# Zertifizierungsreport

**Bundesamt für Sicherheit in der Informationstechnik**

**BSI-PP-0031-2007**

zu

**Schutzprofil**
**Digitales Wahlstift-System, Version 1.0.1**

entwickelt im Auftrag der

**Freien und Hansestadt Hamburg**

**Bundesamt für Sicherheit in der Informationstechnik**

Godesberger Allee 185-189 - 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 9582-5477

**Bundesamt für Sicherheit in der Informationstechnik**

# Zertifikat BSI-PP-0031-2007

# Schutzprofil
# Digitales Wahlstift-System
# Version 1.0.1

entwickelt im Auftrag der

**Freien und Hansestadt Hamburg**

Vertrauenswürdigkeitspaket: EAL 3
mit Zusatz von ADV_SPM.1 und AVA_MSU.3

gültig bis 30.06.2008

Bonn, den 14.03.2007

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 2.3,* unter Nutzung der *Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik Version 2.3*, 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.

**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 9582-5477

# 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 2.3 (ISO/IEC 15408)
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- BSI Zertifikate: Anwendungshinweise und Interpretationen zum Schema (AIS)
- Informationen von der Zertifizierungsstelle zur Methodologie für Vertrauenswürdigkeitskomponenten oberhalb von EAL4 (AIS 34).

---

[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

# 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.

Da das Zertifikat eine begrenzte Gültigkeitsdauer hat, fällt es formal nicht unter diese Anerkennungsvereinbarung. Dennoch erfolgte der Evaluationsprozess für dieses Produkt nach den Regeln der Anerkennungsvereinbarungen.

# 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 „Digitales Wahlstift-System, Version 1.0.1“ hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Schutzprofils „Digitales Wahlstift-System, Version 1.0.1“ wurde von der TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit durchgeführt. Die TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit ist eine vom BSI anerkannte Prüfstelle (ITSEF)[6].

Entwickelt wurde das Schutzprofil „Digitales Wahlstift-System, Version 1.0.1“ im Auftrag der Freien und Hansestadt Hamburg durch das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) GmbH.

Die Entwicklung und Evaluierung des Schutzprofils wurde auf der Grundlage der CC Version 2.3 (ISO/IEC 15408), sowie der AIS durchgeführt.

Den Abschluß der Zertifizierung bilden

- die Vergleichbarkeitsprüfung und
- die Erstellung des vorliegenden Zertifizierungsreports.

Diese Arbeiten wurden am 14. März 2007 vom BSI abgeschlossen.

[6] Information Technology Security Evaluation Facility

# 4 Veröffentlichung

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

Das Schutzprofil „Digitales Wahlstift-System, Version 1.0.1“ ist 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 0228/9582-111 zu erhalten.

Unter der o.g. Internetadresse kann der Zertifizierungsreport auch in elektronischer Form abgerufen werden.

# B Zertifizierungsbericht

## Gliederung des Zertifizierungsberichtes

# 1 PP-Übersicht

Das Schutzprofil (Protection Profile – PP) „Digitales Wahlstift-System, Version 1.0.1“ bezieht sich auf die technische Wahlunterstützung im Wahllokal und zielt insbesondere auf politische Wahlen ab. Es umfasst die Mindestanforderungen an die IT-Sicherheit von technischen Systemen zur Wahlunterstützung, die auf der Verwendung eines Digitalen Wahlstiftes beruhen.

Ein zum PP konformer EVG ist ein Wahlgerät, das

- die Stimmabgabe mit Digitalen Wahlstiften,
- die Registrierung der Stimmen in einer zentralen elektronischen Urne im Wahllokal,
- die Bewertung und Auszählung der in der Urne gespeicherten Stimmen,
- die Feststellung und den Ausdruck des Ergebnisses und
- die Protokollierung sicherheitsrelevanter Ereignisse

ermöglicht.

Ein zum PP konformer EVG besteht aus

- den Digitalen Wahlstiften und zugehörigen Dockingstationen (es werden mindestens drei Stationen benötigt),
- ihrer Firmware zur Aufzeichnung der Stimmen,
- Dateien/Datenbanken zur Speicherung der Stimmen (elektronische Urne) und
- Software zur Kontrolle der Abläufe der Wahlhandlung, Bewertung, Auszählung und Feststellung.

Ein Digitaler Wahlstift wird in Verbindung mit speziell gerasterten Papierstimmzetteln dazu benutzt, handschriftliche Kennzeichnungen zu erfassen, zu speichern und auf einen Computer zu übertragen. Dazu sind im Digitalen Wahlstift eine Kugelschreibermine, eine Kamera (elektronisches Auge), ein Prozessor, ein Datenspeicher, eine Kommunikationseinheit und eine Batterie integriert. Die Kamera erfasst während des Schreibens das Punktraster auf dem Stimmzettel. Diese Daten werden im Digitalen Wahlstift gespeichert und über die Kommunikationseinheit in einer Dockingstation auf einen Computer übertragen. Die Funktionen des Digitalen Wahlstifts werden von einer darin befindlichen Firmware gesteuert.

Eine Verkabelung im Wahllokal ist erforderlich, um die Stimmen vom Stift in die elektronische Urne zu transportieren, um am Ende das Ergebnis zum Drucker schicken zu können und um die Wahldaten auf einen transportablen Datenspeicher zu übertragen. Es besteht darüber hinaus keine Möglichkeit, eine externe Verbindung zum EVG oder seiner IT-Umgebung aufzunehmen (insbesondere keine drahtlose Verbindung).

# 2 Funktionale Sicherheitsanforderungen

Die folgenden funktionalen Sicherheitsanforderungen aus Teil 2 der CC werden im vorliegenden Schutzprofil für den EVG definiert:

| Funktionale Sicherheits-anforderungen | Bedeutung |
|---|---|
| **FAU** | **Sicherheitsprotokollierung** |
| FAU_GEN.1 | Generierung der Protokolldaten |
| **FCS** | **Kryptographische Unterstützung** |
| FCO_NRO.2 | Erzwungener Urheberschaftsbeweis |
| **FDP** | **Schutz der Benutzerdaten** |
| FDP_ACC.2 | Vollständige Zugriffskontrolle |
| FDP_ACF.1 | Zugriffskontrolle basierend auf Sicherheitsattributen |
| FDP_IFC.2 | Vollständige Informationsflußkontrolle |
| FDP_IFF.1 | Einfach Sicherheitsattribute |
| FDP_ITT.2 | Übertragungsseparierung durch Attribute |
| FDP_ITT.4 | Attributbasierende Überwachung der Integrität |
| FDP_RIP.1 | Teilweiser Schutz bei erhalten gebliebenen Informationen |
| FDP_SDI.2 | Überwachung der Integrität der gespeicherten Daten und Reaktionen |
| **FMT** | **Sicherheitsmanagement** |
| FMT_MSA.3 | Initialisierung statischer Attribute |
| FMT_SMF.1 | Spezifikation der Managementfunktionen |
| **FPR** | **Privatheit** |
| FPR_ANO.2 | Anonymität ohne Verlangen nach Informationen |
| FPR_UNL.1 | Unverkettbarkeit |
| **FPT** | **Schutz der TSF** |
| FPT_AMT.1 | Test der abstrakten Maschine |
| FPT_FLS.1 | Erhaltung des sicheren Zustandes bei Fehlern |
| FPT_PHP.1. | Passive Erkennung materieller Angriffe |
| FPT_PHP.3 | Widerstand gegen materielle Angriffe |
| FPT_RCV.1 | Manuelle Wiederherstellung |
| FPT_RCV.4. | Funktionelle Wiederherstellung |
| FPT_TST.1 | TSF testen |
| **FRU** | **Betriebsmittelnutzung** |
| FRU_FLT.1 | Verminderte Fehlertoleranz |

Tabelle 1: SFRs für den EVG

Folgende funktionale Sicherheitsanforderungen aus Teil 2 der CC werden im vorliegenden Schutzprofil für die IT-Umgebung des EVGs definiert:

| Funktionale Sicherheits-anforderungen | Bedeutung |
|---|---|
| **FAU** | **Sicherheitsprotokollierung** |
| FAU_SAR.1 | Durchsicht der Protokollierung |
| FAU_STG.1 | Geschützte Speicherung des Protokolls |
| **FDP** | **Schutz der Benutzerdaten** |
| FDP_ACC.1 | Teilweise Zugriffskontrolle |
| FDP_ACF.1 | Zugriffskontrolle basierend auf Sicherheitsattributen |
| **FIA** | **Identifikation und Authentisierung** |
| FIA_ATD.1 | Definition der Benutzerattribute |
| FIA_UAU.2 | Benutzerauthentisierung vor jeglicher Aktion |
| FIA_UAU.7 | Geschützte Authentisierungsrückmeldung |
| FIA_UID.2 | Benutzeridentifikation vor jeglicher Aktion |
| FIA_USB.1 | Benutzer-Subjekt-Bindung |
| **FMT** | **Sicherheitsmanagement** |
| FMT_MSA.1 | Management der Sicherheitsattribute |
| FMT_MSA.3 | Initialisierung statischer Attribute |
| FMT_SMF.1 | Spezifikation der Managementfunktionen |
| FMT_SMR.1 | Sicherheitsrollen |
| **FPT** | **Schutz der TSF** |
| FPT_STM.1 | Verlässliche Zeitstempel |

Tabelle 2: SFRs für die IT-Umgebung des EVGs

Hinweis: Es werden nur die Titel der SFRs genannt. Detailiertere Informationen befinden sich in Kapitel 5.1 und 5.2 des Schutzprofils [7].

# 3 Vertrauenswürdigkeitspaket

Die Anforderungen an die Vertrauenswürdigkeit, welche vom EVG erfüllt werden müssen, sind in nachfolgender Tabelle aufgeführt. Sie entsprechen der Vertrauenswürdigkeitsstufe EAL3 mit Zusatz von ADV_SPM.1 und AVA_MSU.3 und der Klasse ASE für die Sicherheitsvorgaben aus Teil 3 der CC.

| Vertrauenswürdigkeits-klassen und -komponenten | Bedeutung |
|---|---|
| **ASE** | **Security Target Evaluierung** |
| ASE_DES.1 | EVG-Beschreibung |
| ASE_ENV.1 | Sicherheitsumgebung |
| ASE_INT.1 | ST-Einführung |
| ASE_OBJ.1 | Sicherheitsziele |
| ASE_PPC.1 | PP-Postulate |
| ASE_REQ.1 | IT-Sicherheitsanforderungen |
| ASE_SRE.1 | Explizit dargelegte IT-Sicherheitsanforderungen |
| ASE_TSS.1 | EVG-Übersichtsspezifikation |
| **ACM** | **Konfigurationsmanagement** |
| ACM_CAP.3 | Aututorisierungskontrolle |
| ACM_SCP.1 | EVG-CM-Umfang |
| **ADO** | **Auslieferung und Betrieb** |
| ADO_DEL.1 | Auslieferungsprozeduren |
| ADO_IGS.1 | Installations-, Generierungs- und Anlaufprozeduren |
| **ADV** | **Entwicklung** |
| ADV_FSP.1 | Informelle funktionale Spezifikation |
| ADV_HLD.2 | Sicherheitsspezifischer Entwurf auf hoher Ebene |
| ADV_RCR.1 | Informeller Nachweis der Übereinstimmung |
| ADV_SPM.1 | Informelles EVG-Sicherheitsmodell |
| **AGD** | **Handbücher** |
| AGD_ADM.1 | Systemverwalterhandbuch |
| AGD_USR.1 | Benutzerhandbuch |
| **ALC** | **Lebenszyklusunterstützung** |
| ALC_DVS.1 | Identifikation der Sicherheitsmaßnahmen |
| **ATE** | **Testen** |
| ATE_COV.2 | Analyse der Testabdeckung |
| ATE_DPT.1 | Testen – Entwurf auf hoher Ebene |
| ATE_FUN.1 | Funktionales Testen |
| ATE_IND.2 | Unabhängiges Testen – Stichprobenartig |

| AVA | Schwachstellenbewertung |
|---|---|
| AVA_MSU.3 | Analysieren und Testen auf unsichere Zustände |
| AVA_SOF.1 | Stärke der EVG-Sicherheitsfunktionen |
| AVA_VLA.1 | Schwachstellenanalyse des Entwicklers |

Tabelle 3: Vertrauenswürdigkeitskomponenten (ASE und EAL 3+)

# 4 Geforderte Stärke der Funktionen

Die geforderte Stärke der Sicherheitsfunktionen für dieses Schutzprofil ist:

**SoF-mittel**

# 5 Ergebnis der Evaluierung

Der Evaluierungsendbericht [6] wurde von der Prüfstelle gemäß den Common Criteria [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen Interpretationen des Schemas [4] erstellt, die für den EVG relevant sind. Der Evaluierungsbericht referenziert das Schutzprofil in der Version 1.0. Die zertifizierte Version 1.0.1 des Schutzprofils wurde im Vergleich dazu nur geringfügig editoriell geändert, sodass der ETR auch für die zertifizierte Version gültig ist.

Das Schutzprofil „Digitales Wahlstift-System, Version 1.0.1“ 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:

| Vertrauenswürdigkeits-klassen und -komponenten | Bedeutung | Urteil |
|---|---|---|
| **APE** | **Schutzprofil-Evaluierung** | **Erfüllt** |
| APE_DES.1 | EVG-Beschreibung | Erfüllt |
| APE_ENV.1 | Sicherheitsumgebung | Erfüllt |
| APE_INT.1 | PP-Einführung | Erfüllt |
| APE_OBJ.1 | Sicherheitsziele | Erfüllt |
| APE_PPC.1 | PP-Postulate | Erfüllt |
| APE_REQ.1 | IT-Sicherheitsanforderungen | Erfüllt |
| APE_SRE.1 | Explizit dargelegte IT-Sicherheitsanforderungen | Erfüllt |

Tabelle 4: Vertrauenswürdigkeitskomponenten der Klasse APE

Die Evaluierung hat gezeigt, dass:

- die funktionalen Sicherheitsanforderungen für den EVG aus dem Schutzprofil konform zu Teil 2 der Common Criteria sind.

# 6 Definitionen

## 6.1 Abkürzungen

**BSI** Bundesamt für Sicherheit in der Informationstechnik, Bonn

**CC** Common Criteria - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

**EAL** Evaluation Assurance Level - Vertrauenswürdigkeitsstufe

**EVG** Evaluationsgegenstand

**IT** Informationstechnik

**PP** Protection Profile - Schutzprofil

**SF** Sicherheitsfunktion

**SFR** Security Functional Requirement - Funktionale Sicherheitsanforderung

**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

## 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

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Version 2.3, August 2005

[3] BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)

[4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind

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

[6] Evaluierungsendbericht, Version 2, 30.11.2006, „Technischer Evaluierungsbericht (ETR), BSI-PP-0031, Digitales Wahlstift-System“, TÜV Informationstechnik GmbH, Prüfstelle für IT-Sicherheit

[7] Schutzprofil BSI-PP-0031-2007, Schutzprofil „Digitales Wahlstift-System, Version 1.0.1“, 28.02.2007

Dies ist eine eingefügte Leerseite.

# Anhang: Schutzprofil

Das Schutzprofil „Digitales Wahlstift-System, Version 1.0.1“ wird als separates Dokument zur Verfügung gestellt.

Dies ist eine eingefügte Leerseite.