, dass auf der von GERVA verwendeten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.

- Der Benutzer muss sich ebenfalls davon überzeugen, dass sein verwendeter Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wurde, um Daten auszuforschen oder zu verändern.
- Der Benutzer hat sich regelmäßig von der Korrektheit seines Systems zu überzeugen. Dazu gehören die Integritätsprüfung von GERVA und die Aktualitätsprüfung der Rechnerzeit.
- Eine vertrauenswürdige Administration des Personalcomputers sowie der Internet- bzw. Intranetanbindung muss sichergestellt werden. Bei Einsatz von GERVA in der WTS-Umgebung muss zusätzlich eine vertrauenswürdige Administration des Servers im 4-Augen-Prinzip gewährleistet sein.

2.3 Subjekte, Objekte und Zugriffsarten / Aktionen

Subjekte, Objekte und Zugriffsarten/Aktionen sind nicht definiert. Die Sicherheitspolitik ergibt sich direkt aus dem Signaturgesetz und der Signaturverordnung und ist in den Sicherheitszielen niedergelegt (siehe Abschnitt 2.4.2).

2.4 Bedrohungen und Sicherheitsziele

2.4.1 Bedrohungen

Für den angenommenen Einsatz von GERVA werden die folgenden 7 Bedrohungen angenommen:

B1: Die Signaturerstellung erfolgt durch eine Person, die nicht tatsächlich Signaturschlüssel-Inhaber ist.

B2: Unberechtigte Personen könnten versuchen, die Identifikationsdaten (hier: PIN) auszuspähen.

B3: Die Erzeugung der qualifizierten elektronischen Signatur erfolgt ohne vorhergehende Willenserklärung.

B4: Dem Anwender werden andere Daten angezeigt als jene, die er qualifiziert elektronisch signiert.

B5: Die zu signierenden Daten werden nach ihrer Anzeige vor dem Signieren manipuliert.

B6: Unberechtigte Personen könnten versuchen, unbemerkte Veränderungen an signierten Daten, Signaturen und Zertifikaten vorzunehmen.

B7: Nicht authentische Aussagen über die Zertifikatsprüfungen werden nicht als solche erkannt. (Dies beinhaltet bereits Zertifikatsprüfungen über die API-Schnittstelle durch externe Applikationen.)

2.4.2 Sicherheitsziele und Sicherheitseigenschaften

Der EVG hat die folgenden aus § 17 Abs. 2 SigG und § 15 Abs. 2 SigV abgeleiteten 5 Sicherheitsziele:

SZ1: Der Signiervorgang ist eine durch den Benutzer ausgelöste und bewusste Handlung und wird vor jeder Signaturerzeugung eindeutig angezeigt.

SZ2: Die zu signierenden Daten werden der signierenden Person eindeutig angezeigt. Der Benutzer muss die Daten, auf die sich die Signatur erstrecken soll, eindeutig bestimmen können.

SZ3: Die Korrektheit der qualifizierten elektronischen Signatur wird zuverlässig geprüft (im Sinne, dass Modifikationen bzw. Verfälschungen von signierten Daten und qualifizierten elektronischen Signaturen im Nachhinein erkannt werden können) und zutreffend angezeigt.

SZ4: Die Gültigkeit der Zertifikate muss derart überprüft werden können, dass eindeutig erkannt wird, ob die nachgeprüften Zertifikate zu einem angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

SZ5: Der Signaturschlüsselinhaber der signierten Daten sowie die signierten Daten selbst sind für eine prüfende Person eindeutig feststellbar.

2.5 Sicherheitsfunktionen

Zur Erreichung des Sicherheitsziels und zur Abwehr der Bedrohungen enthält der EVG die folgenden 5 sicherheitsspezifischen Funktionen:

SF1: I & A Management (mit Speicherwiederaufbereitung)

SF1 sorgt für eine sichere Identifikation und Authentisierung des Anwenders mittels seiner Signaturkarte bevor signaturgesetzrelevante Aktionen ausgeführt werden können. GERVA übermittelt hierbei, falls kein Klasse 2 Leser im PIN-PAD Modus eingesetzt wird, die vom Benutzer eingegebene PIN gesichert zur Signaturkarte. Nach Übergabe der PIN wird der Speicher derart aufbereitet, dass nachträglich keine Informationen über die PIN ausgespäht werden können.

SF2: Anstoßen der Erzeugung einer qualifizierten elektronischen Signatur (ES)

SF2 kann zwei unterschiedliche Varianten zur Erzeugung qualifizierter elektronischer Signaturen auf der Signaturkarte anstoßen:

- über die Initiierung eines Druckereignisses:

  Die zu signierenden Daten werden zunächst dem Benutzer in Form eines Bitmaps visualisiert, damit dieser feststellen kann, auf welche Daten sich die zu erstellende Signatur bezieht.

- über beliebige Dateien:

  Es ist möglich beliebige Dateien unabhängig vom Dateityp qualifiziert elektronisch zu signieren. Es erfolgt hier keine Visualisierung der Datei.

In beiden Fällen erfolgt die Signaturerstellung mit der Signaturkarte erst nach expliziter Bestätigung durch den unterzeichnenden Benutzer. Die qualifizierte elektronische Signatur kann unter der Nutzung des Zeitstempeldienstes des Zertifizierungsdiensteanbieters DATEV mit einem Zeitstempel versehen werden. Nach erfolgter Signatur wird diese auf Korrektheit geprüft und in einem Datencontainer abgelegt. Hierbei enthält der Datencontainer je nach Konfiguration entweder keinen Zeitstempel oder einen Online-Zeitstempel.

SF3: Prüfung einer qualifizierten elektronischen Signatur

SF3 prüft eine qualifizierte elektronische Signatur gemäß Signaturgesetz durch Prüfung der mathematischen Korrektheit durch Vergleich eines selbst gebildeten Hashwertes mit dem Signaturhashwert des signierten Dokumentes. Gleichzeitig wird die mathematische Korrektheit der Zertifikatskette der Signaturzertifikate bis zum Root- Zertifikat der RegTP geprüft. Letzteres muss GERVA authentisch zur Verfügung gestellt werden.

Das Ergebnis der Signaturprüfung wird dem Benutzer angezeigt, mögliche Ergebnisse sind:

- Signatur korrekt
- Signatur nicht korrekt

Die Prüfung einer qualifizierten elektronischen Signatur kann ebenfalls durch eine externe Applikation über die GERVA-API initiiert werden. Das Ergebnis der Signaturprüfung wird an die Applikation übergeben.

SF4: Gültigkeitsprüfung von Zertifikaten

SF4 prüft mittels einer OCSP-Anfrage, ob das übermittelte Zertifikat zum aktuellen Zeitpunkt im Verzeichnis des Zertifizierungsdiensteanbieters vorhanden und nicht gesperrt ist. Dabei wird gleichzeitig auch die Gültigkeit der Signatur der Verzeichnisdienstauskunft geprüft. Die Gültigkeitsprüfung realisiert SF4 in zwei Varianten als Online- oder Offlineprüfung. Der EVG verwendet in Abhängigkeit des zu prüfenden Datencontainers (siehe auch SF2) unterschiedliche Prüfzeitpunkte. Ist kein Zeitstempel vorhanden, so wird der Verifikationszeitpunkt als Prüfzeitpunkt verwendet. Andernfalls wird der im Zeitstempel vorhandene Signaturzeitpunkt als Prüfzeitpunkt verwendet.

Die Gültigkeitsprüfung in GERVA erfolgt nach dem Kettenmodell (siehe dazu auch SigG-Model. Die Sicherheitsanker, d. h. die Zertifikate der Wurzelstelle müssen dem

EVG authentisch zur Verfügung gestellt werden. Das Ergebnis der Gültigkeitsprüfung wird dem Benutzer angezeigt.

SF5: Übertragungssicherung

SF5 sichert die Übertragung von Identifikationsdaten (PIN) zwischen GERVA und der Chipkarte gegen Mitlesen im Falle des Einsatzes eines Klasse 1 Kartenlesers ohne Pinpad.

2.6 Korrelation Sicherheitsfunktionen / Bedrohungen / Sicherheitsziele

Die folgende Tabelle zeigt welche Sicherheitsfunktionen den jeweiligen Bedrohungen entgegenwirkt:

	SF1	SF2	SF3	SF4	SF5
B1	X				X
B2	X				X
B3		X			
B4		X			
B5		X			
B6			X		
B7			X	X	

Die Sicherheitsfunktionen sind für die vorgesehene Art der Nutzung der Anwenderkomponente GERVA sowohl geeignet als auch zweckmäßig. Im einzelnen gilt dabei folgendes:

SF1 wirkt der Bedrohung B1 entgegen, da sich ein Benutzer vor der Nutzung des privaten Signaturschlüssels mit seiner nur ihm bekannten PIN authentisieren muss.

SF1 wirkt der Bedrohung B2 entgegen, da die PIN zu keinem Zeitpunkt innerhalb eines resistenten Speichers abgelegt wird. Der flüchtige Speicherbereich, welcher die PIN während der Identifizierung und Authentisierung aufnimmt, wird anschließend wieder aufbereitet.

SF2 wirkt der Bedrohung B3 entgegen, da die Signatur erst nach der Bestätigung des unterzeichnenden Benutzers durchgeführt wird.

SF2 wirkt den Bedrohungen B4 und B5 entgegen, da die zu signierenden Daten dem Anwender einerseits vor dem Signiervorgang eindeutig angezeigt werden und nach der Signaturerstellung in der Chipkarte vom EVG nochmals überprüft wird, ob die

(entschlüsselte) Signatur mit dem zuvor an die Chipkarte gesendeten Hashwert übereinstimmt.

SF3 wirkt der Bedrohung B6 entgegen, da mit dieser Sicherheitsfunktion Manipulationen an signierten Daten, Signaturen und Zertifikaten erkannt werden können.

SF3 wirkt der Bedrohung B7 entgegen, da mit dieser Sicherheitsfunktion die Authentizität bezüglich der Zertifikatsprüfung sichergestellt werden kann.

SF4 wirkt der Bedrohung B7 entgegen, da mit dem OCSP-Request eine authentische Zertifikatsprüfung durchgeführt werden kann.

SF5 wirkt der Bedrohung B1 entgegen, da die zum Erzeugen von qualifizierten elektronischen Signaturen benötigte PIN auf sicherem Weg an die Chipkarte übermittelt wird.

SF5 wirkt der Bedrohung B2 entgegen, da die PIN auf sicherem Wege an die Chipkarte übermittelt wird und auf diesem Wege nicht ausgespäht werden kann.

2.7 Evaluationsstufe und Mechanismenstärke

Die vom Antragsteller angestrebte Evaluationsstufe ist **E2**.

Die vom Antragsteller angestrebte Mindeststärke der Mechanismen ist **hoch**.

3 Ergebnisse der Evaluierung

3.1 Wirksamkeit – Konstruktion

3.1.1 Aspekt 1: Eignung der Funktionalität

ITSEC 3.14 *Die Analyse der Eignung muss die sicherheitsspezifischen Funktionen und Mechanismen den in den Sicherheitsvorgaben identifizierten Bedrohungen zuordnen, denen sie entgegenwirken müssen.*

ITSEC 3.15 *Die Analyse der Eignung muss zeigen, wie die sicherheitsspezifischen Funktionen und Mechanismen den identifizierten Bedrohungen entgegenwirken. Sie muss zeigen, dass es keine identifizierten Bedrohungen gibt, denen nicht eine oder mehrere der aufgeführten sicherheitsspezifischen Funktionen angemessen entgegenwirken.*

ITSEC 3.16 *Es ist zu überprüfen, ob die Analyse der Eignung alle Anforderungen hinsichtlich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die Analyse der Eignung alle Anforderungen an Inhalt, Form und Nachweise (ITSEC 3.14,

3.15) erfüllt sowie alle relevanten Informationen verwendet hat. Die Zuordnungen der Sicherheitsfunktionen zu den Bedrohungen sind in Abschnitt 2.6 dargestellt.

3.1.2 Aspekt 2: Zusammenwirken der Funktionalität

ITSEC 3.18 *Die Analyse des Zusammenwirkens muss eine Analyse aller möglichen Beziehungen zwischen den sicherheitsspezifischen Funktionen und Mechanismen zur Verfügung stellen.*

ITSEC 3.19 *Die Analyse des Zusammenwirkens muss zeigen, dass es nicht möglich ist, eine sicherheitsspezifische Funktion oder einen Mechanismus dazu zu veranlassen, mit den Aufgaben anderer sicherheitsspezifischer Funktionen oder Mechanismen in Konflikt zu geraten oder ihnen entgegenzuwirken. Diese Analyse muss unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

ITSEC 3.20 *Es ist zu überprüfen, ob die Analyse des Zusammenwirkens alle Anforderungen hinsichtlich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die Analyse des Zusammenwirkens alle Anforderungen an Inhalt, Form und Nachweise (ITSEC 3.18, 3.19) erfüllt sowie alle relevanten Informationen verwendet hat.

3.1.3 Aspekt 3: Stärke der Mechanismen

ITSEC 3.22 *Die Analyse der Stärke der Mechanismen muss alle sicherheitsspezifischen Mechanismen auflisten, die innerhalb des EVG als kritisch festgestellt wurden. Sie muss Analysen über die Algorithmen, Prinzipien und Eigenschaften enthalten, die diesen Mechanismen zugrundeliegen oder sie muss auf solche Analysen verweisen.*

ITSEC 3.23 *Die Analyse der Stärke der Mechanismen muss aufzeigen, dass alle kritischen Mechanismen die Definition der beanspruchten Einstufung der Mindeststärke, wie in den Paragraphen 3.6 bis 3.8 beschrieben, erfüllen: im Fall von kryptographischen Mechanismen muss dies durch eine Aussage der zuständigen nationalen Behörde erfolgen. Andere Analysen müssen unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

ITSEC 3.24 *Es ist zu überprüfen, ob alle Mechanismen, die kritisch sind, als solche identifiziert wurden. Es ist zu überprüfen, ob die vorgelegte Analyse der Stärke der Mechanismen alle Anforderungen bezüglich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Es ist zu überprüfen, ob die Spezifikationen/Definitionen aller kritischen Mechanismen die beanspruchte Mindeststärke gewährleisten. Wo erforderlich, sind* ***Penetrationstests*** *durchzuführen, um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen.*

Feststellung der Zertifizierungsstelle: Im Prüfobjekt werden alle kritischen Mechanismen in Typ A und B Mechanismen unterschieden. Die Prüfstelle hat überprüft und festgestellt,

dass alle Mechanismen, die kritisch sind, als solche identifiziert wurden. Die vorgelegte Analyse der Stärke der Mechanismen erfüllt alle Anforderungen an Inhalt, Form und Nachweise (ITSEC 3.22, 3.23) und verwendet alle relevanten Informationen. Die Spezifikationen/Definitionen aller kritischen Mechanismen gewährleisten die geforderte Mindeststärke hoch. Von der Prüfstelle wurden Penetrationstests durchgeführt, welche die Mindeststärke der Mechanismen hoch bestätigen.

3.1.4 Aspekt 4: Bewertung der Konstruktionsschwachstellen

ITSEC 3.26 *Die Liste der Schwachstellen, die durch den Antragsteller vorgelegt werden muss, muss alle ihm bekannten Schwachstellen in der Konstruktion des EVG aufführen. Sie muss jede Schwachstelle ansprechen, eine Analyse ihrer möglichen Auswirkungen beinhalten und die Maßnahmen aufzeigen, die zur Abhilfe vorgeschlagen oder zur Verfügung gestellt werden.*

ITSEC 3.27 *Die Analyse der möglichen Auswirkungen jeder bekannten Schwachstelle muss aufzeigen, dass die betreffende Schwachstelle in der beabsichtigten Einsatzumgebung des EVG nicht ausgenutzt werden kann, weil entweder*

- *die Schwachstelle angemessen durch andere, nicht beeinträchtigte Sicherheitsmechanismen geschützt ist oder*
- *gezeigt werden kann, dass die Schwachstelle in Bezug zu den Sicherheitsvorgaben ohne Bedeutung ist, in der Praxis nicht existieren wird oder dass ihr angemessen durch dokumentierte technische, personelle, organisatorische oder materielle Sicherheitsmaßnahmen außerhalb des EVG entgegengewirkt werden kann. Diese externen Sicherheitsmaßnahmen müssen in der entsprechenden Dokumentation beschrieben (oder hinzugefügt worden) sein.*

Die Analyse muss unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.

ITSEC 3.28 *Es ist zu überprüfen, ob die Liste der bekannten Schwachstellen in der Konstruktion alle Forderungen bezüglich Inhalt, Form und Nachweis, so wie oben beschrieben, erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Es ist eine eigene Schwachstellenanalyse unter Berücksichtigung der aufgelisteten und der während der Evaluation gefundenen Schwachstellen durchzuführen. Es ist zu überprüfen, ob alle Kombinationen von bekannten Schwachstellen untersucht wurden. Es ist zu überprüfen, ob die Analysen der möglichen Auswirkungen der Schwachstellen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Es ist zu überprüfen, ob alle Annahmen und Anforderungen bezüglich externer Sicherheitsmaßnahmen ausreichend dokumentiert wurden. Es sind Penetrationstests durchzuführen, um zu bestätigen oder zu widerlegen, ob die bekannten Schwachstellen in der Praxis wirklich ausgenutzt werden können.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die Liste der bekannten Schwachstellen in der Konstruktion alle Forderungen bezüglich Inhalt,

Form und Nachweise (ITSEC 3.26, 3.27), so wie oben beschrieben, erfüllt. Sie hat überprüft und festgestellt, dass die Analyse alle relevanten Informationen verwendet hat.

Es wurden 3 Konstruktionsschwachstellen vom Hersteller angegeben, denen durch technische, personelle und organisatorischen Maßnahmen entgegen gewirkt wird. Die Prüfstelle hat eine eigene Schwachstellenanalyse durchgeführt und keine weitere Schwachstelle in der Konstruktion gefunden. Die Prüfstelle hat alle Kombinationen der bekannten Schwachstellen untersucht. Die Prüfstelle hat überprüft und festgestellt, dass die Analysen der möglichen Auswirkungen der Schwachstellen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Sie hat überprüft und festgestellt, dass alle Annahmen und Anforderungen bezüglich externer Sicherheitsmaßnahmen ausreichend dokumentiert sind. Penetrationstests mussten von der Prüfstelle nicht durchgeführt werden, da die Gegenmaßnahmen zu den bekannten Schwachstellen in der Verantwortung der Benutzer und Administratoren des EVG liegen.

3.2 Wirksamkeit – Betrieb

3.2.1 Aspekt 1: Benutzerfreundlichkeit

ITSEC 3.31 *Die Analyse der Benutzerfreundlichkeit muss mögliche Betriebsarten des EVG beschreiben, einschließlich des Betriebes nach Bedien- oder Betriebsfehlern, und ihre Konsequenzen und Folgerungen für die Aufrechterhaltung eines sicheren Betriebes.*

ITSEC 3.32 *Die Analyse der Benutzerfreundlichkeit muss aufzeigen, dass jeder menschliche oder andere Fehler, der sicherheitsspezifischen Funktionen oder Mechanismen ausschaltet oder unbrauchbar macht, leicht festzustellen ist. Sie muss zeigen, dass es erkennbar ist, wenn ein EVG in einer Weise konfiguriert oder benutzt werden kann, die unsicher ist (d. h. die sicherheitsspezifischen Funktionen und Mechanismen des EVG erfüllen die Sicherheitsvorgaben nicht), obwohl ein Endnutzer oder Administrator vernünftigerweise von einem sicheren Zustand ausgehen kann. Die Analyse muss unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

ITSEC 3.33 *Es ist zu überprüfen, ob die vorgelegte Analyse der Benutzerfreundlichkeit alle Anforderungen hinsichtlich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Die Analyse ist nach undokumentierten oder unvernünftigen Annahmen über die vorgesehene Betriebsumgebung zu überprüfen. Es ist zu überprüfen, ob alle Annahmen und Forderungen zu externen Sicherheitsmaßnahmen (wie z. B. externe prozedurale, materielle und personelle Kontrollmaßnahmen) ordnungsgemäß dokumentiert wurden. Jede Konfigurations- und Installationsprozedur ist nachzuvollziehen, um zu überprüfen, ob der EVG sicher konfiguriert und benutzt werden kann. Dabei ist lediglich die Dokumentation für den Nutzer und für den Administrator als Grundlage zu benutzen. Wo erforderlich, sind zusätzliche Tests durchzuführen, um die Analyse der Benutzerfreundlichkeit zu bestätigen oder zu widerlegen.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die vorgelegte Analyse der Benutzerfreundlichkeit alle Anforderungen hinsichtlich Inhalt, Form und Nachweisen (ITSEC 3.31, 3.32) erfüllt sowie die Analyse alle relevanten Informationen verwendet hat. Sie hat ferner überprüft und festgestellt, dass die Analyse keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Betriebsumgebung enthält. Die Prüfstelle hat überprüft und festgestellt, dass alle Annahmen und Forderungen zu externen Sicherheitsmaßnahmen in der Betriebsdokumentation niedergelegt wurden. Der EVG liegt in einer festen Konfiguration vor. Die Installationsprozedur ist von der Prüfstelle nachvollzogen worden und es wurde festgestellt, dass der EVG sicher installiert und betrieben werden kann, wenn lediglich die Betriebsdokumentation als Grundlage benutzt wird. Tests der Prüfstelle bestätigen die Analyse der Benutzerfreundlichkeit.

3.2.2 Aspekt 2: Bewertung der operationellen Schwachstellen

ITSEC 3.35 *Die Liste der Schwachstellen, die durch den Auftraggeber vorgelegt werden muss, muss alle ihm bekannten operationellen Schwachstellen des EVG aufführen. Sie muss jede Schwachstelle ansprechen, eine Analyse ihrer möglichen Auswirkungen beinhalten und die Maßnahmen aufzeigen, die zur Abhilfe vorgeschlagen oder zur Verfügung gestellt werden.*

ITSEC 3.36 *Die Analyse der möglichen Auswirkungen jeder bekannten Schwachstelle muss aufzeigen, dass die betreffende Schwachstelle in der beabsichtigten Einsatzumgebung des EVG nicht ausgenutzt werden kann, weil entweder*

- *die Schwachstelle angemessen durch andere, nicht beeinträchtigte externe Sicherheitsmaßnahmen geschützt ist oder*
- *gezeigt werden kann, dass die Schwachstelle bezüglich der Sicherheitsvorgaben ohne Bedeutung ist oder in der Praxis nicht ausgenützt werden kann.*

Die Analyse muss unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Alle geforderten externen Sicherheitsmaßnahmen müssen in der entsprechenden Dokumentation beschrieben (oder hinzugefügt worden) sein.

ITSEC 3.37 *Es ist zu überprüfen, ob die Liste der bekannten operationellen Schwachstellen alle Anforderungen bezüglich Inhalt, Form und Nachweis, so wie oben beschrieben, erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Es ist eine eigene Schwachstellenanalyse unter Berücksichtigung der aufgelisteten und der während der Evaluation gefundenen Schwachstellen durchzuführen. Es ist zu überprüfen, ob alle Kombinationen von bekannten Schwachstellen untersucht wurden. Es ist zu überprüfen, ob die Analysen der möglichen Auswirkungen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Es ist zu überprüfen, ob alle Annahmen und Forderungen zu externen Sicherheitsmaßnahmen ausreichend dokumentiert wurden. Es sind Penetrationstests durchzuführen, um zu bestätigen oder zu widerlegen, ob die bekannten Schwachstellen in der Praxis wirklich ausgenutzt werden können.*

Feststellung der Zertifizierungsstelle: Der Hersteller gibt eine operationelle Schwachstelle an. Die Prüfstelle hat überprüft und festgestellt, dass die vorgelegte Liste der bekannten operationellen Schwachstellen alle Anforderungen hinsichtlich Inhalt, Form und Nachweisen (ITSEC 3.31, 3.32) erfüllt sowie die Analyse alle relevanten Informationen verwendet hat. Die Prüfstelle hat eine eigene Schwachstellenanalyse durchgeführt und keine weitere operationelle Schwachstelle gefunden. Die Prüfstelle hat überprüft und festgestellt, dass die Analysen der möglichen Auswirkung der Schwachstellen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Sie hat überprüft und festgestellt, dass Annahmen und Anforderungen bezüglich externer Sicherheitsmaßnahmen in der Betriebsdokumentation ausreichend dokumentiert werden. Penetrationstests mussten von der Prüfstelle nicht durchgeführt werden, da die Gegenmaßnahmen zu den bekannten Schwachstellen in der Verantwortung der Benutzer und Administratoren des EVG liegen.

3.3 Korrektheit – Konstruktion – Entwicklungsprozess

3.3.1 Phase 1: Anforderungen (Sicherheitsvorgaben)

ITSEC E2.2 *Die Sicherheitsvorgaben müssen die sicherheitsspezifischen Funktionen darlegen, die vom EVG zur Verfügung gestellt werden. Im Falle eines Systems müssen die Sicherheitsvorgaben zusätzlich eine System-Sicherheitspolitik (SSP) enthalten, die die Sicherheitsziele und Bedrohungen des Systems identifiziert. Für ein Produkt müssen die Sicherheitsvorgaben zusätzliche Aussagen enthalten, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung und die für diese Einsatzumgebung angenommenen Bedrohungen identifizieren. Die in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen müssen in informeller Notation (siehe ITSEC Kapitel 2) spezifiziert werden.*

ITSEC E2.3 *Im Falle eines Systems müssen die Sicherheitsvorgaben darlegen, auf welche Weise die vorgeschlagene Funktionalität die Sicherheitsziele erfüllt und wie sie den definierten Bedrohungen angemessen entgegenwirkt. Im Fall eines Produktes müssen die Sicherheitsvorgaben darlegen, warum die Funktionalität für diese Art des Einsatzes zweckmäßig ist und wie sie den angenommenen Bedrohungen entgegenwirkt.*

ITSEC E2.4 *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob es Inkonsistenzen innerhalb der Sicherheitsvorgaben gibt.*

Feststellung der Zertifizierungsstelle: In den Sicherheitsvorgaben wird der EVG als Produkt im Sinne von ITSEC definiert. Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.2, E2.3) für ein Produkt erfüllen. Sie hat überprüft und festgestellt, dass es keine Inkonsistenzen innerhalb der Sicherheitsvorgaben[9] gibt.

[9] Für eine Zusammenfassung der Sicherheitsvorgaben siehe Kapitel 2.

3.3.2 Phase 2: Architekturentwurf

ITSEC E2.5 *Diese Beschreibung muss die grundsätzliche Struktur sowie alle externen Schnittstellen des EVG darlegen. Sie muss die Hard- und Firmware darlegen, die der EVG benötigt, und die Funktionalität der unterstützenden Schutzmechanismen angeben, die in dieser Hard- oder Firmware implementiert sind.* ***Sie muss die Aufteilung des EVG in sicherheitsspezifische und andere Komponenten darlegen.***

ITSEC E2.6 *Die Beschreibung der Architektur muss darlegen, wie die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung gestellt werden.* ***Sie muss darlegen, wie die Trennung in sicherheitsspezifische und andere Komponenten erreicht wird.***

ITSEC E2.7 *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.* ***Es ist zu überprüfen, ob die Trennung von sicherheitsspezifischen und anderen Komponenten wirksam ist.***

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.5, E2.6) erfüllen. Der EVG enthält keine anderen Komponenten im Sinne von ITSEC E2.7. Daher entfällt die Überprüfung der Wirksamkeit der Trennung von sicherheitsspezifischen und anderen Komponenten.

3.3.3 Phase 3: Feinentwurf

ITSEC E2.8 ***Der Feinentwurf muss die Realisierung aller sicherheitsspezifischen und sicherheitsrelevanten Funktionen darlegen. Er muss alle Sicherheitsmechanismen identifizieren. Er muss die sicherheitsspezifischen Funktionen auf Mechanismen und Komponenten abbilden. Alle Schnittstellen der sicherheitsspezifischen und der sicherheitsrelevanten Komponenten müssen mit ihrem Zweck und ihren Parametern dokumentiert werden. Spezifikationen/Definitionen für die Mechanismen müssen zur Verfügung gestellt werden. Diese Spezifikationen müssen für die Analyse der Beziehungen zwischen den verwendeten Mechanismen geeignet sein. Für Komponenten, die weder sicherheitsspezifisch noch sicherheitsrelevant sind, müssen keine Spezifikationen zur Verfügung gestellt werden. Wo mehr als eine Spezifikationsebene vorliegt, muss eine klare und hierarchische Beziehung zwischen den Ebenen bestehen.***

ITSEC E2.9 ***Der Feinentwurf muss darlegen, auf welche Weise die Sicherheitsmechanismen die sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben spezifiziert sind, realisieren. Er muss darlegen, warum Komponenten, für die keine Entwurfsunterlagen zur Verfügung gestellt werden, weder sicherheitsspezifisch noch sicherheitsrelevant sein können.***

ITSEC E2.10 ***Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.***

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.8, E2.9) erfüllen.

3.3.4 Phase 4: Implementierung

ITSEC E2.11 ***Die Testdokumentation muss Testpläne, Testziele, Testverfahren und Testergebnisse enthalten. Die Bibliothek von Testprogrammen muss Testprogramme und -werkzeuge enthalten, mit denen alle Tests, die in der Testdokumentation beschrieben sind, wiederholt werden können.***

ITSEC E2.12 ***Die Testdokumentation muss die Übereinstimmung zwischen den Tests und den in den Sicherheitsvorgaben definierten sicherheitsspezifischen Funktionen darlegen.***

ITSEC E2.13 ***Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die Bibliothek der Testprogramme ist für eine stichprobenweise Überprüfung der Testergebnisse heranzuziehen. Es ist zu überprüfen, ob die Tests alle sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben angegeben sind, umfassen. Zusätzlich sind Tests zur Fehlersuche durchzuführen.***

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.11, E2.12) erfüllen. Die Bibliothek der Testprogramme ist für eine stichprobenweise Überprüfung herangezogen wurden. Die Prüfstelle hat überprüft und festgestellt, dass die Tests alle sicherheitsspezifischen und sicherheitsrelevanten Funktionen umfassen. Zusätzlich sind Tests zur Fehlersuche durchgeführt worden. Dabei wurden keine Fehler gefunden.

3.4 Korrektheit – Konstruktion – Entwicklungsumgebung

3.4.1 Aspekt1: Konfigurationskontrolle

ITSEC E2.15 ***Der Entwicklungsvorgang muss durch ein Konfigurationskontrollsystem unterstützt werden. Die vorgelegte Konfigurationsliste muss alle Basiskomponenten auflisten, aus denen der EVG besteht. Der EVG, seine Basiskomponenten und alle zur Verfügung gestellten Dokumente, einschließlich der Handbücher, müssen eine eindeutige Identifikation besitzen. Die Verwendung dieser Identifikation bei Verweisen wird zwingend vorgeschrieben. Das Konfigurationskontrollsystem muss sicherstellen, dass der in Evaluation befindliche EVG mit der zur Verfügung gestellten Dokumentation übereinstimmt und dass nur autorisierte Änderungen möglich sind.***

ITSEC E2.16 ***Die Informationen über das Konfigurationskontrollsystem müssen darlegen, wie es in der Praxis benutzt wird und wie es im Entwicklungsprozess zusammen mit den Qualitätsmanagementverfahren des Herstellers angewendet wird.***

ITSEC E2.17 ***Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden.*** *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die dokumentierten Verfahren angewendet werden und dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise erfüllen (ITSEC E2.15, E2.16).

3.4.2 Aspekt2: Programmiersprachen und Compiler

ITSEC E2.18 Keine Anforderungen.

ITSEC E2.19 Keine Anforderungen.

ITSEC E2.20 Keine Aufgaben.

Feststellung der Zertifizierungsstelle: Entfällt bei ITSEC E2.

3.4.3 Aspekt3: Sicherheit beim Entwickler

ITSEC E2.21 ***Das Dokument über die Sicherheit der Entwicklungsumgebung muss die geplanten Schutzmaßnahmen bzgl. der Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumente darlegen. Materielle, organisatorische, personelle und andere Sicherheitsmaßnahmen, die durch den Entwickler eingesetzt werden, müssen dargelegt werden.***

ITSEC E2.22 ***Die Information über die Sicherheit der Entwicklungsumgebung muss darlegen, wie die Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumentation gewährleistet werden.***

ITSEC E2.23 ***Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist nach Fehlern in den Verfahren zu suchen.***

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die dokumentierten Verfahren angewendet werden. Die Prüfstelle hat überprüft, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.21, E2.22) erfüllen. Sie hat nach Fehlern in den dokumentierten Verfahren gesucht und festgestellt, dass diese fehlerfrei sind.

3.5 Korrektheit – Betrieb – Betriebsdokumentation

3.5.1 Aspekt1: Benutzerdokumentation

ITSEC E2.25 Die Benutzerdokumentation muss die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind, darlegen. Daneben muss sie auch Richtlinien für ihre sichere Anwendung enthalten. Die Benutzerdokumentation, zu welcher beispielsweise Referenz-Manuale, Benutzeranleitungen etc. gehören, muss strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

ITSEC E2.26 Die Benutzerdokumentation muss darlegen, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt.

ITSEC E2.27 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Feststellung der Zertifizierungsstelle: Vom Hersteller wurde folgende Dokumentation zur Verfügung gestellt:

- Benutzerdokumentation für die signaturgesetzkonforme DATEV Anwenderkomponente GERVA der Version 1.31, Version 3.3, 18.12.2003.

Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.25, E2.26) erfüllen.

3.5.2 Aspekt2: Systemverwalterdokumentation

ITSEC E2.28 *Die Systemverwalter-Dokumentation muss die sicherheitsspezifischen Funktionen darlegen, die für den Systemverwalter von Bedeutung sind. Sie muss zwei Funktionsarten unterscheiden: solche, mit denen der Systemverwalter die Sicherheitsparameter kontrollieren kann, und solche, mit denen er lediglich Informationen abfragen kann. Wenn ein Systemverwalter notwendig ist, muss sie alle Sicherheitsparameter darlegen, die er kontrollieren kann. Sie muss jeden Typ eines sicherheitsrelevanten Ereignisses darlegen, der für die Systemverwaltungsfunktionen von Bedeutung ist. Sie muss Details zu den Verfahren, die für die Sicherheitsadministration relevant sind, in einer Form darlegen, die für die Handhabung ausreichend ist. Sie muss Richtlinien zu der konsistenten und wirksamen Nutzung der Sicherheitseigenschaften des EVG enthalten und darlegen, wie solche Eigenschaften zusammenwirken. Sie muss die Anweisungen darlegen, wie das System/Produkt installiert wird und wie es, wenn erforderlich, konfiguriert wird. Die Systemverwalter-Dokumentation, z. B. Referenz-Manuale, Systemverwalter-Anleitungen etc., muss strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.*

ITSEC E2.29 *Die Systemverwalter-Dokumentation muss darlegen, wie der EVG sicher verwaltet wird.*

ITSEC E2.30 *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.*

Feststellung der Zertifizierungsstelle: Vom Hersteller wurde folgende Dokumentation zur Verfügung gestellt:

- Systemverwalterdokumentation für die signaturgesetzkonforme DATEV Anwenderkomponente GERVA der Version 1.31, Version 1.3, 12.12.2003.

Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.28, E2.29, E2.30) erfüllen.

3.6 Korrektheit – Betrieb – Betriebsumgebung

3.6.1 Aspekt1: Auslieferung und Konfiguration

ITSEC E2.32 *Wenn unterschiedliche Konfigurationen möglich sind, muss die Auswirkung der einzelnen Konfigurationen auf die Sicherheit dargelegt werden. Die Verfahren der Auslieferung und Systemgenerierung sind darzulegen.* ***Ein von der nationalen Zertifizierungsbehörde für diese Stufe zugelassenes Verfahren muss angewendet***

werden, welches die Authentizität des ausgelieferten EVG garantiert. Bei der Generierung des EVG müssen alle Generierungsoptionen und/oder Änderungen so protokolliert werden, dass es später möglich ist, exakt zu rekonstruieren wie und wann der EVG generiert wurde.

ITSEC E2.33 *Die vorgelegten Informationen müssen darlegen, wie die genannten Verfahren die Sicherheit aufrechterhalten.*

ITSEC E2.34 *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.* ***Die korrekte Anwendung der Auslieferungsverfahren ist zu überprüfen. Es ist nach Fehlern in den Verfahren zur Systemgenerierung zu suchen.***

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.33, E2.32) erfüllen. Die korrekte Anwendung des Auslieferungsverfahren ist überprüft worden. Die Auslieferung der Software erfolgt auf einer CD-ROM per Post. Dies entspricht einem in der vom BSI herausgegebenen AIS 10 angegebenen Verfahren, das für die Evaluationsstufe E2 zugelassen ist. Die Prüfstelle hat nach Fehlern in den Verfahren zur Systemgenerierung gesucht und dabei keine Fehler festgestellt.

3.6.2 Aspekt2: Anlauf und Betrieb

ITSEC E2.35 *Die Prozeduren für einen sicheren Anlauf und Betrieb müssen dargelegt werden.* ***Wenn irgendwelche sicherheitsspezifischen Funktionen während des Anlaufs, des normalen Betriebes oder der Wartung ausgeschaltet oder modifiziert werden können, so muss dies dargelegt werden. Wenn der EVG sicherheitsspezifische Hardware-Komponenten enthält, dann müssen hierfür Diagnoseeinrichtungen vorhanden sein, die durch den Systemverwalter, den Benutzer oder selbsttätig in der Einsatzumgebung aktiviert werden können.***

ITSEC E2.36 *Die vorgelegten Informationen müssen darlegen, wie die Prozeduren die Sicherheit aufrechterhalten.* ***Der Antragsteller muss Beispiele von Ergebnissen aller Diagnoseprozeduren der in Hardware implementierten sicherheitsspezifischen Komponenten zur Verfügung stellen. Der Antragsteller muss Beispiele aller Protokollaufzeichnungen vorlegen, die während des Anlaufs und des Betriebes erstellt werden.***

ITSEC E2.37 *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.* ***Die beispielhaften Nachweise für den Anlauf und den Betrieb sind zu überprüfen. Es ist nach Fehlern in den Prozeduren zu suchen.***

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.35, E2.36) erfüllen. Die Überprüfung der beispielhaften Nachweise für den Anlauf und Betrieb entfällt, da der EVG keine sicherheitsspezifische Hardware-komponenten enthält und keine Protokollierung durchführt. Die Prüfstelle hat nach Fehlern in den Prozeduren gesucht und dabei keine Fehler festgestellt.

4 Auszug aus ITSEC und ITSEM

4.1 Vertrauenswürdigkeit - Wirksamkeit

ITSEC 3.2:

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.

4.2 Vertrauenswürdigkeit – Korrektheit

ITSEC 4.2-4.10:

Sieben Evaluationsstufen werden bezüglich des Vertrauens in die Korrektheit eines EVG definiert. E0 bezeichnet die niedrigste, E6 die höchste dieser Stufen. Die sieben Evaluationsstufen können wie folgt *charakterisiert* werden:

Stufe E0

Diese Stufe repräsentiert unzureichende Vertrauenswürdigkeit.

Stufe 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.

Stufe 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.

Stufe 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.

Stufe 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.

Stufe E5

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

Stufe 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.

4.3 Klassifizierung von Sicherheitsmechanismen

ITSEM 6.C.4-6.C.7

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. Ein Beispiel für einen Mechanismus vom Typ A ist ein Authentisierungsprogramm, bei dem ein Passwort verwendet wird; wenn das Passwort erraten werden kann, indem nacheinander alle möglichen Passwörter ausprobiert werden, handelt es sich um einen Authentisierungsmechanismus vom Typ A. Mechanismen vom Typ A bedienen sich häufig eines "Geheimnisses" wie etwa eines Passworts oder eines kryptographischen Schlüssels.

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

Bei der Bewertung der Stärke eines Mechanismus soll der Kontext, in dem der Mechanismus eingesetzt wird, mit berücksichtigt werden. Siehe den Unterabschnitt *Beispiele* weiter unten.

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. Ein mögliches Beispiel für einen Mechanismus vom Typ B wäre die Zugangskontrolle auf der Basis von Zugangskontrolllisten: Bei perfekter Konzipierung und Implementierung kann dieser Mechanismus vom Typ B nicht durch einen direkten Angriff überwunden werden. Mechanismen vom Typ B können jedoch durch indirekte Angriffe überwunden werden, mit denen sich andere Wirksamkeitsanalysen befassen.

4.4 Mindeststärke der Sicherheitsmechanismen

ITSEC 3.5-3.8

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.

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.

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.

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.

5 Literaturreferenzen

[1] ITSEC: *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik,* Version 1.2 (1991)

[2] ITSEM: *Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik,* Version 1.0 (1993)

[3] Laut Abbildung 4 der ITSEC-Kriterien sind für die Stufe E2 mindestens folgende Informationen bzw. Unterlagen für die Durchführung der Schwachstellenanalyse zu verwenden:

a) die Sicherheitsvorgaben,
b) eine informelle Beschreibung der Funktionen,
c) eine informelle Beschreibung des Architektur-Entwurfs und
d) die vollständige Betriebsdokumentation.

6 Abkürzungen

AIS	Anwendungshinweise und Interpretationen zum Schema
BSI	Bundesamt für Sicherheit in der Informationstechnik
EVG	Evaluationsgegenstand
SigG	Signaturgesetz
SigV	Signaturverordnung