Zertifizierungsbericht

Zertifizierungs-Vorgang:	**TUVIT-DSZ-ITSEC-9154**
Produkt / System:	G80-1502LQEDE Firmware Version 1.16
Hersteller:	Cherry GmbH Cherrystraße 19 92675 Auerbach
Auftraggeber:	s. o.
Prüfstelle:	Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH
Evaluierungsbericht:	*Version 1.1 vom 19.05.2004* Dokument-Nummer: *20611194_TÜV_031.02* Verfasser/in: Peter Herrmann
Formaler Ablauf:	vollständig / ordnungsgemäß durchgeführt
Ergebnis:	E2 / niedrig
Evaluierungsauflagen:	keine
Prüfbegleiter:	Dr. Silke Götze
Zertifizierungsauflagen:	keine

Essen, den 24.05.2004

Dr. Christoph Sutter Dr. Silke Götze

Inhaltsverzeichnis

1 GRUNDLAGE UND GEGENSTAND DER ZERTIFIZIERUNG 4

1.1 Evaluationsgegenstand (EVG) und Prüfkriterien 4

1.2 Durchführung der Evaluierung und Evaluierungsendbericht 4

1.3 Prüfergebnis der Evaluierung 4

1.4 Erweiterung der Ergebnisse auf andere Konfigurationen 5

1.5 Auflagen, Hinweise und Empfehlungen aus der Evaluation 5

1.6 Zertifizierungsauflagen und Hinweise 5

1.7 Unabhängigkeit des Prüfbegleiters 5

2 ZUSAMMENFASSUNG DER SICHERHEITSVORGABEN 5

2.1 Definition des EVG und Art der Nutzung 5
2.1.1 Definition des EVG 5
2.1.2 Art der Nutzung 6

2.2 Angenommene Einsatzumgebung 6
2.2.1 Technische Einsatzumgebung 6
2.2.2 Administrative Einsatzumgebung 6

2.3 Subjekte, Objekte und Zugriffsarten / Aktionen 7

2.4 Bedrohungen und Sicherheitsziele 7
2.4.1 Bedrohungen 7
2.4.2 Sicherheitsziele und Sicherheitseigenschaften 7

2.5 Sicherheitsfunktionen 7

2.6 Korrelation Sicherheitsfunktionen / Bedrohungen / Sicherheitsziele 8

2.7 Evaluationsstufe und Mechanismenstärke 10

3 ERGEBNISSE DER EVALUIERUNG 10

3.1 Wirksamkeit – Konstruktion 10
3.1.1 Aspekt 1: Eignung der Funktionalität 10
3.1.2 Aspekt 2: Zusammenwirken der Funktionalität 10

3.1.3 Aspekt 3: Stärke der Mechanismen 11
3.1.4 Aspekt 4: Bewertung der Konstruktionsschwachstellen 11

3.2 Wirksamkeit – Betrieb 13
3.2.1 Aspekt 1: Benutzerfreundlichkeit 13
3.2.2 Aspekt 2: Bewertung der operationellen Schwachstellen 13

3.3 Korrektheit – Konstruktion – Entwicklungsprozess 15
3.3.1 Phase 1: Anforderungen (Sicherheitsvorgaben) 15
3.3.2 Phase 2: Architekturentwurf 15
3.3.3 Phase 3: Feinentwurf 16
3.3.4 Phase 4: Implementierung 16

3.4 Korrektheit – Konstruktion – Entwicklungsumgebung 17
3.4.1 Aspekt1: Konfigurationskontrolle 17
3.4.2 Aspekt2: Programmiersprachen und Compiler 17
3.4.3 Aspekt3: Sicherheit beim Entwickler 17

3.5 Korrektheit – Betrieb – Betriebsdokumentation 18
3.5.1 Aspekt1: Benutzerdokumentation 18
3.5.2 Aspekt2: Systemverwalterdokumentation 18

3.6 Korrektheit – Betrieb – Betriebsumgebung 19
3.6.1 Aspekt1: Auslieferung und Konfiguration 19
3.6.2 Aspekt2: Anlauf und Betrieb 20

4 AUSZUG AUS ITSEC UND ITSEM 20

4.1 Vertrauenswürdigkeit - Wirksamkeit 20

4.2 Vertrauenswürdigkeit – Korrektheit 21

4.3 Klassifizierung von Sicherheitsmechanismen 22

4.4 Mindeststärke der Sicherheitsmechanismen 22

5 LITERATURREFERENZEN 23

6 ABKÜRZUNGEN 23

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 hat die PC-Tastatur mit integriertem Chipkartenleser G80-1502LQEDE, Firmware Version 1.16 der Firma Cherry GmbH, Cherrystraße 19, 92675 Auerbach als Gegenstand und bescheinigt, dass dieser auf Grundlage der *"Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik Version 1.2 (1991)"*[2] und des *„Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik Version 1.0 (1993)"*[3], gegen die produktspezifischen Sicherheitsvorgaben von der Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH[4] 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 17.11.2003 bis zum 19.05.2004 von Peter Herrmann durchgeführt. Die Leitung der Evaluierung wurde von Hans-Werner Blißenbach wahrgenommen und der Evaluierungsendbericht Version 1.1 vom 19.05.2004 (Nummer: 20611194_TÜV_031.02) wurde von Peter Herrmann 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[5] um ein Produkt, welches die Sicherheitsfunktionalität gemäß „Technische Spezifikation der Arztausstattung – Lesegeräte", Version 2.00; Stand 06. März 2003, gültig ab 01. Januar 2003 aufweist:

- Wiederaufbereitung
- Unverfälschtheit
- Schreibschutz

[1] Im folgenden kurz BSI genannt

[2] Im folgenden kurz ITSEC genannt

[3] Im folgenden kurz ITSEM genannt

[4] Im folgenden kurz Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH genannt

[5] Im folgenden kurz EVG genannt

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

1.4 Erweiterung der Ergebnisse auf andere Konfigurationen

Der EVG ist durch den Namen G80-1502LQEDE-2 mit dem Index 05 und G80-1502LQEDE-0 mit dem Index 02 und die Versionsnummer (Firmware Version 1.16) eindeutig gekennzeichnet. Eine Erweiterung der Ergebnisse auf andere Konfigurationen des EVG ist nicht möglich.

Jede Änderung der Hardware/Firmware 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

In dem Evaluierungsendbericht sind keine Auflagen, Hinweise oder Empfehlungen an den Hersteller enthalten.

1.6 Zertifizierungsauflagen und Hinweise

Aus dem Zertifizierungsbericht ergeben sich keine Auflagen oder Hinweise.

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

Beim Evaluationsgegenstand (EVG) handelt sich um eine Standardtastatur mit integriertem Chipkarteninterface (G80-1502LQEDE), zum Verarbeiten von Speicher- und Prozessorchipkarten und besitzt darüber hinaus die Eigenschaft, eindeutig eine Versichertenkarte anhand ihrer Spezifikationsmerkmale zu erkennen und entsprechend der Spezifikation zu verarbeiten. Diese Verarbeitung einer Versichertenkarte ist Gegenstand der Evaluierung.

Die PC-Tastatur mit integriertem Chipkartenterminal wird in folgenden Varianten evaluiert:

- G80-1502LQEDE-2 (Farbe hellgrau) mit dem Index 05 oder
- G80-1502LQEDE-0 (Farbe schwarz) mit dem Index 02.

Die aufgelisteten Produkte unterscheiden sich lediglich in der Farbstellung des Gehäuses. Mechanisch und elektrisch basieren beide Varianten auf dem gleichen Schaltungskonzept und Firmwarestand. Das gilt insbesondere auch für die sicherheitsrelevanten Hardwarekomponenten und die Firmware des EVG, welche die sicherheitsspezifischen Funktionen für beide Varianten identisch realisiert. Die Firmware des Chipkartenterminals besitzt folgende Identifikation:

- Firmware 835-0804 Index 01 (FW Version 1.16)

Das Chipkartenterminal unterstützt eine sichere PIN-Eingabe. Diese sichere PIN-Eingabe ist **nicht** Gegenstand der Evaluierung.

2.1.2 Art der Nutzung

Die PC-Tastatur mit integriertem Chipkartenterminal G80-1502LQEDE stellt im Sinne der ITSEC ein IT-Produkt dar (ITSEC 6.48).

Zweck und der Einsatzbereich des EVG ist es sowohl Speicherchipkarten als auch Prozessorchipkarten zu verarbeiten. Er ist damit für einen universellen Einsatz in chipkartenbasierenden Applikationen bei Ärzten und Kliniken vorgesehen. Prinzipiell kann das Chipkartenterminal aber auch für weitere Applikationen wie Homebanking oder Zugriffskontrolle verwendet werden.

Gegenstand der Zertifizierung ist jedoch nur die Verarbeitung von Speicherkarten im Sinne der Technischen Spezifikation der Arztausstattung – Lesegeräte, Version 2.00; Stand 06. März 2003, gültig ab 01. Januar 2003, also das Lesen und die Ausgabe der Daten von Versichertenkarten. Insbesondere gehört eine sichere PIN-Eingabe **nicht** zum Umfang der Evaluierung.

Die Übertragung der Daten der Versichertenkarte zwischen EVG und dem PC kann wahlweise über die Tastaturschnittstelle (PS/2) oder die serielle Schnittstelle (RS-232) erfolgen. Bei Übertragungen der Daten über die Tastaturschnittstelle verwendet der Hersteller ein proprietäres Protokoll, bei Übertragungen über die serielle Schnittstelle kommt das T=1 Protokoll mit einem vermindertem Funktionsumfang zum Einsatz.

2.2 Angenommene Einsatzumgebung

2.2.1 Technische Einsatzumgebung

Die technische Einsatzumgebung des EVG setzt ein PC-System mit Mini-DIN-Buchse als Tastaturschnittstelle (PS/2) und optional eine 9-polige SUB-D Buchse für die serielle Schnittstelle (RS-232) voraus. Als Chipkarten werden folgende Speicherkarten des deutschen Krankenversicherungswesens verwendet:

- Versichertenkarten mit serial data access protocol (I²C-Bus, S = 8)
- Versichertenkarten mit 3 wire bus protocol (I²C-Bus, S = 9)
- Versichertenkarten mit 2 wire bus protocol (I²C-Bus, S = 10)

2.2.2 Administrative Einsatzumgebung

Das Chipkartenterminal soll in einer sicheren Umgebung (Arztpraxis, Krankenhäuser, Rehakliniken und medizinisches Umfeld) betrieben werden. Es ist sicher zu stellen, dass ein Zugang durch Unbefugte vermieden wird.

2.3 Subjekte, Objekte und Zugriffsarten / Aktionen

- Subjekte sind alle autorisierten und nicht autorisierten Personen.
- Objekte sind die Krankenversichertenkartendaten.
- Zugriffsart ist das Einlesen und die Ausgabe der Krankenversichertenkartendaten.

2.4 Bedrohungen und Sicherheitsziele

2.4.1 Bedrohungen

Für den angenommenen Einsatz werden die folgenden vier Bedrohungen angenommen:

B1: Unbefugtes Sammeln von Versichertenkartendaten

Es könnten im EVG abgelegte Krankenversichertendaten unbefugt abgerufen oder sichtbar gemacht werden.

B2: Manipulieren von Daten der Versichertenkarte

Es könnten die Krankenversichertendaten im EVG oder auf der Chipkarte verändert werden.

B3: Ungültige Versichertenkarten einbringen

Es könnte eine ungültige Versichertenkarte vom EVG eingelesen werden, um ungültige Krankenversichertendaten zum PC-System zu übertragen.

B4: Fehlerhafte Ausgabe der Versichertenkartendaten

Es könnten fehlerhafte Krankenversichertendaten vom EVG zum PC-System übertragen werden.

2.4.2 Sicherheitsziele und Sicherheitseigenschaften

Der EVG hat das folgende Sicherheitsziele:

SZ1: Das Chipkartenlesegerät soll jede gültige Versichertenkarte lesen.

SZ2: Die Daten der Versichertenkarte dürfen weder auf der Karte verändert oder gelöscht noch im Chipkartenlesegerät verändert werden.

SZ3: Ungültige Versichertenkarten sollen identifiziert und abgelehnt werden.

SZ4: Eine Fehlbedienung wird vom EVG erkannt und muss zu einer definierten Fehlerbehandlung führen.

SZ5: Die vom Chipkartenlesegerät übernommenen Daten sind gegen unbefugten Zugriff geschützt.

SZ6: Die Daten einer Versichertenkarte dürfen nur solange im Chipkartenlesegerät zwischengespeichert sein, wie die Versichertenkarte sich im Lesegerät befindet.

SZ7: Daten ungültiger Versichertenkarten dürfen nicht zum PC-System übertragen werden.

2.5 Sicherheitsfunktionen

Zur Erreichung der Sicherheitsziele und zur Abwehr der Bedrohungen enthält der EVG die folgenden fünf sicherheitsspezifischen Funktionen:

SF1: Nach der Entnahme der Versichertenkarte aus dem Chipkartenlesegerät wird der Speicherbereich, der für die Überprüfung der Versichertenkartendaten reserviert wurde, wiederaufbereitet.

SF2: Es wird durch Prüfsummenverfahren sichergestellt, dass eine unverfälschte Datenübertragung von der Versichertenkarte zum Chipkartenlesegerät erfolgt.

SF3: Die Versichertenkarte kann nicht beschrieben werden.

SF4: Das Chipkartenlesegerät überprüft die Kartendaten und weist sie eindeutig als gültige oder ungültige Versichertenkarte aus.

SF5: Das Lesegerät überträgt nur Daten einer gültigen Versichertenkarte zum PC-System.

Unterstützt werden diese Sicherheitsfunktionen durch folgende organisatorische Sicherheitsmaßnahme:

ORG1: Das Chipkartenterminal soll in einer sicheren Umgebung (Arztpraxis, Krankenhäuser, Rehakliniken und medizinisches Umfeld) betrieben werden. Es ist sicher zu stellen, dass ein Zugang durch Unbefugte vermieden wird. Weitere organisatorische Maßnahmen sind nicht zu treffen, um das Produkt einzusetzen.

2.6 Korrelation Sicherheitsfunktionen / Bedrohungen / Sicherheitsziele

Die folgende Tabelle zeigt welche Sicherheitsfunktionen zur Erreichung der Sicherheitsziele und Abwehr der Bedrohungen herangezogen werden:

Bedrohungen	Sicherheitsziele						
	SZ1	SZ2	SZ3	SZ4	SZ5	SZ6	SZ7
B1					ORG1 SF1	SF1	
B2		SF3 SF1			ORG1 SF1	SF1	
B3	SF4 SF5		SF4 SF5	SF4			
B4							SF2 SF5

Die Sicherheitsfunktionen sind für die vorgesehene Art der Nutzung des G80-1502LQEDE sowohl geeignet als auch zweckmäßig. Im einzelnen gilt dabei folgendes:

ORG1 erfüllt SZ5, weil das Lesegerät in einer definiert sicheren Umgebung (Arztpraxis) eingesetzt wird.

ORG1 wirkt gegen B1 und B2, weil die Bedienung nur durch das Praxispersonal zulässig ist.

SF1 erfüllt SZ2, da eine zufällige Datenvermischung nach Entnahme der Versichertenkarte verhindert wird. Außerdem erfüllt SF1 SZ5 und SZ6, da nach Entnahme der Versichertenkarte der Speicherbereich im Lesegerät aufbereitet wird.

SF1 wirkt gegen B1 und B2, weil nach Entnahme der Versichertenkarte aus dem Lesegerät keine persönlichen Daten mehr im Lesegerät zur Verfügung stehen.

SF2 erfüllt SZ7, weil nur bei positivem Prüfsummenverfahren Daten ans System übertragen werden.

SF2 wirkt gegen B4, weil über das Prüfsummenverfahren eine fehlerhafte Übertragung von der Versichertenkarte zum Lesegerät erkannt wird.

SF3 erfüllt SZ2, weil ein spezifikationsgemäßes Beschreiben der Karte nicht möglich ist.

SF3 wirkt gegen B2, weil ein Schreiben auf eine Versichertenkarte durch die Firmware verhindert wird.

SF4 erfüllt SZ1, SZ3 und SZ4, weil sie jede Karte im Kartenschacht eindeutig als gültige oder ungültige Versichertenkarte ausweist. Wird eine Karte als ungültig erkannt, so kann nicht auf die Karte zugegriffen werden und die Fehleranzeige wird aktiviert.

SF4 wirkt gegen B3, weil ungültige Versichertenkarten eindeutig erkannt und optisch angezeigt werden.

SF5 erfüllt SZ1, weil jede gültige Versichertenkarte gelesen wird. Des weiteren erfüllt SF5 SZ3 und SZ7, weil Daten einer ungültigen Versichertenkarte nicht zum PC-System übertragen werden.

SF5 wirkt gegen B3, weil keine Daten von ungültigen Versichertenkarten übertragen werden und gegen B4, weil eine fehlerhafte Übertragung von Versichertenkartendaten erkannt wird.

2.7 Evaluationsstufe und Mechanismenstärke

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

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

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 vorhandenen Mechanismen als kritisch eingestuft und in einen Typ A und vier Typ 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 niedrig. Von der Prüfstelle sind Penetrationstests durchgeführt worden, die die Mindeststärke der Mechanismen 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 wurde eine Schwachstelle vom Hersteller angegeben, die von der Prüfstelle mit dem Ergebnis überprüft wurde, dass die bekannte Schwachstelle in der Praxis nicht ausnutzbar ist. Die Prüfstelle hat eine eigene Schwachstellenanalyse durchgeführt und keine weitere Schwachstellen in der Konstruktion gefunden. Da nur eine Schwachstelle vorlag entfiel die Untersuchung der Kombinationen der bekannten Schwachstellen. Die Prüfstelle hat überprüft und festgestellt, dass die Analysen der möglichen Auswirkungen der Schwachstelle 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 Penetrationstests durchgeführt und bestätigt, dass die bekannte Schwachstelle in der Praxis wirklich 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 ordnungsgemäß dokumentiert wurden. Jede Konfigurations- und Installationsprozedur ist von der Prüfstelle nachvollzogen worden und es wurde festgestellt, dass der EVG sicher konfiguriert und benutzt werden kann, wenn lediglich die Dokumentation für den Nutzer und Administrator zu Grunde gelegt wird. Zusätzliche 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: Die Prüfstelle hat überprüft und festgestellt, dass die Liste der bekannten operationellen Schwachstellen alle Forderungen bezüglich Inhalt, Form und Nachweise (ITSEC 3.35, 3.36), so wie oben beschrieben, erfüllt. Sie hat überprüft und festgestellt, dass die Analyse alle relevanten Informationen verwendet hat.

Es wurde keine Schwachstelle vom Hersteller angegeben. Die Prüfstelle hat eine eigene Schwachstellenanalyse durchgeführt und keine operationelle Schwachstellen gefunden. Damit entfiel die Untersuchung der bekannten Schwachstellen, die Überprüfung der Analyse der möglichen Auswirkungen der Schwachstellen. Sie hat überprüft und festgestellt, dass alle Annahmen und Anforderungen bezüglich externer Sicherheitsmaßnahmen ausreichend dokumentiert sind.

Es wurden keine operationellen Schwachstellen identifiziert. Daher wurden keine Penetrationstests durch die Prüfstelle zur Ausnutzbarkeit der operationellen Schwachstellen durchgeführt.

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[6] 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

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

(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.***

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:

- Kurzanleitung, Chipkarten-Tastatur MultiBoard G80-1502, Artikelnummer 644-0324.01 DE Mai 2004

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:

- Kurzanleitung, Chipkarten-Tastatur MultiBoard G80-1502, Artikelnummer 644-0324.01 DE Mai 2004

Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E2.28, E2.29) 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 des EVG erfolgt in einer Kartonverpackung an die Distributoren und OEM-Kunden, von dort über den Handel und Systemhäuser an den Endkunden. Die Authentizität des EVG wird durch den Typschildaufkleber sowie das auf das Gehäuse aufgebrachte Siegel garantiert.

Die Auslieferung entspricht einem in der vom BSI herausgegebenen AIS 10 angegebenen Verfahren, das für die Evaluationsstufe E2 zugelassen ist.

Eine Systemgenerierung findet nicht statt.

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 beispielhafte Nachweise für den Anlauf und den Betrieb 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