

BSI-DSZ-CC-0444-2008

ZU

**Digitales Wahlstiftsystem
dotVote® Version 1.0**

der

**Diagramm Halbach GmbH & Co. KG und WRS-
Softwareentwicklung GmbH**

im Auftrag von

**Freie und Hansestadt Hamburg
Behörde für Inneres
Amt für Innere Verwaltung und Planung**

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



Deutsches

erteilt vom



IT-Sicherheitszertifikat

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0444-2008

Digitales Wahlstiftsystem

Digitales Wahlstiftsystem dotVote® Version 1.0

von Diagramm Halbach GmbH & Co. KG und
WRS-Softwareentwicklung GmbH

im Auftrag von Freie und Hansestadt Hamburg
Behörde für Inneres
Amt für Innere Verwaltung und Planung

PP-Konformität: Schutzprofil Digitales Wahlstift-System, Version 1.0.1,
BSI-PP-0031-2007

Funktionalität: PP konform plus produktspezifische Ergänzungen
Common Criteria Teil 2 konform

Vertrauenswürdigkeit: Common Criteria Teil 3 konform
EAL 3 mit Zusatz von
ADV_SPM.1 und AVA_MSU.3

gültig bis 30.06.2008

Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle nach der Gemeinsamen Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3 unter Nutzung der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.3 (CC) (ISO/IEC 15408:2005) evaluiert.

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.

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.

Bonn, 11. Juni 2008

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag



Irmela Ruhrmann
Fachbereichsleiterin

L.S.

Dies ist eine eingefügte Leerseite.

Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG¹ 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.....	7
1	Grundlagen des Zertifizierungsverfahrens.....	7
2	Anerkennungsvereinbarungen.....	7
3	Durchführung der Evaluierung und Zertifizierung.....	8
4	Gültigkeit des Zertifikats.....	8
5	Veröffentlichung.....	9
B	Zertifizierungsbericht.....	10
1	Zusammenfassung.....	11
2	Identifikation des EVG.....	13
3	Sicherheitspolitik.....	13
4	Annahmen und Klärung des Einsatzbereiches.....	14
5	Informationen zur Architektur.....	14
6	Dokumentation.....	15
7	Testverfahren.....	15
7.1	Funktionale Tests des Herstellers.....	15
7.2	Unabhängige Tests der Prüfstelle	15
8	Evaluierte Konfiguration.....	16
9	Ergebnis der Evaluierung.....	16
9.1	CC spezifische Ergebnisse.....	16
9.2	Ergebnis der kryptographischen Bewertung.....	17
10	Auflagen und Hinweise zur Benutzung des EVG.....	17
11	Sicherheitsvorgaben.....	17
12	Definitionen.....	18
12.1	Abkürzungen.....	18
12.2	Glossary.....	18
13	Literaturangaben.....	20
C	Auszüge aus den Kriterien.....	22
D	Anhänge.....	30

A Zertifizierung

1 Grundlagen des Zertifizierungsverfahrens

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

- BSIG²
- BSI-Zertifizierungsverordnung³
- BSI-Kostenverordnung⁴
- besondere Erlasse des Bundesministeriums des Innern
- die Norm DIN EN 45011
- BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125) [3]
- Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CC), Version 2.3⁵
- Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Version 2.3
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS)
- Hinweise der Zertifizierungsstelle zur Methodologie für Vertrauenswürdigkeitskomponenten oberhalb von EAL 4 (AIS 34)

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.

Aufgrund der befristeten Gültigkeit des Zertifikats für das zugrundeliegende Schutzprofil wird die Gültigkeit dieses Zertifikats ebenfalls bis 30. Juni 2008 befristet.

Daher fällt dieses Zertifikat formal nicht unter diese Anerkennungsvereinbarung. Dennoch erfolgte der Evaluationsprozess für dieses Produkt nach den Regeln der Anerkennungsvereinbarungen.

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

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 Digitales Wahlstiftsystem dotVote® Version 1.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts Digitales Wahlstiftsystem dotVote® Version 1.0 wurde von datenschutz nord GmbH durchgeführt. Die Evaluierung wurde am 30. Mai 2008 beendet. Das Prüflabor datenschutz nord GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)⁶.

Der Antragsteller ist: Diagramm Halbach GmbH & Co. KG und WRS-Softwareentwicklung GmbH.

Der Sponsor ist: Freie und Hansestadt Hamburg Behörde für Inneres Amt für Innere Verwaltung und Planung.

Das Produkt wurde entwickelt von: Diagramm Halbach GmbH & Co. KG und WRS-Softwareentwicklung GmbH.

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

4 Gültigkeit des Zertifikats

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

Das Produkt ist nur unter den folgenden Bedingungen konform zu den bestätigten Vertrauenswürdigkeitskomponenten:

- alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des EVG, die in diesem Report gestellt werden, werden beachtet.
- das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben beschrieben ist.

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

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Die Zertifizierungsstelle empfiehlt, regelmäßig eine Einschätzung der Widerstandsfähigkeit vornehmen zu lassen.

Aufgrund der befristeten Gültigkeit des Zertifikats für das zugrundeliegende Schutzprofil wird die Gültigkeit dieses Zertifikats ebenfalls bis 30. Juni 2008 befristet.

⁶ Information Technology Security Evaluation Facility

5 Veröffentlichung

Das Produkt Digitales Wahlstiftsystem dotVote® Version 1.0 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: <http://www.bsi.bund.de> und [5]). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können bei den Herstellern des Produktes angefordert werden⁷. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

⁷ Diagramm Halbach GmbH & Co. KG
Am Winkelstück 14
58239 Schwerte

WRS-Softwareentwicklung GmbH
Schillerstr. 2
59065 Hamm

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.

1 Zusammenfassung

Der Evaluierungsgegenstand (EVG) ist das Digitale Wahlstift-System dotVote®, Version 1.0.

Das Digitale Wahlstift-System (DWS) dotVote® 1.0 ist ein Wahlsystem für die elektronische Abgabe, Speicherung, Bewertung und Auszählung von Stimmen. Es unterstützt die gleichzeitige Durchführung mehrerer Wahlen und erlaubt die zeitnahe Ermittlung der Wahlergebnisse, ohne dabei auf die papiergebundenen Stimmzettel verzichten zu müssen.

Für die Aufzeichnung der Stimmen werden Digitale Wahlstifte, d.h. kugelschreiberähnliche Stifte auf der Basis der Anoto-Technologie eingesetzt, die neben der klassischen Kugelschreibermine über ein hinreichend leistungsfähiges Innenleben aus Kamera, Prozessor, Speicher, Ein/Ausgabeeinheit (Dockingstation) und einer Batterie verfügen. Die Dockingstation dient zur Übertragung der Stimmen an einen PC via USB-Schnittstelle.

Die Stimmzettel haben einen speziell bedruckten Hintergrund, der aus winzigen Punkten besteht. Das feine Raster ist mit bloßem Auge lediglich an einer leicht grauen Färbung zu erkennen. Aus diesem Raster werden beim Schreiben die Koordinaten ermittelt, die bei Stimmabgabe nach jedem Wahlvorgang über eine Dockingstation in die zugehörigen elektronischen Wahlurnen verschoben und dort bis zum Schluss der Wahlhandlung gespeichert werden. Aufgezeichnete Stimmen können auch ohne Speicherung gelöscht werden, wenn der Wähler nicht wahlberechtigt ist oder wenn er sein Votum korrigieren möchte.

Nach dem Schluss der Wahlhandlung werden alle in den elektronischen Wahlurnen gespeicherten Stimmen von der Software des DWS dotVote® 1.0 automatisch bewertet. Der Wahlvorstand kann jede Bewertung überprüfen und muss zweifelhafte Stimmen individuell bewerten. Nach der automatischen Auszählung aller Stimmen werden die Wahlergebnisse ausgedruckt und vor späteren Manipulationen geschützt.

Technische Fehler werden so behandelt, dass sich das DWS dotVote® 1.0 zu jedem Zeitpunkt in einem sicheren Betriebszustand befindet. Bei Bedarf kann ein geschützter Wiederanlauf durchgeführt werden, der die Fortsetzung des sicheren Betriebs gewährleistet.

Neben den Digitalen Wahlstiften und der Software des DWS dotVote® 1.0 werden für jedes Wahllokal ausreichend viele Stimmzettel mit Punkteraster, ein PC (Desktop oder Laptop), ein externer Datenträger (Festplattenlaufwerk, Flash Cards etc.) zur redundanten Speicherung der Wahldaten und ein Drucker zum Ausdruck der Wahlergebnisse benötigt.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile Schutzprofil Digitales Wahlstift-System, Version 1.0.1, BSI-PP-0031-2007 [8].

Die Vertrauenswürdigkeitskomponenten sind dem Teil 3 der Common Criteria entnommen (siehe Teil C oder [1], Teil 3). Der EVG erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL 3 mit Zusatz von ADV_SPM.1 und AVA_MSU.3

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6] Kapitel 5.1.1 beschrieben. Sie wurden komplett dem Teil 2 der Common Criteria entnommen. Der EVG ist daher konform zum Teil 2 der Common Criteria.

Die funktionalen Sicherheitsanforderungen für die IT-Umgebung des EVG werden in den Sicherheitsvorgaben [6] im Kapitel 5.2 dargestellt.

Die funktionalen Sicherheitsanforderungen werden durch die folgenden Sicherheitsfunktionen des EVG umgesetzt:

Sicherheitsfunktion des EVG	Thema
SF.Protokollierung	Protokollierung sicherheitsrelevanter Ereignisse
SF.Stimmenlöschung	Löschung der Stimmen im digitalen Wahlstift
SF.Stiftmanagement	Verwaltung der Betriebszustände der digitalen Wahlstifte
SF.Stimmenübertragung	Übertragung der Stimmen von einem Digitalen Wahlstift in die elektronischen Wahlurnen
SF.Wahlmanagement	Verwaltung der Betriebszustände der elektronischen Wahlurnen
SF.Stimmenbewertung	Automatische und manuelle Bewertung der Stimm Datensätze
SF.Ergebnisschutz	Schutz der Wahldaten vor unbemerkter Manipulation und Erzeugung eines Nachweis ihren Ursprungs
SF.Fehlermanagement	Behandlung von Bedienungsfehlern, Betriebsstörungen und Betriebsunterbrechungen
SF.Anlauf	Anlauf des digitalen Wahlstiftsystems
SF.Firmwareschutz	Schutz der Firmware vor unberechtigtem Austausch oder unberechtigter Modifikation
SF.Versiegelung	Versiegelung der digitalen Wahlstifte

Tabelle 1: Sicherheitsfunktionen des EVG

Mehr Details sind in den Sicherheitsvorgaben [6], Kapitel 6.1 dargestellt.

Die in den Sicherheitsvorgaben [6], Kapitel 6.1 für bestimmte Funktionen angegebene Stärke der Funktionen "mittel" wird bestätigt.

Die Bewertung der Stärke der Funktionen erfolgte ohne Einbeziehung der für die Ver- und Entschlüsselung eingesetzten Kryptoalgorithmen (vgl. §4 Abs. 3 Nr. 2 BSIG). Für Details siehe Kap. 9 dieses Berichtes.

Die Werte, die durch den TOE geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in Kapitel 3 dar.

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

Der Evaluierungsgegenstand (EVG) heisst:

Digitales Wahlstiftsystem dotVote® Version 1.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Identifizier	Version	Auslieferungsart
1	HW	Digitale Wahlstifte (incl. Stiftminen, Stiftsiegel, Dockingstationen, Etiketten und Block mit Anoto-Pattern für Funktionstest)	Logitech IO2 BT, P/N 866142-1000	Vorkonfektionierte Zusammenstellung aller im Wahlbüro benötigter Teile
2	SW	Firmware des Digitalen Wahlstifts	FW U44.53	auf Stift gespeichert
3	SW	dotVote® Applikation	1.0	CD
4	DOC	dotVote® Handbuch für den Administrator	2.4	Papier
5	DOC	dotVote® Handbuch für den Wahlvorstand	2.2	Papier
6	DOC	dotVote® Wählerinformation	2.0	Papier

Tabelle 2: Auslieferungsumfang des EVG

Der komplette Lieferumfang (EVG und EVG-Umgebung) ist detailliert in den Sicherheitsvorgaben [6], Kapitel 2.1.2 beschrieben.

Das Auslieferungsverfahren ist durch den Hersteller klar definiert und in den Sicherheitsvorgaben [6], Kapitel 2.1.3 detailliert beschrieben.

3 Sicherheitspolitik

Die Sicherheitspolitik wird durch die funktionalen Sicherheitsanforderungen ausgedrückt und durch die Sicherheitsfunktionen des EVG umgesetzt. Sie behandelt die folgenden Sachverhalte:

Zu keinem Zeitpunkt darf eine Zusammenführung von Wähler und abgegebener Stimme hergestellt werden können. Eine Zuordnung darf auch nicht über die Zeit oder die Reihenfolge der Stimmabgaben ableitbar sein. Darüber hinaus darf das Digitale Wahlstift-System dotVote® 1.0 dem Wähler nicht die Möglichkeit geben, seine Stimme gegenüber anderen zu beweisen.

Es darf an keiner Stelle – weder bei der Stimmabgabe noch bei der Speicherung – möglich sein, Stimmen zu verändern oder zu löschen. Das unberechtigte Hinzufügen von Stimmen in die elektronischen Wahlurnen muss ausgeschlossen werden .

Die Berechnung von Zwischenergebnissen vor dem Schluss der Wahlhandlung muss ausgeschlossen werden.

Die Wahlergebnisse müssen korrekt ermittelt werden, insbesondere müssen alle abgegebenen gültigen Stimmen auch gezählt werden.

Der EVG muss eine Wiederanlauffunktion definieren, falls es zu einer technischen Betriebsstörung oder -unterbrechung kommt. Dabei muss auch der Gefahr des Verlusts oder der Veränderung bereits gespeicherter Stimmen geeignet begegnet werden.

Der EVG muss die Wahldaten durch Erzeugung, Anzeige und Ausdruck eines verifizierbaren Ursprungsnachweises schützen und sicherheitsrelevante Ereignisse protokollieren.

4 Annahmen und Klärung des Einsatzbereiches

Die Annahmen in den Sicherheitsvorgaben sowie Teile der Bedrohungen und organisatorischen Sicherheitspolitiken werden nicht durch den EVG selbst abgedeckt. Diese Aspekte setzen voraus, dass bestimmte Sicherheitsziele durch die EVG-Einsatzumgebung erfüllt werden. Hierbei sind die folgenden Punkte relevant:

- Vertrauenswürdige Administratoren
- Vertrauenswürdige Wahlvorstände, die für einen korrekten Ablauf der Wahl sorgen
- Korrekt installierte und konfigurierte IT-Umgebung
- Notfallkonzept bei Ausfall des EVG

Details finden sich in den Sicherheitsvorgaben [6], Kapitel 4.2.

5 Informationen zur Architektur

Das Digitale Wahlstift-System dotVote® 1.0 besteht aus sechs Teilsystemen:

- Firmware / Wahlstift (FW / HW)
Dieses Teilsystem ist für die Aufnahme von Stimmzetteln zuständig. Der Wahlstift stellt hierfür die notwendige Hardware zur Verfügung. Durch die Firmware des Wahlstiftes ist der von der Wahlstifthardware (Kamera) als bekannt kategorisierte Koordinatenraum auf solchen begrenzt, der explizit für den Einsatz mit dem DWS dotVote® 1.0 vorgesehen ist. Sie übernimmt die unwiederbringliche Löschung der Daten im Stift und leistet darüber hinaus einen Schutz des Firmware-Updates.
- DotVoteFile (SW)
Dieses Programm wird vom Stifftreiber aufgerufen und erhält hiervon alle Daten, die von einem Wahlstift in das DWS dotVote® 1.0 übertragen werden als ein Datenobjekt.
- DotVoteCount (SW)
Dieses Programm wird nach dem Abschluss des Wahltages vom Teilsystem Frontend aufgerufen, damit es die über den Tag gesammelten Rohdaten auswertet (Kreuzerkennung).
- DotVoteFileService (SW)
Dieses Programm wird vom Frontend aufgerufen, wenn ein Wahlstift korrekt mit dem DWS dotVote® 1.0 verbunden wurde, sich jedoch keine Daten im Stiftspeicher befanden (Wahlverzicht).
- Frontend (SW)
Das Frontend hat die Kontrolle über den EVG. Es stellt die Kommunikationsschnittstelle zum Wähler und zum Wahlvorstand dar. Hierfür stellt es Meldungen und Informationen sowie unterschiedliche Verarbeitungsschritte am Bildschirm bereit.
- USB Observer (SW)
Dieses Teilsystem beobachtet die Kommunikation des Wahlstiftes mit dem Stifftreiber. Ergebnisse der Beobachtung speichert es in der Registry.

6 Dokumentation

Die evaluierte Dokumentation, die in Tabelle 2 aufgeführt ist, wird zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem EVG in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des EVG, die im Kapitel 10 enthalten sind, müssen befolgt werden.

7 Testverfahren

7.1 Funktionale Tests des Herstellers

EVG Testkonfiguration:

Der EVG wurde in der in den Sicherheitsvorgaben [6] spezifizierten Einsatzumgebung getestet. Es wurden digitale Wahlstifte (Logitech IO2 BT, P/N 866142-1000) mit der Firmware FW U44.53 sowie die EVG-Software Version 1.0.2.698 genutzt.

Testumfang:

Der EVG an den externen Schnittstellen komplett mit Positiv- und Negativtests für jedes Funktionselement aller Sicherheitsfunktionen getestet.

Testergebnis:

Die durchgeführten Tests zeigten, dass sich der EVG wie dokumentiert verhält.

7.2 Unabhängige Tests der Prüfstelle

EVG Testkonfiguration:

Der EVG wurde in seiner Einsatzumgebung getestet; dazu wurde folgendes Equipment zur Verfügung gestellt:

2 Laptops: Intel Core 2 CPU, 1.83 GHz, 987 MHz, 1,99 GB RAM
Microsoft Windows XP Professional, Version 2002, Service Pack 2

2 Drucker: Kyocera FS-1030D

1 Wahlbox mit 4 Dockingstationen, USB-Netzteil, 2 Taschen Ersatzminen mit Aufdruck dotVote®, 1 USB-Verlängerungskabel, Kennzeichnungsetiketten für Dockingstation, Siegeletiketten Wahlvorstand, Laserdruckerpapier, Funktionsbogen, 4 Wahlstifte mit der Firmware FW U44.53, 2 USB-Sticks (Transcend JetFlash 4GB), EVG-Version: 1.0.2.698

Testumfang:

Es wurden alle Sicherheitsfunktionen des EVG an den externen Schnittstellen getestet. Darüberhinaus wurde eine Auswahl von Tests aus den Testplänen des Herstellers durchgeführt, insbesondere zur Updatefunktionalität des Stiftes, zum Löschen des Stiftspeichers und zum Siegel. Des Weiteren wurden die Herstellertests zum EVG am Frontend – also dort, wo Wahlvorstand und Wähler den EVG benutzen – wiederholt, indem der im Handbuch für den Wahlvorstand beschriebene Ablauf – ausgehend von den Wahlvorbereitungen über die Wahl bis hin zur Stimmzettelsichtung und -prüfung und Versiegelung – der Reihe nach abgetestet wurde.

Testergebnis:

Die durchgeführten Tests zeigten, dass sich der EVG wie dokumentiert verhält.

8 Evaluierte Konfiguration

Dieses Zertifikat bezieht sich auf die folgenden Konfigurationen des EVG:

Der EVG besteht aus den Digitalen Wahlstiften (Logitech IO2 BT, P/N 866142-1000 incl. Stiftminen, Stiftsiegel, Dockingstationen, Etiketten und Block mit Anoto-Pattern für Funktionstest), der zugehörigen Firmware FW U44.53 und der EVG-Software „dotVote® Applikation Version 1.0“.

Für den Betrieb des EVG ist folgende Hardware und Software erforderlich, die nicht zum EVG gehört:

- Stimmzettel mit Anoto-Punkteraster (spezifische Gestaltung für die jeweilige Wahl)
- PC (Desktop oder Laptop) mit mind. 6 USB-Ports (ggf. realisiert über USB-Hub)
- Lautsprecher, Bildschirm, Tastatur (ggf. im Laptop integriert)
- Internes und externes (USB-Stick, mind. 4 GB) Speichermedium
- Drucker mit USB-Anschluss
- Zubehör (Stromversorgung, USB-Kabel, Maus, Druckerpapier)
- Betriebssystem des PCs (Microsoft Windows XP Professional SP2)
- Gerätetreiber für die Kommunikation mit den Speichermedien und dem Drucker
- Applikationsplattform (.NET Framework 1.1.4322)
- MSDE SQL Server 2000 SP4 (Version 8.00.2039) DesktopEngine
- Adobe FlashPlayer Version 9.0.16.0

9 Ergebnis der Evaluierung

9.1 CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR), [7] wurde von der Prüfstelle gemäß den Common Criteria Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005 [1], der Methodologie [2], den Anforderungen des Schemas [3] und allen Interpretationen des Schemas (AIS) [4] erstellt, die für den EVG relevant sind. Die Evaluierungsmethodologie CEM [2] wurde für die Komponenten bis zur Vertrauenswürdigkeitsstufe EAL 3 verwendet.

Das Urteil PASS der Evaluierung wird für die folgenden Vertrauenswürdigkeitskomponenten bestätigt:

- Alle Komponenten der Klasse ASE
- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 3 der CC (siehe auch Teil C des Zertifizierungsreports)
- Die Komponenten
ADV_SPM.1 und AVA_MSU.3

Die Evaluierung hat gezeigt:

- PP Konformität: Schutzprofil Digitales Wahlstift-System, Version 1.0.1, BSI-PP-0031-2007 [8]

- Funktionalität: PP konform plus produktspezifische Ergänzungen
Common Criteria Teil 2 konform
- Vertrauenswürdigkeit: Common Criteria Teil 3 konform
EAL 3 mit Zusatz von
ADV_SPM.1 und AVA_MSU.3
- Die folgenden Sicherheitsfunktionen erfüllen die behauptete Stärke der Funktion:
mittelSF.Wahlmanagement und SF.Firmwareschutz

Die Ergebnisse der Evaluierung gelten nur für den EVG gemäß Kapitel 2 und für die Konfigurationen, die in Kapitel 8 aufgeführt sind.

9.2 Ergebnis der kryptographischen Bewertung

Die Stärke der Kryptoalgorithmen wurde im Rahmen der Evaluierung nicht bewertet (vgl. §4 Abs. 3 Nr. 2 BSIG).

10 Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 2 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des EVG und alle darin enthaltenen Sicherheitshinweise sind zu beachten.

11 Sicherheitsvorgaben

Die Sicherheitsvorgabe [6] wird zur Veröffentlichung in einem separaten Dokument im Anhang A bereitgestellt.

12 Definitionen

12.1 Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
DWS	Digitales Wahlstiftsystem
EAL	Evaluation Assurance Level - Vertrauenswürdigkeitsstufe
EVG	Evaluierungsgegenstand (EVG)
IT	Informationstechnologie
ITSEF	Information Technology Security Evaluation Facility – Prüfstelle für IT-Sicherheit
PP	Protection Profile - Schutzprofil
SF	Sicherheitsfunktion
SFP	Security Function Policy – Politik der Sicherheitsfunktion
SOF	Strength of Function – Stärke der Funktion
ST	Security Target – Sicherheitsvorgaben
TOE	Target of Evaluation –Evaluierungsgegenstand
TSC	TSF Scope of Control – Anwendungsbereich der TSF-Kontrolle
TSF	TOE Security Functions - EVG-Sicherheitsfunktionen
TSP	TOE security policy - EVG-Sicherheitspolitik

12.2 Glossary

Anoto-Technologie - Die von dem schwedischen Unternehmen Anoto Group AB entwickelte und patentierte Anoto-Technologie ermöglicht die digitale Erfassung, Übertragung und Verarbeitung handschriftlicher Texte und Zeichnungen mit einem digitalen Stift und einem auf Papier gedruckten digitalen Punkteraster, das ein Koordinatensystem kodiert.

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

Digitaler Wahlstift - Unter dem Begriff Digitaler Wahlstift werden alle von Anoto Group AB zugelassenen digitalen Stifte verstanden, die die dotforms®-Funktionalität ermöglichen und deren Firmware die in diesen Sicherheitsvorgaben beschriebenen Sicherheitsfunktionen erbringt.

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 - 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.

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 Anwenderbedürfnisse erfüllen.

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

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 Sicherheitspezifikationen, die als Grundlage für die Prüfung und Bewertung eines angegebenen EVG dienen.

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.

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-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.

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.

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

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

13 Literaturangaben

- [1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005
- [3] BSI-Zertifizierung: Verfahrensbeschreibung (BSI 7125)
- [4] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind⁸.
- [5] Deutsche IT-Sicherheitszertifikate (BSI 7148, BSI 7149), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird
- [6] Sicherheitsvorgaben BSI-DSZ-0444-2008, Version 1.6, 08.05.08, Sicherheitsvorgaben Digitales Wahlstift-System dotVote® Version 1.0, Diagramm Halbach GmbH & Co. KG und WRS Softwareentwicklung GmbH (öffentliches Dokument)
- [7] Evaluation Technical Report, Version 1.1, 09.05.08, „Evaluierungsbericht Digitales Wahlstift-System dotVote® Version 1.0“, datenschutz nord GmbH (vertrauliches Dokument)
- [8] Schutzprofil „Digitales Wahlstift-System, Version 1.0.1“, BSI-PP-0031, 28.02.2007, Freie und Hansestadt Hamburg
- [9] Konfigurationsliste für den EVG, Version 5.71, 09.05.08, „Konfigurationsliste Digitales Wahlstift-System dotVote® Version 1.0“, Diagramm Halbach GmbH & Co. KG und WRS Softwareentwicklung GmbH (confidential document)
- [10] Administratorhandbuch, Version 2.4, 31.01.08, „Digitales Wahlstift-System dotVote® Version 1.0 - Handbuch für den Administrator -“
- [11] Benutzerhandbuch, Version 2.2, 15.01.08, „Digitales Wahlstift-System dotVote® Version 1.0 - Handbuch für den Wahlvorstand -“
- [12] Wählerinformation, Version 1.0, 12.12.2007

⁸Inbesondere:

- AIS 32, Version 1, 2 Juli 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 Juni 2004, Evaluation Methodology for CC Assurance Classes for EAL5+

Dies ist eine eingefügte Leerseite.

C Auszüge aus den Kriterien

Anmerkung: Die folgenden Auszüge aus den technischen Regelwerken wurden aus der englischen Originalfassung der CC Version 2.3 entnommen, da eine vollständige aktuelle Übersetzung nicht vorliegt.

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
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)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 11.1)

“Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Evaluation Assurance Level Components							by
		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: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 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 11.4)

“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 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 11.5)

“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 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 11.6)**“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 11.7)**“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 11.8)**“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 11.9)**“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.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

"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 19.4)

"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 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

D Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Die Sicherheitsvorgaben werden in einem eigenen Dokument zur Verfügung gestellt.