Zertifizierungsbericht

Zertifizierungs-Vorgang:	**TUVIT-DSZ-ITSEC-9153**
Produkt / System:	Zeitsigniersystem TSS 400 Version 3.02
Hersteller:	timeproof TIME SIGNATURE SYSTEMS GmbH Harburger Schloßstraße 6-12 21079 Hamburg
Auftraggeber:	s. o.
Prüfstelle:	TÜViT, Prüfstelle für IT-Sicherheit
Evaluierungsbericht:	Version 1.0 vom 02.09.2003 Dokument-Nummer: 20598115_TÜV_009.01 Verfasser: Volker Nies
Formaler Ablauf:	vollständig / ordnungsgemäß durchgeführt
Ergebnis:	E2 / hoch
Evaluierungsauflagen:	eine (siehe Abschnitt 1.5.1)
Prüfbegleiter:	Dr. Christoph Sutter
Zertifizierungsauflagen:	eine (siehe Abschnitt 1.6.1)

Essen, den 16.04.2004

Dr. Ernst-Hermann Gruschwitz Dr. Christoph Sutter

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.

Die Zertifizierung des Zeitsigniersystems *TSS 400, Version 3.02* ist eine **Re-Zertifizierung** auf der Basis der Zertifizierung TUVIT-DSZ-ITSEC-9152-2003 der Vorgängerversion 3.01, die sich von dieser durch der folgenden beiden Anpassungen der Protokollserver-Software bezüglich Zeitstempelresponses gemäß RFC3161 unterscheidet:

1. Die SignedData-Versionsnummer wurde von 2 auf 3 geändert,
2. Im tsa-Feld wird anstelle des Zertifikats-Issuers der SubjectName eingetragen.

Eine Re-Evaluierung war nicht notwendig, da es sich bei den oben genannten Anpassungen um isolierte sicherheitsrelevante Änderungen auf der Implementierungsebene handelt, die auf der Feinentwurfsebene nicht sichtbar sind. Gemäß ITSEM 6.D.20 ergibt sich die Auswirkungsart m3 und damit die Auswirkungsart I2: „Zertifizierungsstelle informieren und Testdokumentation zur Verfügung stellen“. Dazu wurden vom Hersteller alle Tests mit dem Protokollserver erfolgreich wiederholt und die zugehörige Testdokumentation der Zertifizierungsstelle zur Verfügung gestellt.

Zusätzlich sind in der Bedienungsanleitung sowie im Sicherheitshandbuch Änderungen vom Typ „d“ bezüglich der EVG-Versionsnummer und des Zeitstempelaufrufs[2] erfolgt, die keine Auswirkungen auf die Kriterien für „Korrektheit – Betrieb, Benutzerfreundlichkeit und operationelle Schwachstellen“ haben. Daher sind gemäß ITSEM 6.D.34 keine weiteren Maßnahmen erforderlich.

1.1 Evaluationsgegenstand (EVG) und Prüfkriterien

Die Re-Zertifizierung hat das Zeitsigniersystem TSS 400, Version 3.02 der Firma timeproof TIME SIGNATURE SYSTEMS GmbH, Harburger Schloßstraße 6-12, 21079 Hamburg als Gegenstand und bescheinigt, dass dieses auf Grundlage der *“Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik Version 1.2 (1991)“*[3] und des „*Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik Version 1.0 (1993)“*[4], gegen die produktspezifischen Sicherheitsvorgaben von der Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH[5] im Rahmen des letzten Re-

[1] Im folgenden kurz BSI genannt

[2] Siehe auch Abschnitt 2.1.1 unter vom EVG unterstützte Abrufmechanismen und Zeitstempelformate.

[3] Im folgenden kurz ITSEC genannt

[4] Im folgenden kurz ITSEM genannt

[5] Im folgenden kurz TÜViT genannt

Zertifizierungsverfahrens TUVIT-DSZ-ITSEC-9152-2003 evaluiert wurde. Die Ergebnisse dieses Re-Zertifizierungsverfahrens sind weiterhin gültig.

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

1.2 Durchführung der Evaluierung und Evaluierungsendbericht

Die oben genannten Änderungen sind der Zertifizierungsstelle in einer Auswirkungsanalyse angezeigt worden. Eine Überprüfung der Analyse sowie der zur Verfügung gestellten Dokumente und Nachweise hat ergeben, dass für diese Re-Zertifizierung keine Re-Evaluierung notwendig ist. Die Ergebnisse der Erst-Evaluierung sind weiterhin gültig.

Die letzte Re-Evaluierung zum Verfahren TUVIT-DSZ-ITSEC-9152-2003 wurde in der Zeit vom 05.08.2003 bis zum 02.09.2003 von Herrn Volker Nies und Herrn Hans-Werner Bliißenbach durchgeführt. Die Leitung der Evaluierung wurde von Herrn Hans-Werner Bliißenbach wahrgenommen und der Evaluierungsendbericht Version 1.0 vom 02.09.2003 (Nummer: 20598115_TÜV_009.01) wurde von Herrn Volker Nies erstellt.

1.3 Prüfergebnis der Evaluierung

Die letzte Re-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[6] um ein Produkt, welches folgende Sicherheitsfunktionalität aufweist:

- Identifikation und Authentisierung
- Zugriffskontrolle
- Beweissicherung
- Manipulationsfreie Uhr
- Zeitstempelkontrolle

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

1.4 Erweiterung der Ergebnisse auf andere Konfigurationen

Der EVG ist durch Name und Versionsnummer (Version 3.02) 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.

[6] Im folgenden kurz EVG genannt

1.5 Auflagen, Hinweise und Empfehlungen aus der Evaluation

1.5.1 Auflagen für den Hersteller:

Der Evaluierungsendbericht enthält die folgende Auflage an den Hersteller:

1. Der Hersteller muss dafür Sorge tragen, dass auch in Zukunft alle Testwerkzeuge zur Verfügung stehen, um ggf. die Tests unter gleichen Bedingungen nachvollziehen zu können.

1.5.2 Hinweise für den Hersteller

Der Evaluierungsendbericht enthält keine Hinweise aber die folgende Empfehlung für den Hersteller:

- Innerhalb des Statusbildschirms (1. Zeile) erfolgt die für den Benutzer möglicherweise missverständliche Anzeige der Form:

  DCF 08:51:17 07.03.2003,

  in der die Anzeige DCF nur kenntlich macht, dass die Trust Box versucht das DCF77-Signal zu verarbeiten, während die Anzeige von Uhrzeit/Datum stets die Zeit der internen Uhr visualisiert. Im Falle einer zukünftigen Re-Evaluierung des EVG sollte diese Anzeige derart angepasst werden, dass für den Benutzer stets erkennbar ist, ob die Zeit der internen Uhr oder die DCF77-Zeit angezeigt wird.

1.5.3 Hinweise und Empfehlungen für den Anwender

Der Evaluierungsendbericht enthält keine Hinweise und Empfehlungen für den Anwender.

1.6 Zertifizierungsauflagen und Hinweise

1.6.1 Zertifizierungsauflagen

Der Hersteller muss dafür Sorge tragen, dass auch in Zukunft alle Testwerkzeuge zur Verfügung stehen, um ggf. die Tests unter gleichen Bedingungen nachvollziehen zu können.

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 ist das Zeitsigniersystem TSS 400, Version 3.02, bestehend aus einer Trust Box:

- Steuerung: Hardware V2.0, Firmware V3.003
- Uhr: Hardware V2.1, Firmware V3.001
- Signaturcontroller: Hardware V2.0, Firmware V3.002

für die Zeitstempelgenerierung, einer Protokollsoftware:

- Protokollserver V3.02

für die Protokollierung der ausgestellten Zeitstempel und der Integritätssoftware:

- Integritätstester V1.51

zum Feststellen von eventuellen sicherheitstechnischen Veränderungen an der Protokollsoftware. Darüber hinaus wird mit dem EVG die Dokumentation:

- Bedienungsanleitung V1.36 und
- Sicherheitshandbuch V1.19

ausgeliefert.

Die Trust Box vereinigt das Interface zur Signaturerstellungseinheit (Signaturkarte) und eine sichere Uhr in einer Einheit und stellt damit sicher, dass nur die gesetzlich gültige Zeit zur Zeitsignatur verwendet wird. Der EVG erzeugt die Zeitsignatur mit Hilfe von sicheren Signaturerstellungseinheiten, die nicht Bestandteil des EVG sind.

Die Serversoftware dient der Zeitstempelprotokollierung und der Ansteuerung der Trust Box.

Vom EVG werden folgende Abrufmechanismen und Zeitstempelformate unterstützt:

- RFC 3161: Abruf direkt über TCP, sowie über HTTP

  Es werden Anfragen mit SHA1 und RIPEMD-160 Hashwerten unterstützt. Alle Zeitstempel werden, unabhängig vom Format des Hashwerts in der Anfrage, SHA1-RSA signiert.

- PKCS#7: Abruf direkt über TCP durch einen Request der Form:

```
TimeStampReqPKCS7 ::= CHOICE [3]  {
        SEQUENCE {
                version                 INTEGER { V1(0) }
                messageImprint          MessageImprint
        }
}
```

Das Feld „Version“ gibt die Version der Anfrage an, die stets gleich 1 ist. Der MessageImprint ist eine Folge aus dem ASN.1 Code des verwendeten Hashalgorithmus (z. B. OID 1.3.14.3.2.26 für SHA1) sowie dem zeitzustempelnden Hashwert.

Eine schematische Produktübersicht ist in Abbildung 1 gegeben:

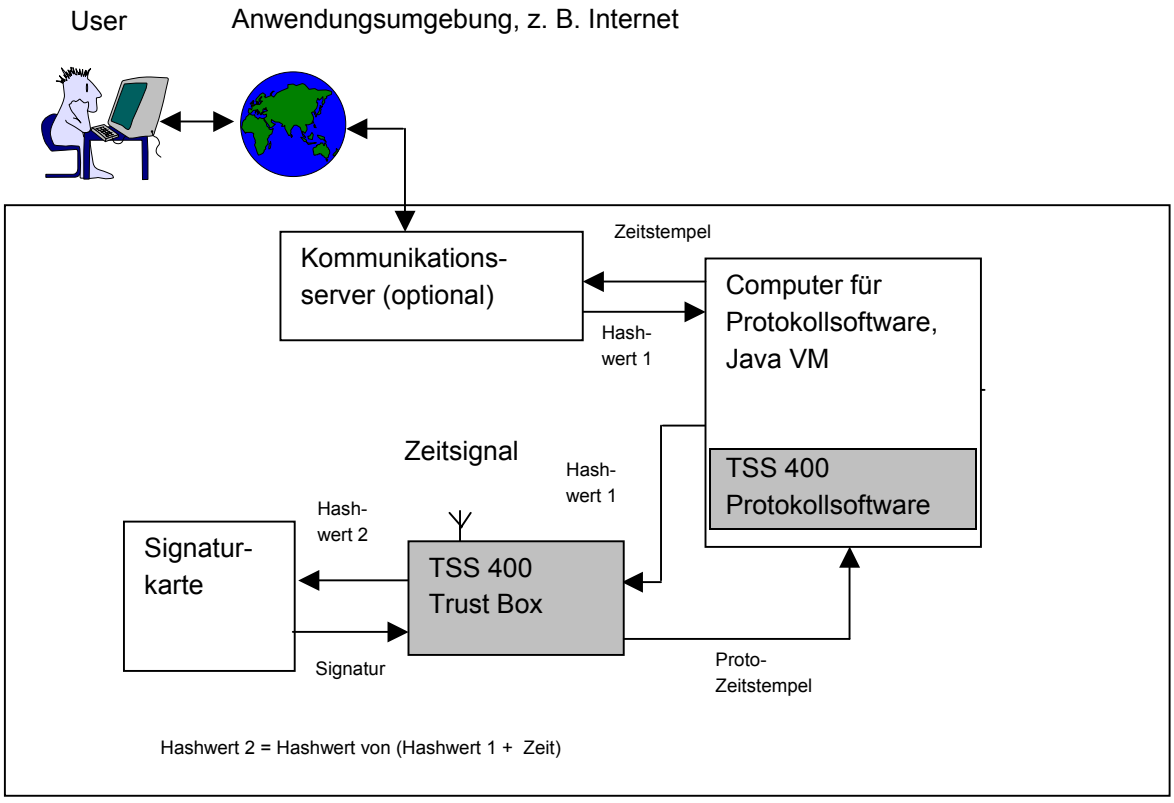

Abbildung 1: Schematische und vereinfachte Produktübersicht. Der EVG besteht aus der TSS 400 Trust Box und der TSS 400 Protokollsoftware (grau hinterlegt).

2.2 Art der Nutzung

Das Zeitsigniersystem TSS 400 muss in einer hinreichend sicheren Umgebung, wie sie zum Beispiel bei Zertifizierungsdiensteanbietern gemäß SigG vorzufinden ist, eingesetzt werden

und kann dort einen Zeitstempeldienst bereitstellen. Im Sinne der ITSEC ist das Zeitsigniersystem TSS 400 ein Produkt.

Der Hashwert[7] von digitalen Daten, die mit einem Zeitstempel versehen werden sollen, wird via Internet über den Kommunikationsserver (optional, nicht Bestandteil des EVG) an den Computer für die Protokollsoftware (nicht Bestandteil des EVG) weitergeleitet. Dieser Computer wird von der Protokollsoftware unter Nutzung einer Java-Virtuelle-Maschine (VM) und der Java-Communications-Erweiterung gesteuert. Von dort aus wird der Hashwert zur Trust Box übertragen.

Die Trust Box empfängt das Zeitsignal und erhält daraus die gesetzlich gültige Zeit. Über den erhaltenen Hashwert, den Zeitpunkt des Eintreffens des Hashwertes in der Trust Box und weitere, vom Signaturaustauschformat festgelegte Informationen, bildet die Trust Box einen weiteren Hashwert 2 und sendet diesen an eine Signaturerstellungseinheit (Signaturkarte), welche den Hashwert 2 verschlüsselt (Erzeugung einer Signatur). Die so erzeugte Zeitsignatur gelangt zur Trust Box.

Der Zeitstempel wird an den Computer für Protokollsoftware übertragen. Von dort erfolgt die Weiterleitung an die Protokollsoftware. Der Zeitstempel wird in einer Protokolldatei gespeichert und erst nach erfolgreicher Speicherung an den Kommunikationsserver weitergeleitet.

2.3 Angenommene Einsatzumgebung

2.3.1 Technische Einsatzumgebung

Für den Betrieb des EVG werden folgende Anforderungen an den bereitzustellenden Computer für die Protokollsoftware gestellt:

- mindestens 256 MB Hauptspeicher,
- zwei serielle Schnittstellen oder parallele Schnittstellen,
- mindestens 20 GByte freier Festplattenspeicher,
- CD-ROM-Laufwerk,
- Prozessor mit einer Rechenleistung vergleichbar einer Sun UltraSPARC II mit 400 MHz bzw. Pentium III 500 MHz und
- Betriebssystem Solaris 5.8, 5.9 (SPARC), SuSE Linux 8 oder Windows XP.

Auf dem Computer muss eine Java Virtuelle Maschine Version 1.4.1 installiert sein sowie zusätzlich die Java-Communications-Erweiterung Version 2.0.

Die o. g. Betriebssysteme sind in der Lage, den logischen Zugriff auf den Rechner auf autorisierte Personen zu beschränken. Zu schützen sind alle Dateien, die zur Ausführung

[7] Genaugenommen der MessageImprint bestehend aus Hashwert und Code (OID) des Hashalgorithmus.

des Protokollservers und der zugrunde liegenden virtuellen Maschine benötigt werden. Dies sind alle Dateien in den Installationsverzeichnissen des Protokollservers und der virtuellen Maschine sowie deren Unterverzeichnissen.

Der Protokollserver muss in einem geschützten Netzwerk betrieben werden, d. h. nur der Service-Port auf der entsprechenden IP-Adresse darf von einem allgemein zugänglichen Netzwerk ausschließlich über eine Firewall oder einen proxy-Server erreichbar sein.

Für den Betrieb bei einem Zertifizierungsdiensteanbieter gemäß SigG ist eine gemäß SigG bestätigte sichere Signaturerstellungseinheit (Signaturkarte) erforderlich.

Eingesetzt werden können die folgenden Karten:

- G+D STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 (unlimited signature generation configuration),
- Telesec PKS-Card 2.0 (Betriebssystem TCOS 2.0 Rel.2),
- Telesec PKS-Card 3.0 (Betriebssystem TCOS 2.0 Rel. 3) und Varianten E4KeyCard bzw. E4NetKeyCard sowie
- Signtrust SEA-Card 2.0 (Betriebssystem TCOS 2.0 Rel. 3).

Zum Betrieb weiterhin erforderlich sind ein Stromanschluss (230 V) mit unterbrechungsfreier Stromversorgung (USV) sowie:

für den direkten Zeitsignalempfang:

- Blitzschutz,
- eine Empfangsantenne für das externe Zeitsignal (DCF),

bzw. für den indirekten Zeitsignalempfang:

- Blitzschutz,
- aufbereitetes Zeitsignal, das den gesetzlichen Forderungen und Genauigkeitsanforderungen[8] genügt.

2.3.2 Administrative Einsatzumgebung

Für den EVG werden folgende Mindestanforderungen an die Betriebsumgebung vorausgesetzt:

Der EVG ist in einer Umgebung untergebracht, welche die Sicherheitsansprüche eines Trustcenters eines Zertifizierungsdiensteanbieters gemäß SigG erfüllt. Er befindet sich in einem Raum, der nur von autorisierten Personen betreten werden darf und kann.

[8] Zeitoffset des Systems: ≤ 10ms; Driftfehler bei Ausfall der externen Zeitsignale ≤ 20µs/Tag

Es werden folgende Rollen definiert:

1. Administrator (Admin)

   Der Administrator ist verantwortlich für die korrekte Inbetriebnahme des Systems durch Vergleich der empfangenen Zeit mit mindestens einer externen gesetzlich gültigen Zeitquelle. Der Administrator erkennt sicherheitstechnische Veränderungen

   - an der Trust Box mittels Sichtprüfung der Siegel und
   - an der Protokollsoftware durch Integritätscheck mit Hilfe der mitgelieferten Integritätssoftware.

   Der Administrator ist Geheimnisträger der Zugangs-Passwörter und PINs der sicheren Signaturerstellungseinheiten. Er verwaltet und verwahrt diese und sorgt dafür, dass sie keinem Dritten zugänglich gemacht werden. Er ist berechtigt, Zugangs-Passwörter zu ändern.

   Der Administrator ist verantwortlich für die Einhaltung der Fristen zur Wartung und Pflege des Systems, sowie für die Genehmigung von Reparaturaufträgen und autorisierten Reparaturen. Der Administrator überprüft Seriennummern sowie Versionsnummern (Hardware; Firmware). Er darf Schaltsekunden dem Zeitsigniersystem TSS 400 bekannt geben.

   Administratoren arbeiten im Vier-Augen-Prinzip (siehe auch Tabelle 1: Rechtematrix). Der Administrator gilt als vertrauenswürdige Person und legt im Rahmen seiner Vollmachten weitere Benutzer und Zugriffsrechte (Berechtigungskontrollverfahren) fest. Alle nachfolgenden Rollen können von ihm ausgefüllt sein.

2. Anwender (User)

   Der Anwender fordert lediglich eine Zeitsignatur an (z. B. über den Kommunikationsserver). Er hat keine weiteren Zugangs- oder Zugriffsrechte.

3. Auditor

   Die Funktion des Auditors kann entweder vom Administrator festgelegt sein oder von ihm selbst eingenommen werden. Der Auditor ist berechtigt den Boxstatus regelmäßig zu überprüfen.

   Der Auditor überprüft Seriennummern sowie Versionsnummern (Hardware; Firmware).

   Er soll sicherheitstechnische Veränderungen an der Trust Box erkennen und ggf. einem Administrator mitteilen.

4. Archivar

   Die Funktion des Archivars kann entweder vom Administrator festgelegt sein oder von ihm selbst eingenommen werden. Der Archivar ist berechtigt, die Archivierung und Zeitstempelung der Tagesprotokolldateien vorzunehmen. Er sorgt für die Sicherstellung der

nötigen Speicherkapazität. Er stellt die nötige Langzeitsicherung der Zeitstempel-protokolldateien sicher.

Für den Betrieb sind die vom Gesetzgeber festgelegten Aufbewahrungsfristen einzuhalten.

Rechte ↓ / Rolle →	Admin.	Auditor	Archivar	User
Signatur anfordern	X	X	X	X
Betreten des Aufstellortes	X	X[1)]	X[1)]	
Festlegung des Berechtigungskontrollverfahrens	X[3)]			
Funktionsüberwachung	X	X		
Kartenwechsel (Signaturkarten)	X[3)]			
Inbetriebnahme/Abschalten	X[3)]			
Gerätewechsel/Installation	X			
Logischer Zugang zum Computer für Protokollsoftware	X		X[1)]	
Bedienung Protokollsoftware	X			
zulässige Softwareupdates [2)]	X			
Ankündigung von Schaltsekunden	X[3)]			

1) nur mit Genehmigung eines Administrators
2) nur evaluierte und zertifizierte Software des Herstellers und für Einsatz bei einem Zertifizierungs-diensteanbieter darüber hinaus gemäß SigG/SigV bestätigte technische Komponente
3) Vier-Augen-Prinzip

Tabelle 1: Rechtematrix

Darüber hinaus müssen die folgenden Maßnahmen zum sicheren Betrieb des EVG berücksichtigt werden (für die Definition von O3-O7 siehe Abschnitt 2.4.2):

- Für die Zugriffskontrolle ist die Durchsetzung der Inhalte der obigen Tabelle durch externe Maßnahmen erforderlich.
- Der Zugriff auf O6 sowie Lesezugriffe auf O4 erfolgen über die Zugangskontrolle zum Raum (Umgebungsvoraussetzung).
- Unberechtigte Zugriffe auf O3, O5 und O7 werden durch das Betriebssystem des Protokollservers unterbunden.
- Die Initialisierungs-PINs der Signaturkarten sind nur den Administratoren bekannt und dürfen keinem Dritten bekannt gemacht werden.

- Zur Initialisierung müssen die Administratoren die anliegende Zeit freigeben (Vier-Augen-Prinzip). Sie müssen sich durch geeignete Maßnahmen versichern, dass die durch die Trust Box empfangene Zeit korrekt ist.
- Berechtigte Zeitsprünge (Schaltsekunden) müssen vor ihrem Auftreten von den Administratoren (Vier-Augen-Prinzip) bekannt gegeben werden.
- Es ist dafür zu sorgen, dass durch einen monatlichen Vergleich der Trust Box – Uhrzeit mit einer geeigneten Referenzzeit (z. B. telefonische Zeitansage), eine eventuelle Manipulation des Zeiteingangssignales erkannt wird.
- Die Administratoren müssen sich ausloggen, sobald sie den EVG verlassen.
- Die Integritätstestsoftware ist bei der Installation, bei Manipulationsverdacht sowie regelmäßig zum Erkennen von eventuellen sicherheitstechnischen Veränderungen zu verwenden.

2.4 Subjekte, Objekte und Zugriffsarten / Aktionen

2.4.1 Subjekte

Die folgenden Subjekte sind definiert:

S1: Administrator

- Zugriffsrechteverwaltung (Berechtigungskontrolle)
- Inbetriebnahme der Uhr
- Inbetriebnahme der Signaturkarten und Kartenwechsel
- Wechsel der Batterie
- Ankündigung von Schaltsekunden
- Überprüfung der Uhrzeit (monatlich)
- Ablesen der Seriennummern sowie der Versionsnummern (Hardware; Firmware)
- sowie die Rechte von S2, S3 und S4

S2: Auditor

- regelmäßige Überprüfung des Boxstatus (Empfehlung: täglich)
- regelmäßige Überprüfung der Integrität von Trust Box und Software (Empfehlung: täglich)
- Ablesen der Seriennummern sowie der Versionsnummern (Hardware; Firmware)

S3: Archivar

- Einsichtnahme in Zeitstempel-Protokolldateien
- Langzeitarchivierung und Zeitstempelung der Zeitstempel-Tagesprotokolldateien

- Sicherstellung der nötigen Plattenkapazität

S4: User

- Anforderung von Zeitstempeln
- Lesen und löschen angeforderter Zeitstempel

Der EVG sieht explizit die Subjekte S1 und S4 vor. S2 und S3 können von S1 festgelegt werden. Technisch und organisatorisch gesehen sind sie optional. Wenn sie aber von S1 definiert sind, dürfen ihre Berechtigungen nicht die vorgesehenen Berechtigungen überschreiten.

2.4.2 Objekte

Die folgenden schützenswerte Objekte sind definiert:

O1: Berechtigungsdaten für Administratoren

O2: PIN der Signaturkarten

O3: Eingangs-Hashwert

O4: Zeit und Status der internen Uhr

O5: Protokolldaten der Zeitstempel

O6: Boxlog (Log der kritischen Abweichungen des Boxstatus; in der Trust Box geführt)

O7: Zeitstempel

2.4.3 Zugriffsarten

Tabelle 2 gibt die erlaubten Zugriffsarten wieder.

Objekte ↓	Subjekte →	S1 Admin.	S2 Auditor	S3 Archivar	S4 User
O1: Berechtigungsdaten für Administratoren		A[1)], C, R*[1)], D[1)]			
O2: PINs der Signaturkarten		I[2) 1)]			
O3: Eingangs-Hashwert		I, R[4)]	I, R[4)]	I, R	I, R[4)]
O4: Zeit und Status der internen Uhr		R, C[2)]	R	R	
O5: Protokolldaten [3)]				R, D	
O6: Boxlog		R[1)]			
O7: Zeitstempel		R[4)], D[4)]	R[4)], D[4)]	R, D[4)]	R[4)], D[4)]

R: Lesen, C: Ändern, D: Löschen, A: Hinzufügen I: Eingeben

* außer Passwort

1) Vier - Augen – Prinzip (4AP). Mindestens 2 Administratoren sind erforderlich.

2) Nur zur Inbetriebnahme nach 4AP

3) Schutz der Protokolldaten wird vom zugrundeliegenden Betriebssystem vorgenommen.

4) selbst erzeugte

Tabelle 2: Zugriffsarten

2.5 Bedrohungen und Sicherheitsziele

2.5.1 Bedrohungen

Für den angenommenen Einsatz des Zeitsigniersystems TSS 400 werden die folgenden 3 Bedrohungen angenommen:

B1: Ausstellen von fehlerhaften Zeitstempeln durch Manipulation des Zeiteingangssignals.

B2: Ausstellen von Zeitstempeln mit der Trust Box, ohne Verwendung der Protokollsoftware.

B3: Setzen einer falschen Start-Zeit der internen Uhr durch unberechtigte Inbetriebnahme.

2.5.2 Sicherheitsziele und Sicherheitseigenschaften

Der EVG hat die folgenden 3 Sicherheitsziele:

SZ1: Es soll ein Zeitstempel generiert werden, der in Verbindung mit SZ2 und SZ3 beweist, dass der Trust Box zu einem bestimmten Zeitpunkt ein Hashwert vorgelegen hat.

SZ2: Die im Zeitstempel angegebene Zeit weicht zum Zeitpunkt der Stempelung von der UTC-Zeit maximal eine halbe Sekunde ab.

SZ3: Alle ausgegebenen Zeitstempel werden in einer Zeitstempel-Protokolldatei gespeichert.

2.6 Sicherheitsfunktionen

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

SF1: Identifikation und Authentisierung (Trust Box)

- Die Administratoren müssen sich mit ihrem Usernamen und ihrem geheimen Passwort (mindestens 6-stellig) gegenüber dem System identifizieren und authentisieren.
- Die Authentisierungsinformation ist vor unbefugtem Zugriff geschützt.
- Fehlerhafte Authentisierungsversuche werden begrenzt.
- Der EVG ermöglicht seinen Administratoren nur im Vier-Augen-Prinzip zu arbeiten.

SF2: Zugriffskontrolle (Trust Box)

- Zugriffe auf die Objekte O1, O2 und O6 sind nur durch zwei eingeloggte Administratoren möglich (Vier-Augen-Prinzip). O2 wird in der Trust Box nicht dauerhaft gespeichert.
- Änderungszugriffe auf O4 sind nur durch zwei eingeloggte Administratoren möglich.

SF3: Beweissicherung (Protokollsoftware, Trust Box)

- Zur Beweissicherung wird eine Protokolldatei der Zeitstempel angelegt.
- Kritische Abweichungen, z. B. längerer Zeitsignalausfall und Temperaturabweichungen, des Betriebszustandes der Trust Box werden aufgezeichnet.
- Es erfolgt keine Freigabe eines Zeitstempels ohne Protokollierung. Ist eine Speicherung nicht möglich, so wird ein Fehlercode an den User geschickt.

SF4: Manipulationsfreie Uhr (Trust Box)

- Die Trust Box empfängt das Zeit-Signal und erhält daraus die gesetzlich gültige Zeit.
- Eine interne Uhr wird mit dem empfangenen gesetzlich gültigen Zeitsignal durch einen Regelalgorithmus abgeglichen.
- Ein Überwachungs- und Regelalgorithmus sorgt dafür, dass ein externes Wegziehen der Zeit oder ein Zeitsprung erkannt wird. Wird eine Manipulation des externen Signals erkannt, wird der Status auf „Zeitmanipulation“ gesetzt und die Regelung außer Betrieb gesetzt. Die interne Uhr läuft mit der Quarzgenauigkeit weiter und liefert auch weiterhin für 7x24 Stunden unter Einhaltung der Genauigkeit die gesetzlich gültige Zeit.
- Kann die Genauigkeit, unter Berücksichtigung der Quarzgenauigkeit der internen Uhr, von 0,5s nicht mehr gewährleistet werden, so wird der Status auf „Zeit ungültig“ gesetzt. Der EVG stellt den Betrieb ein.

SF5: Zeitstempelkontrolle (Trust Box)

- Der Status der internen Uhr wird überprüft. Liefert die interne Uhr nicht die gesetzlich gültige Zeit (Status: „Zeit ungültig“), wird ein Fehlercode an den User geschickt.
- Eingangs-Hashwert und gesetzlich gültige Zeit und weitere, vom Signaturaustauschformat festgelegte Informationen, werden mit SHA-1 gehasht und einer Signaturkarte zum Signieren bereitgestellt.
- Die Signatur der Signaturkarte wird zusammen mit der verwendeten Zeit und weiteren, vom Signaturaustauschformat festgelegte Informationen, an den

Protokollserver übermittelt, damit dieser aus der Zeitinformation und der Signatur den Zeitstempel zusammenstellen kann.

2.7 Korrelation Sicherheitsfunktionen / Bedrohungen / Sicherheitsziele

Die folgende Tabelle zeigt welche Sicherheitsfunktionen den jeweiligen Bedrohungen entgegenwirkt:

	SF1	SF2	SF3	SF4	SF5
B1	X	X		X	X
B2		X	X		
B3	X	X			

Die Sicherheitsfunktionen sind für die vorgesehene Art der Nutzung des Zeitsigniersystems TSS 400 sowohl geeignet als auch zweckmäßig. Im einzelnen gilt dabei folgendes:

Gegen B1 wirken SF1 und SF2, da eine Inbetriebnahme mit erneuter Synchronisation der internen Uhr auf das Zeitsignal nur nach Einloggen durch Identifikation und Authentisierung zweier Administratoren möglich ist.

Gegen B1 wirkt SF4, da eine Manipulation des Zeiteingangssignals durch den Überwachungs- und Regelalgorithmus erkannt wird. Dieser sorgt dafür, dass ein externes Wegziehen der Zeit oder ein Zeitsprung erkannt und durch den Status „Zeitmanipulation“ markiert wird. Dafür wird eine interne Uhr mit einem gesetzlich gültigen Zeitsignal abgeglichen.

Gegen B1 wirkt SF5, da der Status der internen Uhr überprüft wird. Wenn SF4 den Fehlerstatus „Zeit ungültig“ gesetzt hat, findet keine Zeitstempelung statt. So ist sichergestellt, dass der im Zeitstempel angegebene Zeitpunkt die gesetzlich gültige Zeit ist.

Gegen B2 wirkt SF2, da die korrekte Einhaltung der Zugriffsrechte (siehe auch Abschnitt 2.4.3) unentbehrlich ist, um die Protokolldatei zu schützen. Auch wird nur so gewährleistet, dass die Trust Box mit der Protokollsoftware betrieben wird.

Gegen B2 wirkt SF3, da alle Zeitstempel vor deren Ausgabe protokolliert werden. Ist eine Protokollierung nicht möglich, wird ein Fehlercode an den User gegeben. Die Protokolldaten O5 werden nur durch das zugrunde liegende Betriebssystem des Protokollservers geschützt (siehe auch die Maßnahmen in Abschnitt 2.3).

Gegen B3 wirkt SF1, da nur zwei eingeloggte Administratoren die interne Uhr in Betrieb nehmen dürfen. Zur Sicherstellung der Identität findet eine Authentisierung statt.

Gegen B3 wirkt SF2, da unberechtigte Zugriffe auf den Uhrenstatus unterbunden werden.

2.8 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 2.7 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 neun von zehn Mechanismen als kritisch eingestuft und 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 eine 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.

Die Prüfstelle hat die Herstellertests stichprobenartig nachvollzogen und eigene Tests durchgeführt. Die Tests bestätigen, dass die bekannten Schwachstellen bei Beachtung der Hinweise an den Administrator in der Praxis nicht ausgenutzt werden können.

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. Die Installationsprozedur ist von der Prüfstelle nachvollzogen worden und es wurde festgestellt, dass die sichere Konfigurierbarkeit des EVG nur auf Basis von Bedienungsanleitung und Sicherheitshandbuch gegeben ist. 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 zwei operationelle Schwachstellen 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. Sie hat überprüft und festgestellt, dass alle Kombinationen von bekannten Schwachstellen untersucht wurden. 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 Bedienungsanleitung und im Sicherheitshandbuch ausreichend dokumentiert werden. Penetrationstests mussten von der Prüfstelle nicht durchgeführt werden, da die Gegenmaßnahmen zu den bekannten Schwachstellen in der Verantwortung der 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 defi-*

nierten 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.

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. Sie hat überprüft und festgestellt, dass die Trennung von sicherheitsspezifischen und anderen Komponenten wirksam ist.

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.***

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

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 wurden folgende Dokumentationen zur Verfügung gestellt:

- TSS 380/400 Bedienungsanleitung, Version 1.36, time proof TIME SIGNATURE SYSTEMS GmbH
- TSS 400 Sicherheitshandbuch, Version 1.19, time proof TIME SIGNATURE SYSTEMS GmbH

Die Prüfstelle hat bei der letzten Re-Evaluierung (EVG-Version 3.01) überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.25, E2.26) erfüllen. Die Ergebnisse der Evaluierung sind wie in Kapitel 1 dargestellt auch für diese aktualisierte Betriebsdokumentation gültig.

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: Die Systemverwalter-Dokumentation ist mit der oben angegebenen Benutzerdokumentation identisch. Die Prüfstelle hat bei der letzten Re-Evaluierung (EVG-Version 3.01) überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.28,

E2.29, E2.30) erfüllen. Die Ergebnisse der Evaluierung sind wie in Kapitel 1 dargestellt auch für diese aktualisierte Betriebsdokumentation gültig.

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 versiegelten CD und die Trust Box wird ebenfalls versiegelt. 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 Prüfstelle hat die beispielhaften Nachweise für den Anlauf und Betrieb erfolgreich überprüft. Sie 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
I&A	Identifizierung und Authentisierung
SigG	Signaturgesetz