

BSI-DSZ-CC-0433-2008

ZU

Veridat Ident, Volumen, Verwiegung 4.0

der

Veridat Eurotech GmbH

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



Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0433-2008

Abfallbehälter-Identifikationssystem

Veridat Ident, Volumen, Verriegung 4.0

von Veridat Eurotech GmbH

PP-Konformität: Protection Profile Waste Bin Identification
Systems (WBIS-PP) Version 1.04
BSI-PP-0010-2004

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

Vertrauenswürdigkeit: Common Criteria Teil 3 konform
EAL 1



Common Criteria
Arrangement



Das in diesem Zertifikat genannte IT-Produkt wurde von einer akkreditierten und lizenzierten Prüfstelle nach der Gemeinsame 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, 25. Januar 2008

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag



SOGIS - MRA

Bernd Kowalski
Abteilungspräsident

L.S.

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 9582-111

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

Teil A: Zertifizierung

Teil B: Zertifizierungsbericht

Teil C: Auszüge aus den technischen Regelwerken

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)
- 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 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

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.

2.1 Europäische Anerkennung von ITSEC/CC - Zertifikaten

Ein Abkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten, auf deren Grundlage ITSEC-Zertifikate für IT-Produkte unter gewissen Bedingungen anerkannt werden, ist im März 1998 in Kraft getreten (SOGIS-MRA).

Es wurde von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Niederlande, Norwegen, Portugal, Schweden, Schweiz und Spanien. Das Abkommen wurde zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC bis einschließlich der Evaluationsstufe EAL7 erweitert. Das BSI erkennt die Zertifikate der nationalen Zertifizierungsstellen von Frankreich und Großbritannien im Rahmen dieses Abkommens an.

Das SOGIS-MRA-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens anerkannt wird.

2.2 Internationale Anerkennung von CC - Zertifikaten

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

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, 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 Common Criteria-Logo auf dem Zertifikat zeigt, dass das Zertifikat unter den Bedingungen des Abkommens anerkannt wird.

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 Veridat Ident, Volumen, Verwiegung 4.0 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts Veridat Ident, Volumen, Verwiegung 4.0 wurde von der Tele-Consulting security | networking | training GmbH durchgeführt. Die Evaluierung wurde am 16. Januar 2008 beendet. Das Prüflabor Tele-Consulting security | networking | training GmbH ist eine vom BSI anerkannte Prüfstelle (ITSEF)⁶.

Der Sponsor und Antragsteller ist: Veridat Eurotech GmbH

Der Entwickler ist: Mobil Elektronik 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. Da Angriffe mit neuen oder weiterentwickelten Methoden in Zukunft möglich sind, besteht die Möglichkeit, die Widerstandsfähigkeit des Produktes im Rahmen des Assurance Continuity-Programms des BSI regelmäßig überprüfen zu lassen. Die Zertifizierungsstelle empfiehlt, regelmäßig eine Einschätzung der Widerstandsfähigkeit vornehmen zu lassen.

⁶ Information Technology Security Evaluation Facility

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt 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.

5 Veröffentlichung

Der nachfolgende Zertifizierungsbericht enthält die Seiten B-1 bis B-14 und D-1 bis D-2.

Das Produkt Veridat Ident, Volumen, Verriegung 4.0 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: <http://www.bsi.bund.de>). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes angefordert werden.⁷ Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

⁷ Veridat Eurotech GmbH
Daimlerstraße 7
72829 Engstingen

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

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

Gliederung des Zertifizierungsberichtes

1	Zusammenfassung	3
2	Identifikation des EVG	5
3	Sicherheitspolitik	6
4	Annahmen und Klärung des Einsatzbereiches	6
5	Informationen zur Architektur	7
6	Dokumentation	8
7	Testverfahren	8
8	Evaluierte Konfiguration	9
9	Ergebnis der Evaluierung	10
9.1	CC spezifische Ergebnisse	10
9.2	Bewertung der kryptografischen Stärke	10
10	Auflagen und Hinweise zur Benutzung des EVG	11
11	Security Target	11
12	Definitionen	12
12.1	Abkürzungen	12
12.2	Glossary	12
13	Literaturangaben	14

1 Zusammenfassung

Beim EVG handelt es sich um das Abfallbehälter-Identifikationssystem Veridat Ident, Volumen, Verwiegung 4.0, bestehend aus der Sicherheitskomponente der Fahrzeugsoftware ME_VDSC, Version 1.0 und der Sicherheitskomponente der PC-Software ME_TTSC, Version 1.0, den Transpondern (ID-Tags) V-CNT-125ISO (V-CNT-125-0001) und V-CNT-134BDE (V-CNT-134-0001) sowie den Readern TCL101 (EURO I.D. V3.5E) und TCL102 (ASR V2.22).

Abfallbehälter-Identifikations-Systeme (WBIS) im Sinne dieses Dokumentes sind Systeme, durch die Abfallbehälter mit einem ID-Tag (z.B. mit elektronischem Chip, dem Transponder) identifiziert werden, um feststellen zu können, wie oft der einzelne Abfallbehälter geleert worden ist. Dabei handelt es sich bei diesen Systemen nicht um die direkte Identifizierung von Abfällen, sondern um die Identifizierung der Behälter, in denen Abfälle zur Entsorgung bereitgestellt werden.

Der EVG prüft dazu die vom Transponder eingelesenen Daten auf Integrität, ergänzt korrekte Daten durch Datum und Uhrzeit der Leerung, fügt ein Gültigkeits- sowie ein Integritätsmerkmal an und speichert diese Daten dann redundant auf zwei getrennten Speichern im Fahrzeugrechner, damit diese auch bei einem Verlust der Daten in einem der beiden Speicher wiederhergestellt werden können. Bei der Übertragung in die Bürosoftware prüft der EVG in der Sicherheitskomponente der PC-Software die Daten erneut auf Gültigkeit und Integrität und kennzeichnet diese entsprechend.

Damit ist der EVG in der Lage, die für die Abrechnung relevanten Daten (Identifikationsdaten, Zeitstempel) vom Transponder bis in die Bürosoftware vor Manipulation und Verlust zu schützen.

Die Sicherheitsvorgaben [6] stellen die Grundlage für die Zertifizierung dar. Sie basieren auf dem zertifizierten Protection Profile Waste Bin Identification Systems (WBIS-PP) Version 1.04, BSI-PP-0010-2004 [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 1 .

Die funktionalen Sicherheitsanforderungen (Security Functional Requirements SFR) an den EVG werden in den Sicherheitsvorgaben [6], Kapitel 5.1 beschrieben. Sie wurden dem Teil 2 der Common Criteria entnommen und durch neu definierte funktionale Sicherheitsanforderungen ergänzt. Der EVG ist daher gekennzeichnet als Teil 2 erweitert.

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

Sicherheitsfunktion des EVG	Thema
TSF_DAU.1	Datenauthentisierung
TSF_ITT.5	EVG-interner Transfer
TSF_SDI.1	Integrität der gespeicherten Daten
TSF_FLT.1	Fehlertoleranz

Tabelle 1: Sicherheitsfunktionen des EVG

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

Die Werte, die durch den TOE geschützt werden, sind in den Sicherheitsvorgaben [6], Kapitel 3.1, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken in den Kapiteln 3.2 – 3.4 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::

Veridat Ident, Volumen, Verwiegung 4.0

Die folgende Tabelle beschreibt den Auslieferungsumfang:

Nr	Typ	Bezeichnung	Version	Auslieferungsart
1	SW	Sicherheitskomponente der PC-Software: ME_TTSC	1.0	Vom Hersteller installiert
2	SW	Sicherheitskomponente der Fahrzeugsoftware: ME_VDSC	1.0	Vom Hersteller installiert
3	HW	ID-Tag 1: V-CNT-125ISO	V-CNT-125-0001	
4	HW	ID-Tag 2: V-CNT-134BDE	V-CNT-134-0001	
5	HW	Reader 1: TCL101	EURO I.D. V3.5E	Am Fahrzeug montiert
6	HW	Reader 2: TCL102	ASR V2.22	Am Fahrzeug montiert
7	DOK	Systemverwalterhandbuch [9]	1.03 14.12.07	
8	DOK	Benutzerhandbuch [10]	1.03 14.12.07	
9	DOK	Bedienungsanleitung MEVOS [11]	1.0 31.08.07	

Tabelle 2: Auslieferungsumfang des EVG

Der EVG-Teil der Fahrzeugsoftware (ME_VDSC) wird vom Hersteller als Teil der Fahrzeugsoftware installiert und zusammen mit dieser ausgeliefert. Die Versionsabfrage zum EVG-Teil der Fahrzeugsoftware ist im Systemverwalterhandbuch [9] und im Benutzerhandbuch [10] beschrieben.

Die Sicherheitskomponente der PC-Software (ME_TTSC) wird zusammen mit MEVOS-Software ausgeliefert. Die Versionsabfrage ist im Benutzerhandbuch [10] und in der Bedienungsanleitung MEVOS [11] beschrieben.

3 Sicherheitspolitik

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

- Erzeugung eines Gültigkeitsmerkmals für die Leerungsdaten
- Manipulationsschutz der Leerungsdaten bei der Übertragung
- Integritätsschutz der gespeicherten Daten
- Redundante Speicherung

4 Annahmen und Klärung des Einsatzbereiches

Die Annahmen in den Sicherheitsvorgaben 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:

- Montage der Transponder (ID-Tags)
- Vertrauenswürdigen Personal
- Zugangsschutz zum EVG
- Überprüfung der vollständigen Übertragung der Leerungsdatenblöcke
- Datensicherung
- Systeminstallation

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

5 Informationen zur Architektur

Die folgende Abbildung gibt jedoch einen Überblick über das Abfallbehälter-Identifikationssystem.

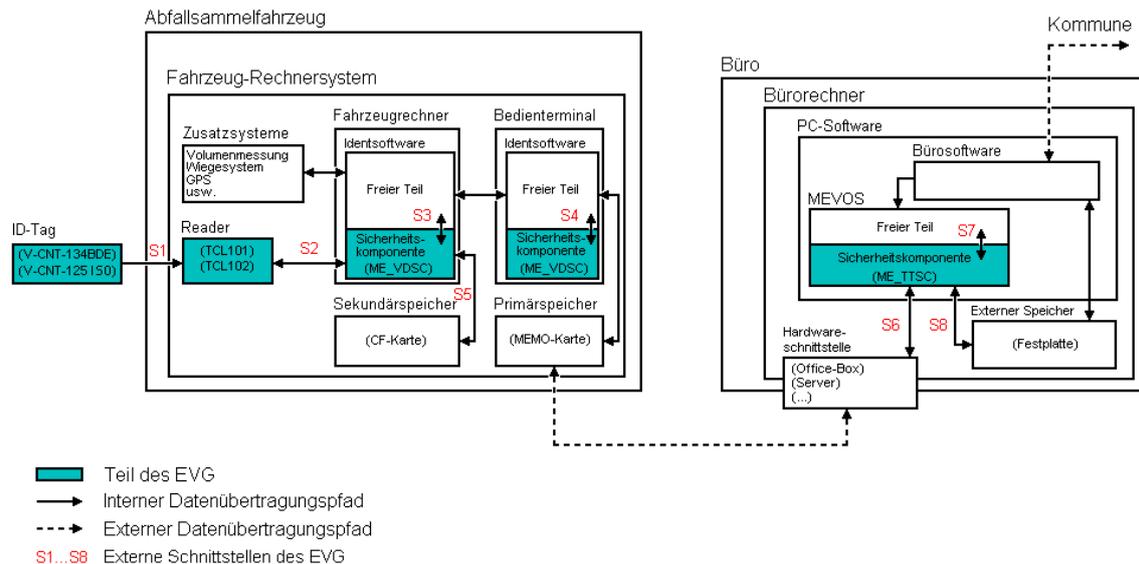


Abbildung 1: Überblick über das Abfallbehälter-Identifikationssystem

Das System besteht aus drei getrennten Teilen. Dies sind die Transponder (ID-Tags) mit den Identifikationsdaten, das Abfallsammelfahrzeug mit dem Fahrzeug-Rechnersystem und der Bürorechner mit der Bürosoftware. Das Fahrzeug-Rechnersystem beinhaltet die Reader, den Fahrzeugrechner und das Bedienterminal (jeweils mit dem EVG-Teil der Fahrzeugsoftware (Sicherheitskomponente ME_VDSC) und dem nicht zum EVG gehörenden Teil der Fahrzeugsoftware) sowie die nicht zum EVG gehörenden externen Speicher und optionalen Zusatzsysteme. Die Bürosoftware auf dem Bürorechner beinhaltet neben der MEVOS-Software mit der zum EVG gehörenden Sicherheitskomponente (ME_TTSC) weitere Teile, die jedoch nicht zum EVG gehören. Des Weiteren verfügt der Bürorechner über eine Hardware-schnittstelle zur Übertragung der Leerungsdaten und einen externen Speicher zur Archivierung der geprüften Leerungsdaten. Die EVG-Teile sind in der Abbildung blau hinterlegt und die verschiedenen Schnittstellen durch schwarze Pfeile gekennzeichnet.

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 Testkonfiguration

Die vom Entwickler bereitgestellte Testkonfiguration bestand aus den Komponenten des EVG und des Produkts in der aktuellen Fassung. Der Entwickler hat alle im Fahrzeug befindlichen Teile des Produktes auf einer Platte montiert und die Teile miteinander verdrahtet.

Das Produkt war gemäß den Vorgaben im Handbuch bereits vorinstalliert. Die Installation der Software MEVOS wurde vom Evaluator gemäß der Beschreibung im Handbuch nachvollzogen. Die Evaluatoren haben sich davon überzeugt, dass der in den Sicherheitsvorgaben [6] spezifizierte EVG für die Tests zur Verfügung stand.

Folgende EVG-Teile wurden für die Tests verwendet:

- Reader 1: TCL 102, Seriennummer 009
- Transponder: V-CNT-134BDE, Version: V-CNT-134-0001
Für den Test wurden unter dieser Bezeichnung Transponder des Herstellers Texas Instruments (RI-TRP-RRHP) und Sokymat (WORLD TAG BDE - 20mm FDX-b 134.2 kHz/ISO 11785) benutzt.
- Reader 2: TCL 101, Seriennummer 004, (TCL 100 in Testphase 1)
- Transponder: V-CNT-125ISO, Version: V-CNT-125-0001
Für den Test wurden unter dieser Bezeichnung Transponder des Herstellers AEG (Trovan PSK, ID 200)
- Bedienterminal EEA 092 704 mit SW Version 704 V1.04, 06.07.07 (Phase 1: 704 V1.00), Seriennummer 18 mit der Sicherheitskomponente der Fahrzeugsoftware; ME_VDSC, Version 1.0
- Hauptsteuerung DSE 055 301 mit SW Version 301 V1.05, 20.07.07 (Phase 1: 301 V1.00), Seriennummer 15 mit der Sicherheitskomponente der Fahrzeugsoftware; ME_VDSC, Version 1.0

Des weiteren stand ein Laptop zur Verfügung, auf dem MEVOS installiert wurde und auf dem eine Kopie der Entwicklungsumgebung zur Verfügung stand:

- Fujitsu Siemens Computers Mobile Genuine Intel(R) CPU T2500 @ 2.00GHz 997 MHz, 0,99 GB RAM
- Microsoft Windows XP Professional Version 2002, Service Pack 2
- MEVOS, Version 1.1.0.2 mit der Sicherheitskomponente der PC-Software, ME_TTSC, Version 1.0

7.2 Zusammenfassung der unabhängigen Prüfstellentests

Es wurden alle Sicherheitsfunktionen des EVG an den zugänglichen Benutzerschnittstellen mit jeweils mindestens einem Testfall getestet, um das korrekte Verhalten der Sicherheitsfunktionen zu überprüfen.

Insgesamt zeigen die Tests, dass sich der EVG wie in den Sicherheitsvorgaben [6] spezifiziert verhält.

Für die postulierte Evaluationsstufe EAL 1 werden keine Herstellertests gefordert.

8 Evaluierte Konfiguration

Der EVG wird ausschließlich in einer Konfiguration betrieben. Er wird durch die Bezeichnung „Abfallbehälter-Identifikationssystem Veridat Ident, Volumen, Verriegelung 4.0, bestehend aus der Sicherheitskomponente der Fahrzeugsoftware ME_VDSC, Version 1.0 und der Sicherheitskomponente der PC-Software ME_TTSC, Version 1.0, den Transpondern (ID-Tags) V-CNT-125ISO (V-CNT-125-0001) und V-CNT-134BDE (V-CNT-134-0001) sowie den Readern TCL101 (EURO I.D. V3.5E) und TCL102 (ASR V2.22)“ identifiziert.

Dieses Zertifikat bezieht sich ausschließlich auf diese Konfiguration des EVG.

9 Ergebnis der Evaluierung

9.1 CC spezifische Ergebnisse

Der Evaluierungsbericht (Evaluation Technical Report, ETR), [7] wurde von der Prüfstelle gemäß den Common Criteria [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 1 verwendet.

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

- Alle Komponenten der Klasse ASE
- Alle Komponenten der Vertrauenswürdigkeitsstufe EAL 1 der CC (siehe auch Teil C des Zertifizierungsreports)

Die Evaluierung hat gezeigt:

- PP Konformität Protection Profile Waste Bin Identification Systems (WBIS-PP) Version 1.04
BSI-PP-0010-2004 [8]
- Funktionalität: PP konform plus produktspezifische Ergänzungen
Common Criteria Teil 2 erweitert
- Vertrauenswürdigkeit Common Criteria Teil 3 konform
EAL 1

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

Der EVG enthält keine kryptografischen Algorithmen. Daher wurden auch keine solchen Mechanismen bewertet.

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. Zusätzlich ist die folgende Auflage zu beachten:

- Im Laufe der Evaluierung hat sich die Hardware-Bezeichnung des Readers für Trovan PKS Transponder von TCL 100 auf TCL 101 geändert. Beim Test der Prüfstelle war der entsprechende Textmodul zur Anzeige der Bezeichnung am Bedienterminal noch nicht geändert worden. Es wird dem Hersteller zur Auflage gemacht, den EVG nur mit einem aktualisierten Textmodul auszuliefern.

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
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
WBIS	Waste Bin Identification System – Abfallbehälter-Identifikationssystem

12.2 Glossary

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

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 Spezifikationen, 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 sind.
- [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-0433-2008, Version 1.8, 10.01.2008, "Sicherheitsvorgaben Veridat Ident, Volumen, Verwiegung 4.0", Veridat Eurotech GmbH (öffentliches Dokument)
- [7] Evaluationsbericht, Version 3, 15.01.2008, Evaluationsbericht BSI-DSZ-CC-0433 zu Veridat Ident, Volumen, Verwiegung 4.0, Tele-Consulting GmbH (vertrauliches Dokument)
- [8] Protection Profile Waste Bin Identification Systems (WBIS-PP) Version 1.04
BSI-PP-0010-2004
- [9] Systemverwalterhandbuch, Version 1.03, 14.12.2008, „Systemverwalterhandbuch Abfall-Behälter-Identifikations-System: Veridat Ident, Volumen, Verwiegung 4.0“, Veridat Eurotech GmbH
- [10] Benutzerhandbuch, Version 1.03, 14.12.2008, „Benutzerhandbuch Abfall-Behälter-Identifikations-System: Veridat Ident, Volumen, Verwiegung 4.0“, Veridat Eurotech GmbH
- [11] Bedienungsanleitung MEVOS, Version 1.0, 31.08.2007, „Bedienungsanleitung MEVOS V1.0“, Veridat Eurotech GmbH

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.

Dies ist eine eingefügte Leerseite.