Zertifizierungsreport

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0185-2002

zu

DATA-Defender 1.0

der

Fachhochschule Aachen

Fachbereich Elektrotechnik und Informationstechnik

und

IBH-IMPEX Elektronik GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0185-2002

DATA-Defender 1.0

der

Fachhochschule Aachen

Fachbereich Elektrotechnik und Informationstechnik

und

IBH-IMPEX Elektronik GmbH

Common Criteria Vereinbarung

Das in diesem Zertifikat genannte IT-Produkt wurde nach den *Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1,* unter Nutzung der *Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Teil 1 Version 0.6, Teil 2 Version 1.0*, evaluiert.

Prüfergebnis:

Funktionalität:	**Produktspezifische Sicherheitsvorgaben** **Schutz der Benutzerdaten durch Überlagerung (Superposition) der kompromittierenden elektromagnetischen Emissionen durch ein besonderes Schutzsignal**
Vertrauenswürdigkeitspaket:	**CC Teil 3 konform** **EAL 1**

Dieses Zertifikat gilt nur für die angegebene Version des Produktes in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport.

Die Evaluation wurde in Übereinstimmung mit den Bestimmungen des Zertifizierungsschemas des Bundesamtes für Sicherheit in der Informationstechnik durchgeführt. Die im Evaluationsbericht enthaltenen Schlussfolgerungen der Prüfstelle sind in Einklang mit den erbrachten Nachweisen.

Die auf der Rückseite aufgeführten Anmerkungen sind Bestandteil dieses Zertifikates.

Bonn, den 8. Mai 2002

Der Präsident des Bundesamtes für
Sicherheit in der Informationstechnik

IT Security Certified

Dr. Henze L.S. SOGIS-MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik, Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers - im folgenden Antragsteller genannt - durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produktes gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produktes, die Einzelheiten der Bewertung und Hinweise für den Anwender.

[1] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

Gliederung

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

Die Zertifizierungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- BSIG[2]
- BSI-Zertifizierungsverordnung[3]
- BSI-Kostenverordnung[4]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN 45011
- BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1[5]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM)
  - Teil 1, Version 0.6
  - Teil 2, Version 1.0
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)

---

[2] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember 1990, Bundesgesetzblatt I S. 2834

[3] Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung-BSIZertV) vom 7.Juli 1992, Bundesgesetzblatt I S. 1230

[4] Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 29. Oktober 1992, Bundesgesetzblatt I S. 1838

[5] Bekanntmachung des Bundesministeriums des Innern vom 22. September 2000 im Bundesanzeiger S. 19445

2 Anerkennungsvereinbarungen

Um die Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von IT-Sicherheitszertifikaten - sofern sie auf ITSEC oder Common Criteria (CC) beruhen - unter gewissen Bedingungen vereinbart. Zertifikate der Unterzeichnerstaaten werden damit in den jeweils anderen Unterzeichnerstaaten anerkannt.

2.1 ITSEC/CC - Zertifikate

Das SOGIS-Abkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten, auf Grundlage der ITSEC, ist am 3. März 1998 in Kraft getreten. Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Evaluationsstufe EAL7 erweitert.

2.2 CC - Zertifikate

Im Mai 2000 wurde eine Vereinbarung (Common Criteria-Vereinbarung) über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und Schutzprofilen auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 zwischen den nationalen Stellen in Australien, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Kanada, Neuseeland, Niederlande, Norwegen, Spanien und den USA unterzeichnet. Im November 2000 ist Israel der Vereinbarung beigetreten, Schweden im Februar 2002.

3 Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Produkt DATA-Defender 1.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts DATA-Defender 1.0 wurde von der Schlumberger Sema - Competence Center Informatik GmbH im Rahmen einer erweiterten Prüfbegleitung durch das BSI durchgeführt.

Antragsteller und Entwickler ist die Fachhochschule Aachen, Fachbereich Elektrotechnik und Informationstechnik, Labor für Nachrichtentechnik und EMV. Hersteller ist die IBH-IMPEX Elektronik GmbH.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 8. Mai 2002 vom BSI abgeschlossen.

Das bestätigte Vertrauenswürdigkeitspaket gilt nur unter der Voraussetzung, dass

- alle Auflagen bzgl. Generierung, Konfiguration und Betrieb, soweit sie im nachfolgenden Bericht angegeben sind, beachtet werden,
- das Produkt in der beschriebenen Umgebung - sofern im nachfolgenden Bericht angegeben - betrieben wird.

Dieser Zertifizierungssreport gilt nur für die hier angegebene Version des Produktes. Die Gültigkeit kann auf neue Versionen und Releases des Produktes ausgedehnt werden, sofern der Antragsteller eine Re-Zertifizierung des geänderten Produktes entsprechend den Vorgaben beantragt und die Prüfung keine sicherheitstechnischen Mängel ergibt.

Hinsichtlich der Bedeutung der Vertrauenswürdigkeitsstufen und der bestätigten Stärke der Funktionen vgl. die Auszüge aus den technischen Regelwerken am Ende des Zertifizierungsreports.

4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-10.

Das Produkt DATA-Defender 1.0 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller[6] des Produktes angefordert werden. Unter der o. g. Internetadresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

[6] IBH-IMPEX Elektronik GmbH, Friederikenplatz 55a, 06844 Dessau

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

Gliederung des Zertifizierungsberichtes

1 Zusammenfassung

Personal Computer und deren CRT- und TFT-Monitore setzen kompromittierende Emissionen (CEM) in unterschiedlicher elektromagnetischer Form frei:

- als hochfrequente Strahlung,
- als hochfrequente Oberflächenwellen entlang metallischer Leiter,
- als hochfrequente, elektrische Spannungen und Ströme im Energieversorgungsnetz.

Der EVG erzeugt exakt auf den Frequenzen der kompromittierenden, hochfrequenten Emissionen digitale Rauschsignale, die sich allen 3 Formen elektromagnetischer kompromittierender Emissionen überlagern.

Durch die Überlagerung wird die Dekodierung der kompromittierenden hochfrequenten Signale verhindert, weil die kompromittierenden Signale und die digitalen Rauschsignale nicht mehr separierbar sind.

Der EVG ist betreibbar mit den international üblichen Netzspannungen. Er hat kleines Bauvolumen und geringes Gewicht. Er kann nahezu unauffällig zu jedem PC oder Monitor gestellt werden.

Die Evaluation des Produkts DATA-Defender 1.0 wurde von der Schlumberger Sema - Competence Center Informatik GmbH durchgeführt und am 24. April 2002 abgeschlossen.

Antragsteller und Entwickler ist die Fachhochschule Aachen, Fachbereich Elektrotechnik, Labor für Nachrichtentechnik und EMV. Hersteller ist die IBH-IMPEX Elektronik GmbH.

1.1 Vertrauenswürdigkeitspaket

Der EVG erfüllt die Vertrauenswürdigkeitsanforderungen der Vertrauenswürdigkeitsstufe 1 (EAL 1) – funktionell getestet.

1.2 Funktionalität

TSF_SUP.1 Schutz der Benutzerdaten durch Überlagerung (Superposition) der kompromittierenden Emissionen durch ein besonderes Schutzsignal

1.3 Stärke der Funktionen

Die Stärke der Funktionen wird beim Vertrauenswürdigkeitspaket EAL 1 nicht bewertet, da EAL 1 keine Komponente aus der Familie AVA_SOF enthält, die sich mit der Bewertung der Stärke der Funktionen befasst.

1.4 Zusammenfassung der Bedrohungen und der organisatorischen Sicherheitspolitik, auf die das evaluierte Produkt ausgerichtet ist

Ein Angreifer mit grundlegenden Kenntnissen der Hochfrequenztechnik könnte versuchen, die kompromittierenden Emissionen eines PC's zu empfangen und zu dekodieren, um Kenntnisse über vertrauliche Informationen zu erhalten.

Sicherheitspolitiken wurden nicht definiert. Sämtlichen Sicherheitsanforderungen sind von den Bedrohungen abgeleitet.

1.5 Spezielle Konfigurationsanforderungen

Der EVG wird als fertiges und einsatzbereites Gerät geliefert. Es gibt daran keine Einstell- oder Programmiermöglichkeiten und somit keine unterschiedlichen Konfigurationen.

1.6 Annahmen über die Einsatzumgebung

Der EVG kann nur an PC-Arbeitsplätzen eingesetzt werden,

- deren Konfiguration einen abgesetzten, nicht im PC integrierten, über steckbare, 15-polige Kabel angeschlossenen Monitor beinhaltet und
- in denen die Pixelfrequenz des Signals von der Grafikkarte zum Monitor (Monitorsignal) zwischen 20 MHz und 80 MHz liegt.

Der EVG wird zwischen PC und Monitor mittels des Monitorkabels eingeschleift.

1.7 Gewährleistungsausschluß

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluß hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluß hatte, ist weder enthalten noch zum Ausdruck gebracht.

2 Identifikation des EVG

Zum Lieferumfang des EVG gehören:

DATA - Defender	Version 1.0	Hardware
Netzgerät mit Netz- und Geräteanschlusskabel, 230 V / 6 V		Hardware
15-poliges Monitorverlängerungskabel		Hardware
Benutzer-Handbuch mit - Geräteidentifikation, - allgemeiner Funktionsbeschreibung, - betriebliche Vorgaben zur Logistik und zum Einsatzbereich, - technischer Betriebsanleitung.	Version 1.0	Papier

3 Sicherheitspolitik

Die Sicherheitspolitik des EVG ist es, den möglichen Verlust der Vertraulichkeit von Daten, der durch kompromittierende Emissionen eines PC's verursacht wird, zu verhindern. Zu diesem Zweck stellt der EVG eine Funktionalität zur Verfügung, die verhindert, dass die kompromittierenden Emissionen eines PC's aus seinen Gesamt-Emissionen dekodiert werden können.

4 Annahmen und Klärung des Einsatzbereiches

4.1 Annahmen über den Einsatz

Für den EVG (TOE) und den PC, an dem der EVG eingesetzt wird, ist eine gesicherte Logistik bei den Nutzern des EVG, wie z.B. Organisationen, Einrichtungen, Unternehmen und Betrieben, vorhanden. EVG und PC sind nur autorisierten Nutzern zugänglich, um das Risikopotential aus Manipulation und Austausch zu reduzieren.

Andernfalls sind vor jeder Nutzung die Gehäusesiegel und das Typenetikett zu prüfen.

4.2 Angenommene Einsatzumgebung

Der EVG wird an PC-Arbeitsplätzen eingesetzt, deren

- Pixelfrequenz von 20 MHz bis zu 80 MHz beträgt.
- gesamte elektromagnetische Emissionen, bestehend aus kompromittierenden und nicht kompromittierenden Emissionen, unter den zulässigen EMV-Grenzpegeln der europäischen EMV-Normen (emc-standards) für gestrahlte und leitungsgebundene Emissionen liegen.
- Konfiguration einen abgesetzten, nicht im PC integrierten, über steckbare, 15-polige Kabel angeschlossenen Monitor beinhaltet. Der EVG wird zwischen PC und Monitor mittels des Monitorkabels eingeschleift.

4.3 Klärung des Einsatzbereich

Der EVG schützt die an einem PC verarbeiteten Daten vor den Verlust der Vertraulichkeit, der durch die kompromittierenden hochfrequenten elektromagnetischen Emissionen eines PC's verursacht werden kann. Weiteren Bedrohungen der Vertraulichkeit, z. B. durch unbefugten Zugriff auf den PC, ist durch entsprechende zusätzlichen Maßnahmen zu begegnen.

5 Informationen zur Architektur

Die Vertrauenswürdigkeitsstufe EAL 1 fordert vom Hersteller keine Informationen zur Architektur.

6 Dokumentation

Das nachstehend genannte Dokument wird zusammen mit dem Produkt an den Kunden ausgeliefert:

Benutzerhandbuch – DATA-Defender 1.0 –, Version 1.0 vom 27. Februar 2002

7 Testverfahren

EAL 1 fordert keine Tests des Entwicklers.

Für die unabhängigen Tests hat die Prüfstelle einen Testplan erstellt und dem entsprechend alle wichtigen Eigenschaften, der vom EVG zur Verfügung gestellten Sicherheitsfunktionalität, getestet.

8 Evaluierte Konfiguration

Die evaluierte Konfiguration des EVG ist das handelsübliche Gerät DATA-Defender, Version 1.0, mit dem in Kapitel 2 angegebenen Lieferumfang.

Der EVG wird als fertiges und einsatzbereites Gerät geliefert. Es gibt daran keine Einstell- oder Programmiermöglichkeiten und somit keine unterschiedlichen Konfigurationen.

9 Ergebnisse der Evaluierung

Der EVG erfüllt alle Vertrauenswürdigkeitsanforderungen nach EAL 1. Die Ergebnisse zu den einzelnen Vertrauenswürdigkeitskomponenten sind in der nachstehenden Tabelle zusammengefasst:

Vertrauenswürdigkeits-klasse	**EAL 1 Vertrauenswürdigkeits-komponente**	**Urteil**
Sicherheitsvorgaben	ASE_DES.1	erfüllt
	ASE_ENV.1	erfüllt
	ASE_INT.1	erfüllt
	ASE_OBJ.1	erfüllt
	ASE_PPC.1	erfüllt
	ASE_REQ.1	erfüllt
	ASE_SRE.1	erfüllt
	ASE_TSS.1	erfüllt
Konfigurationsmanagement	ACM_CAP.1	erfüllt
Auslieferung und Betrieb	ADO_IGS.1	erfüllt
Entwicklung	ADV_FSP.1	erfüllt
	ADV_RCR.1	erfüllt
Handbücher	AGD_ADM.1	erfüllt
	AGD_USR.1	erfüllt
Testen	ATE_IND.1	erfüllt

10 Kommentare und Empfehlungen des Evaluators

Es gibt keine zusätzlichen Empfehlungen und Hinweise zu denen in [5] und [6].

11 Anhänge

keine

12 Sicherheitsvorgaben

Die Sicherheitsvorgaben [5] sind als separates Dokument veröffentlicht.

13 Definitionen[7]

13.1 Abkürzungen

CC Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

EVG Evaluierungsgegenstand

IT Informationstechnik

PP Protection Profile - Schutzprofil

SF Sicherheitsfunktion

SOF Strength of Function - Stärke der Funktionen

ST Security Target - Sicherheitsvorgaben

TSC TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle

TSF TOE Security Functions - EVG-Sicherheitsfunktionen

TSP TOE security policy - EVG-Sicherheitspolitik

13.2 Glossar

Zusatz - Das Hinzufügen einer oder mehrerer Vertrauenswürdigkeitskomponenten aus Teil 3 der CC zu einer EAL oder einem Vertrauenswürdigkeitspaket.

Erweiterung - Das Hinzufügen von funktionalen Anforderungen, die nicht in Teil 2 enthalten sind, und/oder von Vertrauenswürdigkeitsanforderungen, die

[7] deutsche Übersetzung

nicht in Teil 3 enthalten sind, zu den Sicherheitsvorgaben bzw. dem Schutzprofil.

Formal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik, die auf bewährten mathematischen Konzepten basiert.

Informell - Ausgedrückt in natürlicher Sprache.

Objekt - Eine Einheit im TSC, die Informationen enthält oder empfängt und mit der Subjekte Operationen ausführen.

Schutzprofil - Eine implementierungsunabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG, die besondere Konsumentenbedürfnisse erfüllen.

Sicherheitsfunktion - Ein Teil oder Teile eines EVG, auf die zur Durchsetzung einer hierzu in enger Beziehung stehenden Teilmenge der Regeln der EVG-Sicherheitspolitik Verlaß sein muß.

Sicherheitsvorgaben - Eine Menge von Sicherheitsanforderungen und Sicherheitsspezifikationen, die als Grundlage für die Prüfung und Bewertung eines angegebenen EVG dienen.

Semiformal - Ausgedrückt in einer Sprache mit beschränkter Syntax und festgelegter Semantik.

Stärke der Funktionen - Eine Charakterisierung einer EVG-Sicherheitsfunktion, die den geringsten angenommenen Aufwand beschreibt, der notwendig ist, um deren erwartetes Sicherheitsverhalten durch einen direkten Angriff auf die zugrundeliegenden Sicherheitsmechanismen außer Kraft zu setzen.

SOF-Niedrig - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen angemessenen Schutz gegen zufälliges Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein geringes Angriffspotential verfügen.

SOF-Mittel - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen angemessenen Schutz gegen naheliegendes oder absichtliches Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein mittleres Angriffspotential verfügen.

SOF-Hoch - Eine Stufe der EVG-Stärke von Funktionen, bei der die Analyse zeigt, dass die Funktionen einen geeigneten Schutz gegen geplantes oder organisiertes Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein hohes Angriffspotential verfügen.

Subjekt - Eine Einheit innerhalb des TSC, die die Ausführung von Operationen bewirkt.

Evaluationsgegenstand - Ein IT-Produkt oder -System - sowie die dazugehörigen Systemverwalter- und Benutzerhandbücher - das Gegenstand einer Prüfung und Bewertung ist.

EVG-Sicherheitsfunktionen - Eine Menge, die die gesamte Hardware, Software, und Firmware des EVG umfaßt, auf die Verlaß sein muß, um die TSP korrekt zu erfüllen.

EVG-Sicherheitspolitik - Eine Menge von Regeln, die angibt, wie innerhalb eines EVG Werte verwaltet, geschützt und verteilt werden.

Anwendungsbereich der TSF-Kontrolle - Die Menge der Interaktionen, die mit oder innerhalb eines EVG vorkommen können und den Regeln der TSP unterliegen.

14 Literaturangaben

[1] Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.1 (ISO/IEC 15408)

[2] Gemeinsame Methodologie Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Teil 1 Version 0.6, Teil 2 Version 1.0

[3] BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125, Version 5.1, Januar 1998)

[4] Deutsche IT-Sicherheitszertifikate (BSI 7148, BSI 7149)

[5] Sicherheitsvorgaben – DATA-Defender 1.0 –, Version 1.0 vom 19. April 2002

[6] Benutzerhandbuch – DATA-Defender 1.0 –, Version 1.0 vom 27. Februar 2002

C Auszüge aus den technischen Regelwerken

CC Teil 1[8]:

Kennzeichnung der Evaluationsergebnisse (Kapitel 5.4)

„Das Ergebnis „akzeptierend“ einer Prüfung und Bewertung muß eine Darlegung sein, die beschreibt, bis zu welchem Grad dem EVG vertraut werden kann, die Anforderungen zu erfüllen. Die Ergebnisse müssen bezüglich Teil 2 (funktionale Anforderungen), Teil 3 (Vertrauenswürdigkeitsanforderungen) oder direkt eines PP wie folgt gekennzeichnet sein:

a. **Konform zu Teil 2** - Ein PP oder EVG ist konform zu Teil 2, wenn die funktionalen Anforderungen nur aus den in Teil 2 enthaltenen funktionalen Komponenten erstellt wurden.

b. **Teil 2 erweitert** - Ein PP oder EVG ist Teil 2 erweitert, wenn darin funktionale Anforderungen enthalten sind, die nicht aus Teil 2 stammen.

c. **Konform zu Teil 3** - Ein PP oder EVG ist konform zu Teil 3, wenn die Anforderungen an die Vertrauenswürdigkeit die Form einer **EAL** oder eines ausschließlich aus Vertrauenswürdigkeitskomponenten aus Teil 3 erstellten **Vertrauenswürdigkeitspakets** haben.

d. **Teil 3 mit Zusatz -** Ein PP oder EVG wird mit Teil 3 mit Zusatz gekennzeichnet, wenn die Anforderungen an die Vertrauenswürdigkeit die Form einer **EAL** oder eines **Vertrauenswürdigkeitspakets** haben und zusätzlich andere Vertrauenswürdigkeitskomponenten aus Teil 3 eingebunden sind.

e. **Teil 3 erweitert** - Ein PP oder EVG ist Teil 3 erweitert, wenn die Anforderungen an die Vertrauenswürdigkeit die Form einer **EAL** haben, die mit zusätzlichen, nicht in Teil 3 enthaltenen Vertrauenswürdigkeitsanforderungen verknüpft ist oder einem **Vertrauenswürdigkeitspaket**, das aus Vertrauenswürdigkeitsanforderungen besteht (oder ausschließlich aus ihnen besteht), die nicht im Teil 3 enthalten sind.

f. **Konform zum PP** - Ein EVG ist nur dann konform zu einem PP, wenn es mit allen Teilen des PP übereinstimmt.“

[8] deutsche Übersetzung

CC Teil 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	3
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Table 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.“

Evaluation assurance level 3 (EAL3) - methodically tested and checked **(chapter 6.2.3)**

„Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed **(chapter 6.2.4)**

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

„Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives
Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.“

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.“

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.“
„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“