Bundesamt für Sicherheit in der Informationstechnik

BSI-PP-0025-2006

zu

Schutzprofil
für USB-Datenträger, Version 1.4

entwickelt von der

Fachhochschule Bonn-Rhein-Sieg

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon +49 (0)3018 9582-0, Infoline +49 (0)3018 9582-111, Telefax +49 (0)3018 9582-455

BSI-Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 (0)3018 9582-0, Infoline +49 (0)3018 9582-111, Telefax +49 (0)3018 9582-455

Bundesamt für Sicherheit in der Informationstechnik

Zertifikat BSI-PP-0025-2006

Schutzprofil für USB-Datenträger, Version 1.4

Common Criteria Vereinbarung

entwickelt von der

Fachhochschule Bonn-Rhein-Sieg

Vertrauenswürdigkeitspaket: **EAL 2 augmented by ADV_SPM.1**

Bonn, den 19. April 2006

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Dr. Helmbrecht L.S.

Das oben genannte Schutzprofil wurde von einer akkreditierten und lizenzierten Prüfstelle 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, ergänzt um Final Interpretations in Übereinstimmung mit Common Criteria Version 2.2 und Common Methodology Part 2, Version 2.2 evaluiert.

Dieses Zertifikat gilt nur für die angegebene Version des Schutzprofils 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 stehen in Einklang mit den erbrachten Nachweisen.

Mit diesem Zertifikat ist weder eine generelle Empfehlung des Schutzprofils noch eine Garantie des Bundesamtes für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluß hatte, verbunden.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon +49 (0)3018 9582-0, Infoline +49 (0)3018 9582-111, Telefax +49 (0)3018 9582-455

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] neben der Zertifizierung von Sicherheitsprodukten der Informationstechnik auch die Aufgabe, Schutzprofile (PP)[2] für solche Produkte zu zertifizieren.

Ein Schutzprofil definiert eine implementierungsunabhängige Menge von IT-Sicherheitsanforderungen an eine Kategorie von Produkten (Systeme oder Komponenten). Anwender können durch Erstellung und Zertifizierung eines Schutzprofils oder Verweis auf ein solches ihre IT-Sicherheitsbedürfnisse ausdrücken, ohne Bezug auf ein konkretes Produkt zu nehmen. Schutzprofile können als Grundlage für eine Produktzertifizierung herangezogen werden. Produkte, die eine solche Zertifizierung durchlaufen haben, erhalten ein eigenes Zertifikat.

Die Zertifizierung eines Schutzprofils wird auf Veranlassung des Schutzprofil-Entwicklers - im folgenden Antragsteller genannt - durchgeführt. Entwickler eines Schutzprofils können IT-Hersteller, aber auch IT-Anwender sein.

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

Die Evaluierung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder von der Prüfstelle des 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 Schutzprofils, 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

[2] Protection Profile

Gliederung

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

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

- BSIG[3]
- BSI-Zertifizierungsverordnung[4]
- BSI-Kostenverordnung[5]
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN 45011
- BSI-Zertifizierung: Verfahrensbeschreibung [BSI 7125]
- Verfahren der Erteilung eines PP-Zertifikats durch das BSI
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik [CC], Version 2.1[6] (ISO/IEC 15408)
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik [CEM]
  - Teil 1, Version 0.6
  - Teil 2, Version 1.0
- BSI Zertifikate: Anwendungshinweise und Interpretationen zum Schema [AIS]

Die Verwendung der CC Version 2.1, der CEM Teil 2 Version 1 und der Final Interpretations als Teil der AIS 32 ergibt eine Übereinstimmung des Zertifizierungsergebnisses mit CC Version 2.2 und CEM Version 2.2 wie durch die Gremien im CC Anerkennungsabkommen festgelegt.

---

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

[4] 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

[5] Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Kostenverordnung-BSI-KostV) vom 3. März 2005, Bundesgesetzblatt I S. 519

[6] Bekanntmachung des Bundesministeriums des Innern vom 22. September 2000

2 Anerkennungsvereinbarungen

Um die Mehrfach-Entwicklung des gleichen Schutzprofils in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von Zertifikaten für Schutzprofile unter gewissen Bedingungen vereinbart.

Im Mai 2000 wurde eine 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. Israel trat im November 2000 der Vereinbarung bei, Schweden im Februar 2002, Österreich im November 2002, Ungarn und Türkei im September 2003 und Japan im November 2003, die Tschechische Republik im September 2004, die Republik Singapore im März 2005, Indien im April 2005.

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 Schutzprofil für USB-Datenträger, Version 1.4 [PP] hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Schutzprofils für USB-Datenträger, Version 1.4 wurde von der media transfer AG durchgeführt. Das Prüflabor der media transfer AG ist eine vom BSI anerkannte Prüfstelle (ITSEF)[7].

Antragsteller und Entwickler ist die Fachhochschule Bonn-Rhein-Sieg, Fachbereich Informatik.

Sponsor ist das Bundesamt für Sicherheit in der Informationstechnik.

Entwickelt wurde das Schutzprofil für USB-Datenträger, Version 1.4, von Thomas Gilles im Auftrag der Fachhochschule Bonn-Rhein-Sieg.

Die Entwicklung und Evaluierung des Schutzprofils wurde auf der Grundlage der CC Version 2.1 (ISO/IEC 15408), sowie der AIS durchgeführt.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 19.04.2006 vom BSI abgeschlossen.

[7] Information Technology Security Evaluation Facility

4 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-8.

Das Schutzprofil für USB-Datenträger, Version 1.4 ist in die BSI-Liste der zertifizierten Schutzprofile, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: http://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline +49 (0)3018 9582 111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Entwickler[8] des Schutzprofils angefordert werden. Unter der o. g. Internet-adresse kann der Zertifizierungsreport auch in elektronischer Form beim BSI abgerufen werden.

[8] Fachhochschule Bonn-Rhein-Sieg
Fachbereich Informatik
53757 Sankt Augustin

B Zertifizierungsbericht

Gliederung des Zertifizierungsberichtes

1 PP-Übersicht

Dieses Schutzprofil betrachtet alle Massenspeicher, die an die USB-Schnittstelle angeschlossen werden können. Diese Geräte werden als USB-Datenträger bezeichnet.

Geht ein USB-Datenträger verloren, wird verlegt oder entwendet, so darf daraus nicht resultieren, dass die vertraulichen Daten im Speicher an unberechtigte Personen fallen. Des Weiteren darf es unberechtigten Personen nicht möglich sein, vertrauliche Daten auf dem Datenträger zu löschen oder zu manipulieren. Dazu definiert dieses Schutzprofil einen Basissatz an Sicherheitsanforderungen zur Wahrung der Vertraulichkeit der Daten selbst bei logischen und physischen gezielten Angriffen. Auch die Wahrung der Integrität der Daten im Falle einer Störung wird in den Anforderungen definiert.

Ein wesentlicher Aspekt der anwenderfreundlichen IT-Sicherheit des USB-Datenträgers ist die vollständige Implementierung der Sicherheitsfunktionen im Datenträger selbst. Dadurch wird die Nutzung des PP-konformen USB-Datenträgers an vielen Wirtssystemen möglich, da an diese keine SW-Anforderungen gestellt werden.

Eine einmalige Authentisierung reicht aus, um eine Verbindung zu den vertraulichen Daten zu etablieren. Nach der Authentisierung erbringt der Datenträger seine Sicherheitsleistung transparent.

Das Schutzprofil geht nur soweit auf HW-Annahmen ein, wie diese zwingend notwendig sind. Dies ermöglicht ein breites Spektrum an technischen Lösungen.

Es bleibt dem Hersteller überlassen, Produkte die zu diesem Schutzprofil konform sind, um zusätzliche Sicherheitsfunktionen zur Erhöhung der Sicherheitsleistung zu erweitern. Einige Hinweise dazu werden in Form von Anwendungsbemerkungen im PP vorgestellt. Die Erweiterungen können in den Sicherheitsvorgaben (Security Target – ST) spezifiziert werden, welche die Basis für eine Zertifizierung eines konkreten Produktes darstellen.

2 Funktionale Sicherheitsanforderungen

Dieses Kapitel enthält die funktionalen Anforderungen, die ein EVG erfüllen muss, um konform zum Schutzprofil für USB-Datenträger, Version 1.4 zu sein.

Die folgenden funktionalen Sicherheitsanforderungen aus Teil 2 der CC werden im vorliegenden Schutzprofil verwendet:

Komponente	**Name der Komponente**
FCS_CKM.1	Kryptografische Schlüsselgenerierung
FCS_CKM.4	Zerstörung des kryptografischen Schlüssels
FCS_COP.1	Kryptografischer Betrieb
FDP_ACC.1	Teilweise Zugriffskontrolle
FDP_ACF.1	Zugriffskontrolle basierend auf Sicherheitsattributen
FIA_SOS.1	Verifizierung von Geheimnissen
FIA_UAU.1	Zeitpunkt der Authentisierung
FIA_UAU.6	Wiederauthentisierung
FMT_MSA.1	Management der Sicherheitsattribute
FMT_SMF.1	Spezifikation der Management Funktionen
FMT_SMR.1	Sicherheitsrollen
FPT_FLS.1	Erhaltung des sicheren Zustandes bei Fehlern
FPT_RCV.4	Funktionelle Wiederherstellung

Tabelle 1: funktionale Sicherheitsanforderungen

3 Vertrauenswürdigkeitspaket

Die Anforderungen an die Vertrauenswürdigkeit, welche vom TOE (EVG) erfüllt werden müssen, sind in nachfolgender Tabelle aufgeführt. Sie entsprechen der Vertrauenswürdigkeitsstufe EAL 2 aus Teil 3 der Common Criteria ergänzt um die Komponente ADV_SPM.1.

Komponente	Name der Komponente
ACM_CAP.2	Konfigurationsteile
ADO_DEL.1	Auslieferungsprozeduren
ADO_IGS.1	Installations-, Generierungs- und Anlaufprozeduren
ADV_FSP.1	Informelle funktionale Spezifikation
ADV_HLD.1	Beschreibender Entwurf auf hoher Ebene
ADV_RCR.1	Informeller Nachweis der Übereinstimmung
ADV_SPM.1	Sicherheitsmodell
AGD_ADM.1	Systemverwalterhandbuch
AGD_USR.1	Bernutzerhandbuch
ATE_COV.1	Nachweis der Testabdeckung
ATE_FUN.1	Funktionales Testen
ATE_IND.2	Unabhängiges Testen
AVA_SOF.1	Stärke der EVG-Sicherheitsfunktionen
AVA_VLA.1	Schwachstellenanalyse des Entwicklers

Tabelle 2: Vertrauenswürdigkeitskomponenten

4 Geforderte Stärke der Funktionen

Die geforderte Stärke der Sicherheitsfunktionen für dieses Schutzprofil die auf dem Authentisierungsmechanismus beruhen ist:

SoF-mittel

5 Ergebnis der Evaluierung

Der Evaluation Technical Report [ETR] wurde von der Prüfstelle gemäß den Common Criteria [CC], der Methodologie [CEM], den Anforderungen des Schemas [7125] und allen Interpretationen des Schemas [AIS] erstellt, die für den EVG relevant sind.

Das Schutzprofil für USB-Datenträger erfüllt die Anforderungen an Schutzprofile, die in den CC in der Klasse APE festgelegt sind.

Die folgende Tabelle zeigt die Ergebnisse der Evaluierung der Klasse APE:

CC Aspekt	Ergebnis
CC Class APE	PASS
APE_DES.1	PASS
APE_ENV.1	PASS
APE_INT.1	PASS
APE_OBJ.1	PASS
APE_REQ.1	PASS
APE_SRE.1	PASS

Tabelle 3: Ergebnisse der Evaluierung

6 Definitionen

6.1 Abkürzungen

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

EAL Evaluation Assurance Level – Vertrauenswürdigkeitsstufe

EVG Evaluationsgegenstand

HW Hardware

IT Informationstechnik

PP Protection Profile - Schutzprofil

SF Sicherheitsfunktion

SOF Strength of Function - Stärke der Funktionen

ST Security Target – Sicherheitsvorgaben

SW Software

TOE Tarfet Of Evaluation

TSC TSF Scope of Control - Anwendungsbereich der TSF-Kontrolle

TSF TOE Security Functions - EVG-Sicherheitsfunktionen

TSP TOE security policy - EVG-Sicherheitspolitik

USB Universal Serial Bus

6.2 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 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.

7 Literaturangaben

[AIS] Anwendungshinweise und Interpretationen zum Schema (AIS), soweit für den EVG relevant

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

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

[7125] BSI-Zertifizierung: Verfahrensbeschreibung

[7148] BSI-Liste zertifizierter Produkte

[PP] Schutzprofil für USB-Datenträger, Version 1.4, 27. März 2006

[ETR] Evaluation Technical Report, Version 1.1, 29. März 2006

Anhang: Schutzprofil

Das Schutzprofil für USB-Datenträger, Version 1.4 [PP] wird als separates Dokument zur Verfügung gestellt.