Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-CC-PP-0037-2008

zu

Common Criteria Schutzprofil
für
Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0

entwickelt durch

Gesellschaft für Informatik e. V.

im Auftrag von

Bundesamt für Sicherheit in der Informationstechnik

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-CC-PP-0037-2008

**Common Criteria Schutzprofil
für Basissatz von Sicherheitsanforderungen
an Online-Wahlprodukte, Version 1.0**

entwickelt durch Gesellschaft für Informatik e. V.

im Auftrag des Bundesamt für Sicherheit in der Informationstechnik

Vertrauenswürdigkeitspaket des Schutzprofiles:
Common Criteria Teil 3 konform
EAL 2 mit Zusatz von
ALC_CMC.3 (substituting ALC_CMC.2)
ALC_CMS.3 (substituting ALC_CMS.2)
ALC_DVS.1
ALC_LCD.1

Common Criteria Arrangement

Common Criteria

Das Schutzprofil wurde von einer akkreditierten und lizenzierten Prüfstelle unter Nutzung der Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1 in Übereinstimmung mit den Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (CC) 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 einer anderen Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, verbunden.

Bonn, 21. Mai 2008

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Irmela Ruhrmann L.S.
Fachbereichsleiterin

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Dies ist eine eingefügte Leerseite.

Vorbemerkungen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] neben der Zertifizierung von Sicherheitsprodukten für die Informationstechnik auch die Aufgabe, Schutzprofile 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 geschieht auf Veranlassung des BSI oder eines Antragstellers. Antragsteller können IT-Hersteller oder IT-Anwender sein.

Bestandteil des Verfahrens ist die Evaluierung (Prüfung und Bewertung) des Schutzprofils gemäß den Common Criteria [1].

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.

[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 3.1[5]
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 3.1
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)
- Verfahren der Erteilung eines Schutzprofil-Zertifikats durch das BSI.

2 Anerkennungsvereinbarungen

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

2.1 Internationale Anerkennung von CC - Zertifikaten

Im Mai 2000 wurde eine Vereinbarung (Common Criteria-Vereinbarung) über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 verabschiedet (CC-MRA). Diese Vereinbarung schließt die Anerkennung von Schutzprofilen auf Basis der CC ein.

Der Vereinbarung sind bis Februar 2007 die nationalen Stellen folgender Nationen beigetreten: Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Republik Korea, Neuseeland,

---

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 3. März 2005, Bundesgesetzblatt I S. 519

5 Bekanntmachung des Bundesministeriums des Innern vom 10. Mai 2006 im Bundesanzeiger, datiert 19. Mai 2006, S. 19445

Niederlande, Norwegen, Österreich, Schweden, Spanien, Republik Singapur, Tschechische Republik, Türkei, Ungarn, USA. Eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen kann auf der Internetseite http://www.commoncriteriaportal.org eingesehen werden.

Das Logo der Common-Criteria-Vereinbarung auf dem Zertifikat zeigt, dass dieses Zertifikat unter die Anerkennungsvereinbarung fällt.

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 Common Criteria Schutzprofil für Basissatz von Sicherheits-anforderungen an Online-Wahlprodukte Version 1.0 hat das Zertifizierungsverfahren beim BSI durchlaufen. Die Evaluierung wurde am 28. April 2008 beendet.

Die Evaluierung des Schutzprofil Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte Version 1.0 wurde von SRC Security Research & consulting GmbH durchgeführt. Das Prüflabor SRC Security Research & consulting GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Der Antragsteller für diese Zertifizierung ist: Gesellschaft für Informatik e.V.

Der Auftraggeber ist: Bundesamt für Sicherheit in der Informationstechnik

Den Abschluss der Zertifizierung bilden die Vergleichbarkeitsprüfung und die Erstellung des vorliegenden Zertifizierungsreports durch das BSI.

4 Gültigkeit des Zertifikats

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Schutzprofils.

Die Gültigkeit kann auf neue Versionen des Schutzprofils erweitert werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d. h. eine Re-Zertifizierung oder ein Maintenance Verfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

Die Bedeutung der Vertrauenswürdigkeitsstufen und die Stärke der Funktionen werden in den Auszügen aus dem technischen Regelwerk am Ende des Zertifizierungsreports erläutert.

5 Veröffentlichung

Das Schutzprofil Common Criteria Schutzprofil für Basissatz von Sicherheits-anforderungen an Online-WahlprodukteVersion 1.0 ist in die BSI-Liste der zertifizierten Schutzprofile aufgenommen worden, die regelmäßig veröffentlicht wird (siehe auch Internet: http://www.bsi.bund.de und [3]). Nähere Informationen sind über die BSI-Infoline +49 (0)228/9582-111 zu erhalten.

---

6 Information Technology Security Evaluation Facility

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Auftraggeber[7] des Schutzprofil angefordert werden. Unter der o. g. Internetadresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

[7] Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53133 Bonn

Dies ist eine eingefügte Leerseite.

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- dem zur Zertifizierung vorgelegten Schutzprofil,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

1 Schutzprofil Übersicht

Das Schutzprofil Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte wurde im Auftrag des Bundesamt für Sicherheit in der Informationstechnik zusammen mit der Gesellschaft für Informatik e.V. erstellt und dient als Grundlage für die Entwicklung von Security Targets zur Zertifizierung von IT-Produkten.

Es definiert einen Basissatz von Sicherheitsanforderungen, den jedes Online-Wahlprodukt zumindest erfüllen muß, um einige Arten von Vereinswahlen, Gremienwahlen, etwa in den Hochschulen, im Bildungs- und Forschungsbereich, und insbesondere nicht-politische Wahlen mit geringem Angriffspotential sicher auszuführen.

Das betrachtete Online-Wahlprodukt ist in ein Phasenmodell für den Ablauf einer Wahl eingebettet. Eine Wahl besteht aus drei Phasen: Wahlvorbereitung, Wahldurchführung inkl. Stimmauszählung und Archivierung. Die Anforderungen beziehen sich nur auf die Phase Wahldurchführung inkl. der Stimmauszählung, nicht aber auf die Wahlvorbereitung (wie beispielsweise die Erstellung der Wahlberechtigungsliste) und die Archivierung der Wahldurchführungs- und Ergebnisdaten. Anforderungen an den Übergang zu den angrenzenden Phasen werden in Sicherheitszielen für die Umgebung zum Ausdruck gebracht.

Die Stimmabgabe ist die zentrale Funktion während der Wahldurchführung. Sie erfolgt aus der Ferne, über ein offenes Netzwerk und von einem Endgerät, das in der Lage ist, den gesamten Inhalt des Stimmzettels darzustellen und die Vorgaben des Wahlveranstalters für die Art der Darstellung, insb. die Reihenfolge der Wahlvorschläge, umzusetzen. Die abgegebenen Stimmen werden in der Urne auf dem Wahlserver gespeichert. Durch Stimmauszählung aller abgegebenen Stimmen wird nach Wahlende auf dem Wahlserver das Ergebnis ermittelt und festgestellt. Das betrachtete Online-Wahlprodukt ist ein verteiltes Produkt, das aus einem serverseitigen EVG und aus einem clientseitigen EVG besteht (vgl. [7], Kapitel 1.2.1). Der serverseitige EVG verwaltet die Wahlberechtigungsliste und die Urne. Am clientseitigen EVG führt der Wähler die Wahlhandlung aus, um seine Stimme abzugeben.

Die Werte, die von einem zum Schutzprofil konformen Produkt (TOE) zu schützen sind, werden im Schutzprofil [7], Kapitel 3 aufgeführt. Basierend auf diesen Werten wird die Sicherheitsumgebung durch Annahmen, Bedrohungen und Organisatorische Sicherheitspolitiken definiert. Dies ist im Schutzprofil [7], Kapitel 3.1 – 3.3, dargestellt.

Diese Annahmen, Bedrohungen und Organisatorischen Sicherheitspolitiken werden auf Sicherheitsziele für einen TOE, der konform zum Schutzprofil ist, und auf Sicherheitsziele für die IT-Umgebung eines solchen TOE abgebildet. Diese Ziele werden im Schutzprofil [7], Kapitel 4 beschrieben.

Das Schutzprofil verlangt, dass eine auf ihm basierende produktbezogene Sicherheitsvorgabe den Konformitätsgrad „strict“ erfüllt.

2 Funktionale Sicherheitsanforderungen

Die Sicherheitsziele werden durch eine Menge von funktionalen Sicherheitsanforderungen (SFR) erfüllt. Diese müssen von einem zum Schutzprofil konformen Produkt (TOE) umgesetzt werden.

Das Schutzprofil definiert aktive Einheiten, die als Subjekte bezeichnet werden. Folgende Arten von Subjekten werden definiert:

- Wähler: Alle aktiven Einheiten im clientseitigen oder serverseitigen EVG, die die Aktionen der Wahlhandlung auslösen. Weil alle Aktionen von der Person, die die Wahlhandlung ausführt, verursacht werden, wird für Subjekt und Benutzer der gleiche Begriff verwendet.
- Wahlvorstand: Alle aktiven Einheiten im serverseitigen EVG, die die Aktionen für den Ablauf der Wahldurchführung inkl. Stimmauszählung auslösen. Weil alle Aktionen von der Person, die für den ordnungsgemäßen Ablauf der Wahldurchführung inkl. Stimmauszählung zuständig ist, verursacht werden, wird für Subjekt und Benutzer der gleiche Begriff verwendet.

Das Schutzprofil definiert passive Einheiten, die als Objekte bezeichnet werden. Objekte sind die Ziele von Operationen, die von Subjekten ausgeführt werden können. Sie sind Behälter, die Informationen enthalten. Innerhalb des EVG gibt es folgende Arten von Informationen:

- Authentisierungsnachrichten, Identifikationsdaten, Protokollaufzeichnungen, Rückmeldungen, Stimmabgabevermerke, Stimmdatensätze, Stimmen, Stimmzettel, Stimmzetteldaten, Wahldurchführungsdaten, Wahlende-Zeitpunkt, Wahlergebnis, Zwischenergebnis

Subjekte und Objekte besitzen bestimmte Sicherheitsattribute, die Informationen enthalten, welche ein korrektes Verhalten des EVG ermöglichen. Diese sind:

- Anzahl der Autorisierungen für die angeforderte Operation: Dieses Attribut wird zur Verweigerung kontrollierter Operation verwendet. Deren Ausführung wird verhindert, solange nicht genügend viele Mitglieder des Wahlvorstands für die Autorisierung der angeforderten Operation authentisiert wurden.
- Wahlzeitraum: Dieses Attribut wird zur Kontrolle des Ablaufs der Wahldurchführung inkl. Stimmauszählung verwendet. Es besitzt vor dem Starten der Wahldurchführung den Wert Vorbereitung, nach dem Starten der Wahldurchführung den Wert Durchführung und nach dem Beenden der Wahldurchführung den Wert Auszählung.
- Stimmberechtigungsattribut: Dieses Attribut wird zur Kontrolle der Stimmberechtigung des Wählers verwendet. Es spiegelt den Stimmabgabevermerk wieder. Seine möglichen Werte sind unbekannt, mit oder ohne Stimmberechtigung. Bei der Eröffnung jeder Wahlhandlung wird das Attribut auf den Wert unbekannt gesetzt. Wenn der Wähler erfolgreich identifiziert und authentisiert wurde, wird der Wert des Attributs auf den Wert mit oder den Wert ohne geändert, je nach Stimmabgabevermerk. Nach der erfolgreichen Stimmabgabe und entsprechendem Vermerk erhält das Attribut den Wert ohne.
- Wahlhandlungsattribut: Dieses Attribut wird zur Kontrolle des Fortschritts der Wahlhandlung verwendet. Es kann die Werte vor oder nach Einleitung der Stimmabgabe annehmen. Bei der Eröffnung jeder Wahlhandlung wird das Attribut auf den Wert vor gesetzt. Die Einleitung der Stimmabgabe ändert das Attribut auf den Wert nach. Wird die Einleitung der Stimmabgabe widerrufen, erhält das Attribut wieder den Wert vor.

Das Schutzprofil definiert funktionale Sicherheitsanforderungen in den Bereichen:

- Protokollierung (Generierung der Protokolldaten, Durchsicht der Protokollierung)

- Schutz der Benutzerdaten (Einfache Datenauthentisierung, Teilweise Informationsflusskontrolle (Wahlhandlung), Einfache Sicherheitsattribute (Wahlhandlung), Teilweise Informationsflusskontrolle (Wahldurchführung inkl. Stimmauszählung), Einfache Sicherheitsattribute (Wahldurchführung inkl. Stimmauszählung), Keine unerwünschten Informationsflüsse, Überwachung der Integrität der gespeicherten Daten und Reaktionen, Teilweiser Schutz bei erhalten gebliebenen Informationen (Stimmzettel), Teilweiser Schutz bei erhalten gebliebenen Informationen (Urne), Einfache Vertraulichkeit des Datenaustausches, Einfache Integrität des Datenaustausches)
- Identifikation und Authentisierung (Definition der Benutzerattribute, Zeitpunkt der Authentisierung (für Wähler), Benutzerauthentisierung vor jeglicher Aktion (für Wahlvorstand), Wiederauthentisierung (für Wahlvorstand), Zeitpunkt der Identifikation (für Wähler), Benutzeridentifikation vor jeglicher Aktion (für Wahlvorstand), Benutzer-Subjekt-Bindung (für Wähler), Benutzer-Subjekt-Bindung (für Wahlvorstand))
- Sicherheitsmanagement (Einschränkungen der Sicherheitsrollen)
- Schutz der privaten Daten (Anonymität, Unverkettbarkeit (Netzwerk), Unverkettbarkeit (Urne))
- Schutz der TSF (Manuelle Wiederherstellung, Funktionelle Wiederherstellung, TSF Testen)
- EVG-Zugriff (Durch TSF eingeleitete Beendigung, Durch Benutzer eingeleitete Beendigung, TOE-Sitzungseinrichtung)
- Vertrauenswürdiger Pfad/Kanal

Die funktionalen Sicherheitsanforderungen an einen TOE sind im Schutzprofil [2], Kapitel 5.1 enthalten. Sie sind alle den Common Criteria, Teil 2 entnommen. Das Schutzprofil ist daher bezüglich der funktionalen Sicherheitsanforderungen wie folgt gekennzeichnet:

Common Criteria Teil 2 konform

3 Anforderungen an die Vertrauenswürdigkeit

Das Paket von Vertrauenswürdigkeitskomponenten für ein Produkt das dieses Schutzprofil erfüllen soll ist komplett den Vertrauenswürdigkeitskomponenten aus Teil 3 der Common Criteria entnommen. Das Vertrauenswürdigkeitspaket lautet daher:

Common Criteria Teil 3 konform
EAL 2 mit Zusatz
von ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, ALC_LCD.1

(Zur Definition und dem Umfang von Vertrauenswürdigkeitspaketen gemäß den Common Criteria siehe Teil C dieses Reportes oder [1], Teil 3).

4 Ergebnis der Schutzprofil-Evaluation

Der Evaluierungsbericht (Evaluation Technical Report, ETR) [6] wurde von der Prüfstelle gemäß den Common Criteria [1], der Methodologie [2], den Anforderungen des Schemas [4] und allen Anwendungshinweisen und Interpretationen des Schemas (AIS) [5] erstellt.

Das Ergebnis der Evaluierung lautet “PASS” für die Vertrauenswürdigkeitskomponenten der Klasse APE.

Im Einzelnen wurden die folgenden Vertrauenswürdigkeitskomponenten bewertet:

APE_INT.1 - PP introduction
APE_CCL.1 - Conformance claim
APE_SPD.1 - Security problem definition
APE_OBJ.2 - Security objectives
APE_ECD.1 - Extended components definition
APE_REQ.2 - Derived security requirements

Die Ergebnisse der Evaluierung sind nur anwendbar für die Version des Schutzprofil, die im Kapitel 1 angegeben ist.

5 Auflagen und Hinweise für den Gebrauch

Die folgenden Auflagen und Hinweise beim Gebrauch des Schutzprofil sind zu beachten:

- Die Erfüllung der im Schutzprofil festgelegten Anforderungen reicht aus, um einige Arten von Vereinswahlen, Gremienwahlen, etwa in den Hochschulen, im Bildungs- und Forschungsbereich, und insbesondere nicht-politische Wahlen mit geringem Angriffspotential sicher auszuführen. Zur sicheren Durchführung von Online-Wahlen mit höherem Angriffspotential, wie etwa Betriebsratswahlen oder parlamentarische Wahlen, sind weitere Sicherheitsanforderungen zu formulieren und mit nachweisbaren Maßnahmen durchzusetzen, um die Annahmen über die Anwendungsumgebungen, wie sie hier beschrieben sind, zu erfüllen. Weitergehende Anforderungen zur Erfüllung der Annahmen über die Wahlumgebung mit höherem Angriffsrisiko können nahtlos auf den hier beschriebenen Kern der zentralen Anforderungen aufbauen und diesen ergänzen, keinesfalls ersetzen.
- Der Wortlaut der im Teil 2 der CC in englischer Sprache definierten funktionalen Anforderungen wurden in Abstimmung mit dem BSI ins Deutsche übersetzt. Bezogen auf die Konformität zu Teil 2 der CC gilt im Zweifelsfall die englische Originalfassung.
- Im Schutzprofil sind zahlreiche Anwendungshinweise enthalten, die der Autor einer produktspezifischen Sicherheitsvorgabe beachten soll.

6 Schutzprofil Dokument

Das Schutzprofil Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte [7] wird als separates Dokument im Teil D: Anhänge, Anhang A zu diesem Zertifizierungsbericht bereitgestellt.

7 Definitionen

7.1 Abkürzungen

BSI Bundesamt für Sicherheit in der Informationstechnik, Bonn

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

CCRA Common Criteria Recognition Arrangement

EAL Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

EVG Evaluationsgegenstand - TOE: Target of Evaluation

IT	Informationstechnik
ITSEF	Information Technology Security Evaluation Facility - Prüfstelle
PP	Protection Profile - Schutzprofil
SF	Sicherheitsfunktion
SFP	Security Function Policy - Funktionale Sicherheitspolitk
ST	Security Target - Sicherheitsvorgaben
TSF	TOE Security Functionality - EVG-Sicherheitsfunktionalität
TSP	TOE security policy **–** EVG-Sicherheitspolitik
TOE	Target of Evaluation

7.2 Glossar

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.

Evaluationsgegenstand – Eine Zusammenstellung aus Software, Firmware und/oder Hardware ergänzt um die dazugehörigen Handbücher.

EVG-Sicherheitsfunktionalität - Eine Zusammenstellung, die die gesamte Hardware, Software, und Firmware des EVG umfasst, auf die Verlass sein muss, um die funktionalen Sicherheitsanforderungen korrekt zu erfüllen.

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

Informell - Ausgedrückt in natürlicher Sprache.

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

Schutzprofil - Eine implementierungsunabhängige Darlegung eines Sicherheitsbedarfs für eine Kategorie von EVGs.

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

Sicherheitsvorgaben - Eine implementierungsabhängige Darlegung eines Sicherheitsbedarfs für einen spezifisch identifizierbaren EVG.

Subjekt - Eine aktive Einheit innerhalb des EVG, die Operationen auf Objekten ausführt.

Zusatz - Das Hinzufügen einer oder mehrerer Anforderungen zu einem Paket.

8 Literaturangaben

1 Common Criteria for Information Technology Security Evaluation, Version 3.1, Teil 1: Rev. 1, September 2006, Teil 2: Rev. 2, September 2007, Teil 3: Rev. 2, September 2007

2 Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev.1, September 2006

3 Deutsche IT-Sicherheitszertifikate (BSI 7148, BSI 7149), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird

4 BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)

5 Anwendungshinweise und Interpretationen zum Schema (AIS), die für das Schutzprofil relevant sind.

6 Evaluierungsbericht, Evaluation Technical Report für eine PP-Evaluierung, Version 1.1, 28.04.2008, SRC Security Research & Consulting GmbH, Zertifizierungs-ID: BSI-CC-PP-0037 (vertrauliches Dokument)

7 Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, BSI-CC-PP-0037, Version 1.0, 18. April 2008, Bundesamt für Sicherheit in der Informationstechnik

Dies ist eine eingefügte Leerseite.

C Auszüge aus den technischen Regelwerken

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 3.1 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part1:

Conformance claim (chapter 9.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformatnce claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assuarance components in CC Part 3

Additionally, the conformance claim may include a statement made with respect to packagees, in which case it consists of one the following:

- **Package name Conformant** - A PP or ST is conformant to a pre-defined (e.g. EAL) if:
  - the SFRs of the PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- **Package name Augmented** - A PP or ST is an augmentation of a predefined package if:
  - the SRFs of the PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package
  - the SARs of the PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SFR in the package.

  Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE cna therefore also be e.g. CC Part 2 conformant.

  Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- **PP Conformant** - A PP or ST meets specific PP(s), which are listed as part of the conformance result.

- **Conformance Statement** (only for Pps) – this statement describes the manner in which PPs or Sts must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex A“

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.”

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decompositon.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures

Assurance Class	Assurance Components
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 CC 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 8.1)

“Table 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 7 of this CC 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 standard 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VLA	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

D Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Das Schutzprofil Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte [7] wird in einem eigenen Dokument zur Verfügung gestellt.