VERIDAT IDENT, VOLUMEN, VERWIEGUNG 4.0

SICHERHEITSVORGABEN
(Security Target)

Version 1.8

10. Januar 2008

Evaluierungsgrundlage:

Common Criteria, Version 2.3

Gemeinsame Kriterien für die Prüfung und Bewertung
der Sicherheit von Informationstechnik

Vertrauenswürdigkeitsstufe: EAL1

Hersteller:

EUROTECH GmbH
Daimlerstrasse 7
D-72829 Engstingen

fon (+49) (0) 7129 9369 0
fax (+49) (0) 7129 9369 29
info@veridat.com
http://www.veridat.com

Systementwicklung:

MOBIL ELEKTRONIK GMBH

Bössingerstraße 33
D-74243 Langenbeutingen
☎ +49 (0) 7946 / 9194 - 0
FAX +49 (0) 7946 / 9194 - 130

http://www.mobil-elektronik.com

Inhaltsverzeichnis

Revisionsindex 5

1 ST-Einführung 6

1.1 ST Identifikation 6

1.2 ST Übersicht 6

1.2.1 Darstellungshinweise 7

1.3 Postulat der Übereinstimmung mit CC 8

2 EVG Beschreibung 9

2.1 Produkt-Typ 9

2.1.1 EVG Komponenten: 11

2.1.2 Schnittstellen des EVG: 12

2.1.3 Hardwarevorrausetzungen 13

2.2 Allgemeine Funktionalität 14

2.3 Art der Nutzung 15

3 EVG Sicherheitsumgebung 16

3.1 Schutzwürdige Objekte, Subjekte und Angreifer 16

3.2 Annahmen 17

3.3 Bedrohungen 18

3.3.1 Bedrohungen, denen vom EVG zu begegnen ist 18

3.3.2 Bedrohungen, denen durch die Umgebung zu begegnen ist 18

3.4 Organisatorische Sicherheitspolitiken 18

4 Sicherheitsziele 19

4.1 Sicherheitsziele für den EVG 19

4.2 Sicherheitsziele für die Umgebung 20

5 IT Sicherheitsanforderungen 21

5.1 Funktionale Sicherheitsanforderungen an den EVG 21

5.1.1 Einfache Datenauthentisierung (FDP_DAU.1) 21

5.1.2 EVG-interner Transfer (FDP_ITT) 21

5.1.2.1 Schutz der Integrität des internen Transfers (FDP_ITT.5) (CC Teil 2 erweitert) 21

5.1.3 Integrität der gespeicherten Daten (FDP_SDI) 21

5.1.3.1 Überwachung der Integrität gespeicherter Daten (FDP_SDI.1) 21

5.1.4 Fehlertoleranz (FRU_FLT) 22

5.1.4.1 Verminderte Fehlertoleranz (FRU_FLT.1) 22

5.2 Anforderungen an die Vertrauenswürdigkeit des EVG 22

5.2.1 Konfigurationsmanagement (ACM) 23

5.2.1.1 Versionsnummern (ACM_CAP.1) 23

5.2.2 Auslieferung und Betrieb (ADO) 23

5.2.2.1 Installations-, Generierungs- und Anlaufprozeduren (ADO_IGS.1) 23

5.2.3 Entwicklung (ADV) 24

5.2.3.1 Informelle, funktionale Spezifikation (ADV_FSP.1) 24

5.2.3.2 Informeller Nachweis der Übereinstimmung (ADV_RCR.1) 24

5.2.4 Handbücher (AGD) 25

5.2.4.1 Systemverwalterhandbuch (AGD_ADM.1) 25

5.2.4.2 Benutzerhandbuch (AGD_USR.1) 26

5.2.5 Testen (ATE) 26

5.2.5.1 Unabhängiges Testen - Übereinstimmung (ATE_IND.1) 26

5.3 Sicherheitsanforderungen an die IT Umgebung 27

5.4 Sicherheitsanforderungen an die nicht IT Umgebung 27

6 EVG Übersichtsspezifikation 28

6.1 EVG Sicherheitsfunktionen (TSF) 28

6.1.1 Datenauthentisierung (TSF_DAU.1) 28

6.1.2 EVG-interner Transfer (TSF_ITT.5) 28

6.1.3 Integrität der gespeicherten Daten (TSF_SDI.1) 29

6.1.4 Fehlertoleranz (TSF_FLT.1) 29

6.2 Maßnahmen zur Vertrauenswürdigkeit 30

7 Postulate 31

7.1 PP Verweis 31

7.2 PP Anpassung 31

7.3 PP Ergänzungen 31

8 Erklärung 32

8.1 Erklärung zu den Sicherheitszielen 32

8.2 Erklärung zu den Sicherheitsanforderungen 34

8.2.1 Erklärung zu den funktionalen Sicherheitsanforderungen des EVG 34

8.2.2 Erklärung zu den Anforderungen an die Vertrauenswürdigkeit des EVG 36

8.2.3 Erklärung zu der Anforderung an die Stärke der EVG-Sicherheitsfunktionen 36

8.2.4 Erklärung zu der gegenseitigen Unterstützung der funktionalen Anforderungen und der Anforderung an die Vertrauenswürdigkeit des EVGs 36

8.3 Erklärung zu der EVG Übersichtsspezifikation 37

8.3.1 Erklärung der EVG-Sicherheitsmaßnahmen 39

8.4 Erklärung zu den PP Postulate 39

9 Anhang 40

9.1 Abkürzungen 40

9.2 Glossar 41

Revisionsindex

Revision	Beschreibung	Datum	Autor
0.1	Neues Dokument	02.05.2006	Adrian Pongrac (ME)
0.2	Dokumentlayout an ME Standard angepasst. Dokumentname geändert. Formale Änderungen gemäß den Hinweisen durch TeleConsulting. Ergänzung fehlender bzw. unvollständiger Teile.	10.05.2006	Adrian Pongrac (ME)
0.3	Änderungen und Korrekturen nach Vorprüfung durch TeleConsulting.	23.05.2006	Adrian Pongrac (ME)
1.0	Version zur offiziellen Bewertung.	29.05.2006	Adrian Pongrac (ME)
1.1	Kapitel 5.1.2.1: Formulierung der funktionalen Anforderung FDP_ITT.5 laut Prüfbericht von TeleConsulting abgeändert. Kapitel 6.1.1 und 6.1.3 laut BSI Review präzisiert. Kapitel 8.3 laut BSI Review, die Erklärung zu der EVG Übersichtsspezifikation genauer erläutert.	24.01.2007	Adrian Pongrac (ME)
1.2	Überarbeitung des Dokuments laut BSI Review ZK_0433_ASE_01.rtf: Kapitel 1.2, 2 und 6.1 überarbeitet. Version 2.3 der CC benutzt.	09.07.2007	Adrian Pongrac (ME)
1.3	Kapitel 2.1.1, 2.1.2, 2.2 und 6.2 überarbeitet. Kapitel 5.2: Überschriften der Unterkapitel gemäß Tabelle 5-1 korrigiert. Kapitel 9.2 ergänzt.	11.07.2007	Adrian Pongrac (ME)
1.4	Kapitel 2.1.2: S3 korrigiert.	12.07.2007	Adrian Pongrac (ME)
1.5	Bezeichnung TCL100 durch TCL101 ersetzt. Tabelle 2-1 aktualisiert.	18.10.2007	Adrian Pongrac (ME)
1.6	Überarbeitung des Dokuments laut BSI Review ZK_0433_ASE_03.rtf.	04.12.2007	Adrian Pongrac (ME)
1.7	Tabelle 8-7 korrigiert. Tabelle 8.8 neu.	13.12.2007	Adrian Pongrac (ME)
1.8	Kapitel 6.1.2, letzten Abschnitt erweitert.	10.01.2008	Adrian Pongrac (ME)

1 ST-Einführung

Der Evaluationsgegenstand (EVG) ist Teil des Produktes „Veridat Ident, Volumen, Verwiegung 4.0“, bei dem es sich um ein Abfallbehälter-Identifikationssystem handelt, welches spezielle Daten einer Abfallsammeltour erfasst.

Dieses Dokument Sicherheitsvorgaben (SV) stellt die Grundlage zur Evaluierung von Teilen des Produktes „Veridat Ident, Volumen, Verwiegung 4.0“ dar. Für die Bewertung der Sicherheit wird das Schutzprofil Abfallbehälter-Identifikations-Systeme WBIS-PP (Version 1.04) verwendet. Die SV halten sich dabei strikt an dieses Schutzprofil und stellen entsprechende Beschreibungen und Aussagen bezogen auf den EVG zur Verfügung.

1.1 ST Identifikation

Titel:	Veridat Ident, Volumen, Verwiegung 4.0 Sicherheitsvorgaben
EVG:	Veridat Ident, Volumen, Verwiegung 4.0
CC-Version:	The Common Criteria for Information Technology Security Evaluation 2.3, August 2005
PP:	Protection Profile Waste Bin Identification Systems WBIS-PP Version 1.04
Vertrauenswürdigkeitsstufe	EAL1

1.2 ST Übersicht

Der EVG ist ein Abfallbehälter-Identsystem gemäß WBIS-PP. Es ist für den Einbau in Entsorgungsfahrzeuge gedacht, mit dessen Hilfe Abfallbehälter identifiziert und die Anzahl der Leerungen erfasst werden können, um die Leistungserbringung dem jeweiligen Gebührenpflichtigen zuzuordnen und nachzuweisen. Das Produkt kann zusätzlich zu den Identifikationsdaten und dem Zeitstempel, den so genannten Leerungsdatensatz, durch weitere Informationen ergänzen. Das Produkt besitzt hierzu weitere Schnittstellen, so z.B. zum Volumenmess-System, zu einem Wiegesystem (CleANopen), zu einem Positionsbestimmungs-System (GPS), etc., die optional an das System angeschlossen werden können. Die Zusatzsysteme sind nicht Teil des EVG! Die Daten der Zusatzsysteme sind jedoch im Leerungsdatensatz berücksichtigt.

Das Ziel der Sicherheitsvorgaben ist es ein gewisses Maß an Vertrauen in die Funktionalität des Systems zu erreichen. Dabei liegt das Hauptaugenmerk auf dem Schutz und die Unversehrtheit der Entleerungsdaten.

Bezeichnung:	Veridat Ident, Volumen, Verwiegung 4.0
Herstellung u. Entwicklung:	Veridat Eurotech GmbH Daimlerstraße 7 D-72829 Engstingen
Systemintegration:	Mobil Elektronik GmbH Bössingerstrasse 33 D-74243 Langenbeutingen

1.2.1 Darstellungshinweise

Die in Kapitel 5.1 „Funktionale Sicherheitsanforderungen an den EVG“ aufgeführten Familienkomponenten sind dem WBIS-PP entnommen, die wiederum der CC Teil 2 entnommen sind. Diese Komponenten enthalten vorgegebene Texte zur Definition der funktionalen Sicherheitsanforderungen an einen EVG, wobei Textteile als Zuweisung (assignments) oder als Auswahl (selections) gekennzeichnet sind und vom Autor einer PP oder ST formuliert bzw. ausgewählt werden. Diese Textteile werden als Operationen bezeichnet. Es muss durch entsprechende Hervorhebung dieser Operationen klar erkennbar und unterscheidbar sein, was „assignments“ und was „selections“ sind. Alle Operationen der hier aufgeführten Komponenten enthalten nur Zuweisungen. Im WBIS-PP sind diese durch kursive Schriftart dargestellt. In diesen Sicherheitsvorgaben werden die Zuweisungen ***kursiv und in fetter Schriftart*** dargestellt.

1.3 Postulat der Übereinstimmung mit CC

Diese SV erfüllen die Regeln und Vereinbarungen der Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005, Teile 2 und 3.

Der EVG ist Teil 2 erweitert.

Der EVG ist Teil 3 konform und erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe EAL1. Der EVG ist konform zum Schutzprofil "Waste Bin Identification Systems (WBIS-PP)", Version 1.04.

Die SV enthalten und erfüllen alle Sicherheitsaspekte des Protection Profile Waste Bin Identification Systems WBIS-PP, Version 1.04.

2 EVG Beschreibung

2.1 Produkt-Typ

Die folgenden Angaben beziehen sich zunächst allgemein auf das Produkt. Anschließend, nach der Auflistung des Lieferumfangs, folgt die Beschreibung des EVGs, als Teil des Produktes.

Für den Leistungsnachweis eines Entsorgungsunternehmens ist es erforderlich, die notwendigen Daten einer Entsorgungstour erfassen zu können. Hierzu können spezielle Abfall-Behälter-Identifikations-Systeme in die Entsorgungsfahrzeuge als Zusatzausstattung eingebaut werden. Ein solches Identsystem umfasst neben den im Fahrzeug eingebauten Komponenten auch ein Teil-System zur Kennzeichnung der Abfallbehälter in Form von fest am Behälter angebrachten Transpondern, sowie eine spezielle PC-Software als Schnittstelle zwischen den Fahrzeugdaten und den Daten einer beliebigen Bürosoftware.

Da in einem solchen System relativ große Datenmengen anfallen und auf verschiedenen Kommunikationswegen ausgetauscht werden, wird seitens der Kunden (entsorgungspflichtige Körperschaften, Bürger) ein hohes Maß an Vertrauen in die technische Funktionsfähigkeit des Systems vorausgesetzt. Dabei sind die Daten vor Manipulation und Verlust zu schützen.

Das Identsystem „Veridat Ident, Volumen, Verwiegung 4.0“ ist ein solches System und enthält EVG-Komponenten gemäß der Beschreibung im WBIS-PP Version 1.04, und somit entsprechende Funktionen zum Schutz der Anwenderdaten vor Datenverlust und Manipulation.

Der Lieferumfang des Produktes „Veridat Ident, Volumen, Verwiegung 4.0“ besteht in der Basisversion aus folgenden Komponenten:

- **PC-Software** (MEVOS und Bürosoftware) mit Sicherheitsmodul als Schnittstelle zwischen Fahrzeugsoftware und Bürosoftware, zur Installation auf den Bürorechner.
- **Externes Laufwerk** für kontaktlose Speicherkarten (Office-Box) zum Anschluss an den Bürorechner.
- **Fahrzeugrechner** für das Abfallsammelfahrzeug, mit integriertem CF Karten Leser (und diversen Schnittstellen zu Zusatzsystemen wie Volumenmessung, Wiegesystem, GPS-System, usw.)
- **Bedienterminal** für die Fahrerkabine, mit integriertem Laufwerk für kontaktlose Speicherkarten. Das Terminal wird via CAN-Bus mit dem Fahrzeugrechner verbunden.
- **Reader** (wahlweise 2 Typen: TCL101 (125kHz) oder TCL102 (134kHz)), zum Anschluss an den Fahrzeugrechner, inklusive passender Antennen.
- **ID-Tag**s mit den Identifizierungsdaten eines Abfallbehälters (jeweils passend zum Reader)
- **Speichermedien** (CF- und kontaktlose Speicherkarten)

Zum EVG nach WBIS-PP Version 1.04, gehören die Komponenten:

ID-Tag,
Fahrzeugsoftware,
und das Sicherheitsmodul.

Entsprechend dieser Aufteilung, besteht das Produkt „Veridat Ident, Volumen, Verwiegung 4.0“, ebenfalls aus 3 EVG-Komponenten:

ID-Tag:
Transponder V-CNT-125ISO bzw.
Transponder V-CNT-134BDE gemäß ISO 11784/85.

Software des Fahrzeug-Rechnersystems:
Diese ist im Fahrzeugrechner und Bedienterminal (Identsoftware), sowie im Reader (TCL101 bzw. TCL102) enthalten. Gemeinsam bilden sie logisch betrachtet die Fahrzeugsoftware. Da die Fahrzeugsoftware des Produktes weitere Funktionalitäten besitzt, die nicht Teil der Fahrzeugsoftware laut WBIS-PP Version 1.04 sind, ist sie jeweils in 2 Teile getrennt. Somit enthält die Software des Fahrzeug-Rechnersystems einen EVG-Teil (Sicherheitskomponenten ME_VDSC und Reader TCL101 bzw. TCL102) und einen freien Software-Teil. Die diversen Zusatzsysteme des Produktes sind nicht Teil des EVG. Die Daten dieser Zusatzsysteme sind jedoch als dritter Bestandteil AT3 im Leerungsdatensatz AT enthalten.

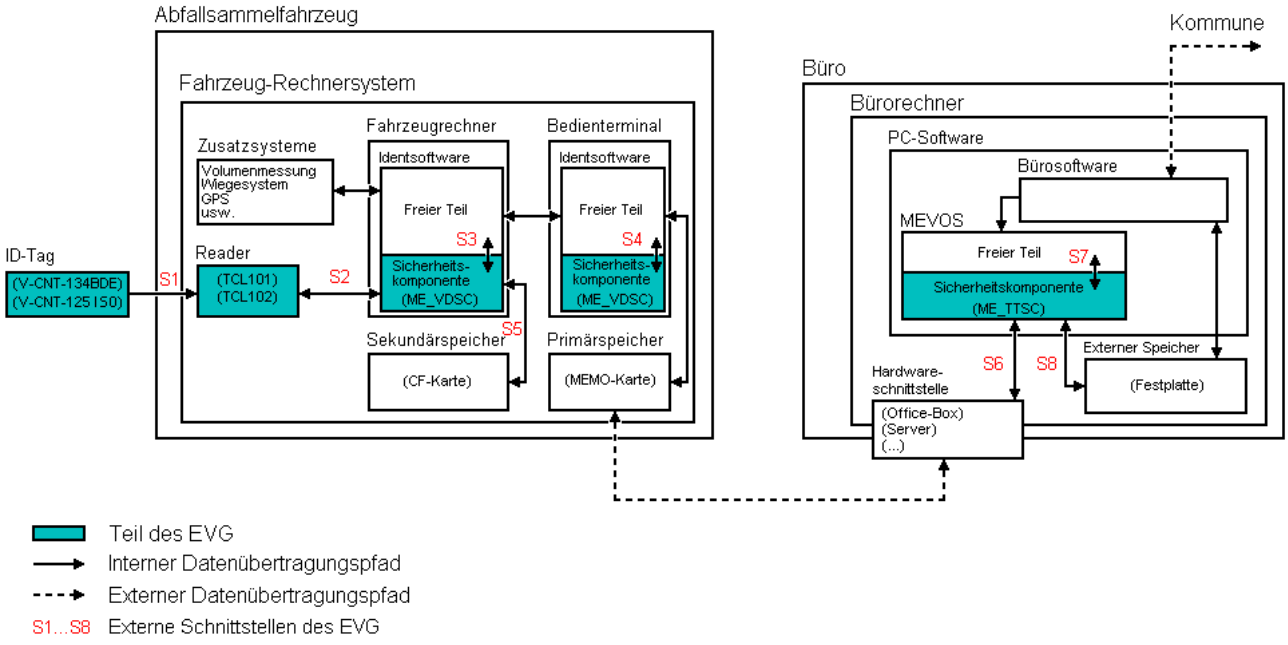
Sicherheitsmodul:
Das Sicherheitsmodul ist ein Teil der PC-Software. Die PC-Software besteht aus der Software MEVOS und der Bürosoftware. Die MEVOS wiederum enthält eine Sicherheitskomponente (ME_TTSC), die das Sicherheitsmodul nach WBIS-PP Version 1.04 darstellt.

2.1.1 EVG Komponenten:

Tabelle 2-1: Komponenten des EVG

Komponente	Bezeichnung	Version
Sicherheitskomponente der PC-Software	ME_TTSC	1.0
Sicherheitskomponente der Fahrzeugsoftware	ME_VDSC	1.0
ID-Tag 1	V-CNT-125ISO	V-CNT-125-0001
ID-Tag 2	V-CNT-134BDE	V-CNT-134-0001
Reader 1	TCL101	EURO I.D. V3.5E
Reader 2	TCL102	ASR V2.22

Abbildung 2-1: Komponenten des EVG



Mit „Interner Datenübertragungspfad“ sind festgelegte Wege des Datentransports gemeint, die lokal auf das jeweilige Teilsystem (Abfallsammelfahrzeug bzw. Büro) begrenzt sind.

Mit „Externer Datenübertragungspfad“ sind nicht festgelegte, änderbare Wege des Datentransports gemeint. Sie sind prinzipiell beliebig. Der Datentransport kann z.B. durch persönliches Überbringen des Primärspeichers (kontaktlose Speicherkarte) oder mittels drahtloser Übertragungsformen, bei dem die Daten auf den Speichern (Primärspeicher – Externer Speicher) ausgetauscht werden, realisiert sein.

Die Sicherheitskomponente ME_TTSC entspricht dem im WBIS-PP Version 1.04 dargestellten Sicherheitsmodul.

Die Sicherheitskomponente ME_VDSC und die Software des Readers TCL101 bzw. TCL102, bilden zusammen die Fahrzeugsoftware, entsprechend der dargestellten Fahrzeugsoftware im WBIS-PP Version 1.04. Die Sicherheitskomponente im Fahrzeugrechner entspricht der Sicherheitskomponente im Bedienterminal (enthalten also identische Funktionen, wobei sie durch verschieden angebundene Datenübertragungspfade logischerweise nicht den identischen Funktionsumfang ermöglichen bzw. benötigen).

Der ID-Tag V-CNT-125ISO bzw. V-CNT-134BDE entspricht dem ID-Tag gemäß WBIS-PP Version 1.04.

2.1.2 Schnittstellen des EVG:

Bezeichnung	Schnittstelle	Beschreibung
S1	Schnittstelle zwischen ID-Tag und Reader	Diese Schnittstelle ist unidirektional. Es können nur Daten des ID-Tag an den Reader gesendet werden, nicht umgekehrt. Die Daten sind CRC geschützt.
S2	Schnittstelle zwischen Reader und Fahrzeugrechner	Diese Schnittstelle ist bidirektional. Hier erfolgt der Datenaustausch zwischen dem Reader und dem Fahrzeugrechner. Der Fahrzeugrechner steuert den Reader. Der Reader sendet die angeforderten Daten. Der Datenaustausch ist durch CRC oder Prüfsummen geschützt.
S3	Schnittstelle zwischen dem EVG-Teil der Fahrzeugsoftware und dem freien Teil der Fahrzeugsoftware (auf Seiten des Fahrzeugrechners)	Diese Schnittstelle ist bidirektional. Zum Einen gelangen hier Daten der optionalen Zusatzsysteme in die Sicherheitskomponente des Fahrzeugrechners. Zum Anderen gelangen hier die mittels CRC geschützten Leerungsdatensätze AT und Leerungsdatenblöcke AT+ zur Übertragung zum Primär- und Sekundärspeicher. Bei letzterem Fall handelt es sich um eine reine Treiberschnittstelle.
S4	Schnittstelle zwischen dem EVG-Teil der Fahrzeugsoftware und dem freien Teil der Fahrzeugsoftware (auf Seiten des Bedienterminals)	Diese Schnittstelle ist bidirektional. Sie kann im Falle des Ausfalls des Fahrzeugrechners einen Teil der Funktionalität der Sicherheitskomponente des Fahrzeugrechners übernehmen. Es handelt sich hier um eine reine Treiberschnittstelle.
S5	Schnittstelle zwischen dem EVG-Teil der Fahrzeugsoftware und dem Sekundärspeicher	Diese Schnittstelle ist bidirektional. Dabei wird der über die Schnittstelle erhaltene Leerungsdatensatz AT, welcher mit einem CRC-Wert vom EVG-Teil versehen wurde, auf dem Sekundärspeicher abgespeichert.
S6	Schnittstelle zwischen der Hardwareschnittstelle und dem EVG-Teil der MEVOS Software	Diese Schnittstelle ist bidirektional. Hier werden die CRC geschützten Tourberichte (Leerungsdatensätze AT und Leerungsdatenblöcke AT+) und Tourpläne ausgetauscht.
S7	Schnittstelle zwischen dem EVG-Teil und dem freien Teil der MEVOS Software	Diese Schnittstelle ist bidirektional. Hiermit werden Steuerbefehle an den EVG-Teil übergeben und Informationsmeldungen an den freien Teil der Software zurückgeliefert.
S8	Schnittstelle zwischen dem EVG-Teil der MEVOS Software und dem externen Speicher	Diese Schnittstelle ist bidirektional. Der geprüfte Leerungsdatenblock AT+ (Tourbericht) wird bei korrektem CRC-Wert auf dem externen Speicher abgelegt und somit der Bürosoftware zur Verfügung gestellt. Ein auf dem externen Speicher, von der Bürosoftware bereitgestellter Tourplan, gelangt hierüber zum EVG-Teil.

2.1.3 Hardwarevorrausetzungen

Transponder 125kHz:

Readertyp:	TCL 101 (im Lieferumfang enthalten)
Hersteller:	pts Technology & Systems GmbH
Beschreibung:	Mit dem Lesegerät TCL 101 können nur PSK/Trovan-RO-Transponder ausgelesen werden. Da es für den Einsatz auf Entsorgungssammelfahrzeugen konzipiert wurde, ist abweichend von den üblichen Aufbaukonzepten, die Antennentreiberelektronik bereits im Gehäuse integriert. An das Lesegerät lassen sich speziell für diese Anwendung entwickelten passive Zahn- und Stabantennen anschließen. Zusätzlich zu der bereits im Decoder vorhandenen Überwachung der Antennenfunktion, wurde eine unabhängige, auch während des Lesevorgangs aktive, Überwachung der Antennenleistung realisiert. Die Ansteuerung der Lesevorgänge erfolgt über die RS232-Schnittstelle.

Transponder 134kHz:

Readertyp:	TCL 102 (im Lieferumfang enthalten)
Hersteller:	pts Technology & Systems GmbH
Beschreibung:	Mit dem Lesegerät TCL 102 können BDE-konforme RO-Transponder ausgelesen werden. Das Lesegerät ist für den Einsatz auf Entsorgungssammelfahrzeugen konzipiert und besitzt eine bereits im Gehäuse integrierte Antennentreiberelektronik. An das Lesegerät lassen sich speziell für diese Anwendung entwickelten passive Zahn- und Stabantennen anschließen. Zusätzlich zu der bereits im Decoder vorhandenen Überwachung der Antennenfunktion, wurde eine unabhängige, auch während des Lesevorgangs aktive, Überwachung der Antennenleistung realisiert. Die Ansteuerung der Lesevorgänge erfolgt über die RS232-Schnittstelle.

Fahrzeugsoftware:

Fahrzeugrechner:	DSE 055 301 (im Lieferumfang enthalten)
Hersteller:	Mobil Elektronik GmbH
Beschreibung:	Mobiltaugliche Datenerfassungs- und Steuerelektronik für den Einsatz als Datenlogger in Problemfahrzeugen, Datenlogger für Feldversuchsbegleitung, Langzeitdatenlogger als Unfallrecorder, Programmiertool, Gateway, Bordcomputer für Identsysteme etc. Die Speicherung der Daten erfolgt auf handelsüblichen Compact-Flash Karten. Als Schnittstellen stehen diverse Ein-/Ausgänge, 2 x CAN-Bus und RS232C zur Verfügung.
Bedienterminal:	EEA 092 704 (im Lieferumfang enthalten)
Hersteller:	Mobil Elektronik GmbH
Beschreibung:	Mobiltaugliche Anzeige- und Bedieneinheit mit 16 Tasten und LCD Grafikdisplay mit 240x64 Pixel und Hintergrundbeleuchtung. Integriertes Laufwerk für kontaktlose Speicherkarten und diverse Schnittstellen (Ein-/Ausgänge, 1 x CAN-BUS, RS232C).

PC-Software:

Hardware:	IBM-kompatibler PC mit paralleler oder serieller Schnittstelle. Windows 95/98/ME/NT/2000/XP (im Lieferumfang nicht enthalten) und ein externes Laufwerk für kontaktlose Speicherkarten (Office-Box, im Lieferumfang enthalten).

2.2 Allgemeine Funktionalität

Jede Entsorgungstour beginnt mit der Übertragung der Tourdaten. Dabei übergibt die Bürosoftware die entsprechenden Daten (Tourplan) an das Sicherheitsmodul, welches die Daten entsprechend gesichert zur Übertragung an das Fahrzeug zur Verfügung stellt. Vor dem Tourstart werden die übertragenen Tourdaten von der kontaktlosen Speicherkarte im Bedienterminal an den Fahrzeugrechner übertragen und geprüft. Sind die Tourdaten korrekt und unbeschädigt, kann mit der Entsorgungstour begonnen werden.

Die Fahrzeugsoftware ist in der Lage, zwei verschiedene Grundtypen von Transpondern (je nach angeschlossenem Reader), welche seit Jahren in der Entsorgungsbranche im Einsatz sind, auszulesen. Über die an den beiden Liftern angebrachten Antennen bzw. mittels einer Handantenne, können Abfallbehälter während bzw. vor einer Leerung identifiziert werden. Bei den Identifikationsdaten handelt es sich um einen eindeutigen, nicht geheimen, so genannten ID-Tag.

Bei der Übertragung der Transponder-Daten (AT1) sowohl vom Transponder zum Reader, als auch vom Reader zum Fahrzeugrechner, werden Prüfverfahren eingesetzt, die Fehler in der Übertragung erkennen können.

Nachdem ein Behälter erfasst wurde, können je nach Ausstattung des Systems, zu den Behälterdaten ID-Tag (AT1) und Zeitstempel (AT2), weitere Daten (AT3) dem Leerungsdatensatz (AT) hinzugefügt werden. Ist ein Leerungsdatensatz (AT) abgeschlossen (z.B. ein neuer Behälter ist erfasst), wird er umgehend abgespeichert. Dies erfolgt an zwei unterschiedlichen Stellen. Zum Einen auf der CF Karte (Sekundärspeicher) des Fahrzeugrechners und zum Anderen auf der kontaktlose Speicherkarte (Primärspeicher) des Bedienterminals. Jeder einzelne Leerungsdatensatz (AT) wird bei der Speicherung mittels eines Prüfsummenverfahrens geschützt.

Nach Abschluss der Tour, wird der durch einen CRC-Wert geschützte Leerungsdatenblock (AT+), bestehend aus den ebenfalls separat durch einen CRC-Wert geschützten Leerungsdatensätzen (AT), als Tourbericht an das Büro übertragen und dort eingelesen. Dabei überprüft das Sicherheitsmodul die Daten (CRC-Werte) und übergibt sie bei Korrektheit und Unversehrtheit an die Bürosoftware weiter. Zusätzlich ist ein einfaches Nachweisverfahren realisiert, mit dessen Hilfe eine Validierung des Leerungsdatenblockes (AT+) als auch jedes einzelnen Leerungsdatensatzes (AT) erfolgen kann. Hierzu wird dem Leerungsdatenblock (AT+) als auch jedem einzelnen Leerungsdatensatz (AT) die im Fahrzeugrechner hinterlegte Fahrzeug-Identifikation hinzugefügt.

Bei Verlust oder Beschädigung der Daten während der Übertragung zum Büro oder bei Verlust auf dem Bürorechner, können die redundant abgespeicherten Daten auf der CF Karte (Sekundärspeicher) des Fahrzeugrechners abgerufen und erneut zum Büro übertragen werden.

Zusätzlich ist mittels eindeutiger Tourpläne und der eindeutigen Zuordnung von Tourplan zu Tourbericht, das Büro in der Lage, fehlende Berichte zu identifizieren und gezielt (ggf. erneut) anzufordern.

2.3 Art der Nutzung

Im Folgenden werden die Sicherheitsfunktionalitäten des EVG explizit dargestellt. Ziel dieser Funktionen ist es, die Schnittstellen des EVG mit seinen offensichtlichen Schwachstellen und somit die Daten der Anwendung zu schützen.

Tabelle 2-2

Sicherheitsfunktion	Beschreibung
Manipulationsschutz der Identifikationsdaten im ID-Tag	Manipulationen an den Identifikationsdaten (AT1) im ID-Tag werden durch Prüfsummenverfahren abgefangen. Unter Manipulation werden dabei z.B. mechanische Einwirkungen angenommen
Korrekte Identifikation der Abfallbehälter	Durch eindeutige Identifikationsdaten (AT1) und deren Prüfung erfolgt eine korrekte Identifikation von Abfallbehältern.
Manipulationsschutz der Leerungsdatensätze im Fahrzeug	Die im Fahrzeug erzeugten Leerungsdatensätze (AT) werden während der Speicherung und Übertragung im Fahrzeug manipulationsgeschützt. Unter Manipulation wird dabei z.B. eine Störung durch elektromagnetische Strahlung angenommen.
Manipulationsgesicherte Übertragung der Leerungsdatenblöcke (Tourbericht) vom Fahrzeug an die Bürosoftware und Übertragung der Tourdaten (Tourplan) von der Bürosoftware zum Fahrzeug.	Übertragungen der Leerungsdatenblöcke (Tourbericht) bzw. Übertragungen der Tourdaten (Tourplan) außerhalb des Fahrzeugs, werden manipulationsgeschützt. Unter Manipulation wird dabei z.B. eine Störung durch elektromagnetische Strahlung oder die Erzeugung und Übertragung von beliebigen Leerungsdaten an die Bürosoftware angenommen.
Verhinderung von unerkanntem Datenverlust.	Zur Verhinderung von Datenverlusten werden die Leerungsdaten in einem zweiten Speicher vorgehalten. Dieser ist als Ringspeicher ausgeführt. Somit sind die Daten für eine bestimmte Zeit verfügbar. Durch regelmäßige Backups und Prüfung der Daten durch den Benutzer, werden Verluste rechtzeitig erkannt und können mittels des zweiten Speichers wiederhergestellt werden.
Generierung eines Nachweises zur Gültigkeit der Daten.	Eine im Fahrzeugrechner hinterlegte eindeutige Fahrzeug-Identifikation wird als Nachweis zur Gültigkeit der Daten jedem Leerungsdatenblock (AT+) und jedem Leerungsdatensatz (AT) hinzugefügt. Mit Hilfe der im Büro angezeigten Fahrzeug-Identifikation ist die Gültigkeit der Daten und somit ihre Herkunft feststellbar.

3 EVG Sicherheitsumgebung

Dieser Abschnitt dient der formalen Festlegung von Art und Umfang des gewünschten Sicherheitsrahmens bezüglich des EVG.

3.1 Schutzwürdige Objekte, Subjekte und Angreifer

Im folgenden Abschnitt werden die zu schützenden Daten sowie die Anwender und Angreifer des EVG definiert.

Schutzwürdige Objekte

AT Ein Leerungsdatensatz AT zu einer Leerung ist ein schutzwürdiges Objekt in einem WBIS.
Ein Leerungsdatensatz AT besteht aus den Datenfeldern:
AT1 Identifikationsdaten des Abfallbehälters
AT2 Zeitstempel (Datum und Uhrzeit) des Leerungsvorgangs
AT3 Weitere Daten von Zusatzsystemen.

AT+ Bei der Übertragung der Leerungsdatensätze AT von der Fahrzeugsoftware zum Sicherheitsmodul im Büro werden die Leerungsdatensätze zu einem Leerungsdatenblock AT+ zusammengefasst. Der Leerungsdatenblock AT+ ist ein schutzwürdiges Objekt in einem WBIS bei der Kommunikation zwischen der Fahrzeugsoftware und dem Sicherheitsmodul.

(Siehe WBIS-PP, Kapitel 3, Seite 13.)

Subjekte

S.Trusted *Vertrauenswürdige Benutzer*

Besatzung des Fahrzeugs, Benutzer des Bürorechners. Personen, die das System installieren oder warten. Ferner Personen, die für die Sicherheit der Umgebung verantwortlich sind.

(Siehe WBIS-PP, Kapitel 3, Seite 13.)

Angreifer

S.Attack *Angreifer*

Eine Person oder ein für eine Person aktiver Prozess, die sich außerhalb des EVG befinden. Das Hauptziel des Angreifers S.Attack ist es, sensitive Daten der Anwendung zu modifizieren oder zu verfälschen. Der Angreifer verfügt höchstens über Kenntnisse offensichtlicher Schwachstellen.

(Siehe WBIS-PP, Kapitel 3, Seite 13.)

3.2 Annahmen

Im Folgenden werden Annahmen über den Sicherheitsrahmen bzw. die Benutzung des EVG getroffen.

A.Id *ID-Tag*

Das ID-Tag befindet sich fest am Abfallbehälter. Die Identifizierungsdaten (AT1) des Abfallbehälters sind in dem ID-Tag gespeichert. Es werden nur ID-Tags mit einmaligen Identifizierungsdaten installiert. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des EVG sicherzustellen.

(Siehe WBIS-PP, Kapitel 3.1, Seite 14.)

A.Trusted *Vertrauenswürdiges Personal*

Die Besatzung des Fahrzeugs und die Benutzer des Bürorechners (S.Trusted) sind autorisiert und vertrauensvoll. Alle Personen, die das System installieren oder warten sind autorisiert und vertrauenswürdig (S.Trusted). Alle Personen, die für die Sicherheit der Umgebung verantwortlich sind, (S.Trusted) sind autorisiert und vertrauenswürdig.

(Siehe WBIS-PP, Kapitel 3.1, Seite 14.)

A.Access *Zugangsschutz*

Die Umgebung stellt durch geeignete Maßnahmen (Verschluss, Zugangskontrolle durch Passwörter usw.) sicher, dass nur die Benutzer bzw. das Servicepersonal (S.Trusted) den direkten Zugang zu allen Komponenten des Evaluierungsgegenstands, außer zum ID-Tag, haben. Die Beeinflussung der internen Verbindungskanäle durch einen potenziellen Angreifer (S.Attack) innerhalb der IT - Struktur des Bürorechners ist aufgrund geeigneter Maßnahmen ausgeschlossen.

(Siehe WBIS-PP, Kapitel 3.1, Seite 14.)

A.Check *Überprüfung der Vollständigkeit*

Der Benutzer (S.Trusted) prüft in regelmäßigen Abständen, ob alle Leerungsdatenblöcke (AT+) von dem Fahrzeugrechner übertragen worden sind (Vollständigkeit der Übertragungen). Erkannte Datenverluste werden vom Benutzer in einem bestimmten Zeitraum durch erneute Anforderung beim Fahrzeugrechner behoben. Dieser Zeitraum ist konsistent mit der Kapazität des entsprechenden Speichers am Fahrzeugrechner, der zur Speicherung der Leerungsdatenblöcke (AT+) zur Verfügung steht.

(Siehe WBIS-PP, Kapitel 3.1, Seite 14.)

A.Backup *Datensicherung*

Der Benutzer (S.Trusted) sichert die vom EVG erzeugten Daten regelmäßig im Archiv. Der EVG schützt nicht vor Datenverlusten im Archiv.

(Siehe WBIS-PP, Kapitel 3.1, Seite 14.)

A.Installation *Systeminstallation*

Bei Installation, Service oder Wartung des Identifikationssystems wird sichergestellt, dass eine eindeutige Fahrzeug-Identifikation im Fahrzeugrechner hinterlegt wird.

(WBIS-PP erweitert.)

3.3 Bedrohungen

Im Folgenden werden Bedrohungen definiert, gegen die eine Schutzmaßnahme erforderlich wird.

3.3.1 Bedrohungen, denen vom EVG zu begegnen ist

T.Man *Manipulierte Identifikationsdaten*

Ein Angreifer (S.Attack) manipuliert die Identifizierungsdaten (AT1) im ID-Tag durch Mittel (z.B. mechanische Einwirkung), die die Identifizierungsdaten (AT1) ausschließlich rein zufällig verfälschen.

(Siehe WBIS-PP, Kapitel 3.2, Seite 14.)

T.Jam#1 *Gestörte Identifikationsdaten*

Ein Angreifer (S.Attack) stört die Übertragung der Identifizierungsdaten (AT1) vom ID-Tag zum Reader im Fahrzeug durch Mittel (z.B. elektromagnetische Strahlung), die die Identifizierungsdaten (AT1) ausschließlich rein zufällig verfälschen.

(Siehe WBIS-PP, Kapitel 3.2, Seite 15.)

T.Create *Ungültige Leerungsdatensätze*

Ein Angreifer (S.Attack) erzeugt beliebige Leerungsdatenblöcke und überträgt diese an das Sicherheitsmodul.

(Siehe WBIS-PP, Kapitel 3.2, Seite 15.)

T.Jam#2 *Verfälschte Leerungsdatensätze*

Ein Angreifer (S.Attack) verfälscht Leerungsdatensätze (AT) während der Bearbeitung und der Speicherung innerhalb des Fahrzeuges oder stört die Übertragung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul z.B. durch elektromagnetische Strahlung, um Daten der Leerungsdatenblöcke (AT+) ausschließlich rein zufällig zu verfälschen.

(Siehe WBIS-PP, Kapitel 3.2, Seite 15.)

3.3.2 Bedrohungen, denen durch die Umgebung zu begegnen ist

Im WBIS-PP werden keine Bedrohungen definiert, denen durch die Umgebung zu begegnen ist. Zusätzliche Bedrohungen werden in diesen Sicherheitsvorgaben nicht definiert.

3.4 Organisatorische Sicherheitspolitiken

P.Safe *Fehlertoleranz*

Die Fahrzeugsoftware muss sicherstellen, dass die Daten der Leerungsdatenblöcke (AT+) durch eine redundante Speicherung in einem sekundären Speicher so zu schützen sind, dass die Übertragung der Leerungsdatenblöcke von der Fahrzeugsoftware zum Sicherheitsmodul nach einem Verlust der Daten in einem primären Speicher möglich ist.

(Siehe WBIS-PP, Kapitel 3.3, Seite 15.)

4 Sicherheitsziele

Die Sicherheitsziele werden dargestellt als:

- Sicherheitsziele für den EVG
- Sicherheitsziele für die Umgebung

4.1 Sicherheitsziele für den EVG

OT.Inv#1 *Erkennung von ungültigen Identifikationsdaten*

Der EVG muss Manipulationen der Identifikationsdaten (AT1), die im ID-Tag gespeichert sind oder während der Übertragung zwischen ID-Tag und Reader im Fahrzeug, erkennen.

(Siehe WBIS-PP, Kapitel 4.1, Seite 16.)

OT.Inv#2 *Erkennung von ungültigen Leerungsdatensätzen*

Der EVG muss jegliche Versuche der Übertragung von beliebigen (z.B. ungültigen) Leerungsdatenblöcken (AT+) zum Sicherheitsmodul erkennen. Der EVG muss Manipulationen der Leerungsdatensätze (AT) während der Verarbeitung und Speicherung innerhalb des Fahrzeuges und Manipulationen der Leerungsdatenblöcke (AT+) durch zufällige Störungen während der Übertragung von der Fahrzeugsoftware zum Sicherheitsmodul erkennen.

(Siehe WBIS-PP, Kapitel 4.1, Seite 16.)

OT.Safe *Fehlertoleranz*

Als Teil des EVG, muss die Fahrzeugsoftware sicherstellen, dass die Daten der Leerungsdatenblöcke (AT+), durch redundantes Speichern der Daten in einem sekundären Speicher erfolgt, um im Falle eines Verlustes der Leerungsdatenblöcke (AT+) im primären Speicher der Fahrzeugsoftware, hiermit die Übertragung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul möglich ist.

(Siehe WBIS-PP, Kapitel 4.1, Seite 16.)

4.2 Sicherheitsziele für die Umgebung

OE.Id *ID-Tag*

Der ID-Tag befindet sich fest am Abfallbehälter. Die Identifizierungsdaten (AT1) des Abfallbehälters sind in dem ID-Tag gespeichert. Es sind nur ID-Tags mit einmaligen Identifizierungsdaten in Gebrauch. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des EVG sicherzustellen.

(Siehe WBIS-PP, Kapitel 4.2, Seite 16.)

OE.Trusted *Vertrauenswürdiges Personal*

Es muss organisatorisch abgesichert sein, dass die Besatzung des Fahrzeugs und die Benutzer des Bürorechners (S.Trusted) autorisiert und vertrauenswürdig sind. Alle Personen, die das System installieren oder warten, müssen autorisiert und vertrauenswürdig sein (S.Trusted). Alle Personen, die für die Sicherheit der Umgebung verantwortlich sind, (S.Trusted) müssen autorisiert und vertrauenswürdig sein.

(Siehe WBIS-PP, Kapitel 4.2, Seite 16/17.)

OE.Access *Zugangsschutz*

Die Umgebung muss durch geeignete Maßnahmen (Verschluss, Zugangskontrolle durch Passwörter usw.) sicherstellen, dass nur Benutzer bzw. das Servicepersonal (S.Trusted) den direkten Zugang zu allen Komponenten des EVG, außer zum ID-Tag, haben. Die Beeinflussung der internen Verbindungskanäle durch einen potenziellen Angreifer (S.Attack) innerhalb der IT Struktur des Bürorechners muss durch geeignete Maßnahmen ausgeschlossen werden.

(Siehe WBIS-PP, Kapitel 4.2, Seite 17.)

OE.Check *Überprüfung der Vollständigkeit*

Es muss sichergestellt sein, dass der Benutzer (S.Trusted) in regelmäßigen Abständen prüft, ob alle Leerungsdatenblöcke (AT+) von dem Fahrzeugrechner übertragen worden sind. Erkannte Datenverluste müssen vom Benutzer durch wiederholte Anforderung der Daten wiederhergestellt werden. Die Zeiträume müssen konsistent mit der Kapazität des entsprechenden Speichers am Fahrzeugrechner sein.

(Siehe WBIS-PP, Kapitel 4.2, Seite 17.)

OE.Backup *Datensicherung*

Es muss sichergestellt sein, dass der Benutzer (S.Trusted) regelmäßig Kopien von den vom EVG erzeugten Daten anlegt.

(Siehe WBIS-PP, Kapitel 4.2, Seite 17.)

OE.Installation *Systeminstallation*

Bei Installation, Service oder Wartung des Identifikationssystems muss sichergestellt sein, dass eine eindeutige Fahrzeug-Identifikation im Fahrzeugrechner hinterlegt ist.

(WBIS-PP erweitert.)

5 IT Sicherheitsanforderungen

Die IT Sicherheitsanforderungen werden beschrieben durch die

- funktionalen Sicherheitsanforderungen an den EVG, beschrieben in Kapitel 5.1
- Anforderungen an die Vertrauenswürdigkeit des EVG, beschrieben in Kapitel 5.2
- Sicherheitsanforderungen an die IT Umgebung, beschrieben in Kapitel 5.3
- Sicherheitsanforderungen an die nicht IT Umgebung, beschrieben in Kapitel 5.4

5.1 Funktionale Sicherheitsanforderungen an den EVG

Die funktionalen Sicherheitsanforderungen an den EVG werden beschrieben durch die Klassenfamilien:

- FDP_DAU Datenauthentisierung (Kapitel 5.1.1),
- FDP_ITT EVG-interner Transfer (Kapitel 5.1.2),
- FDP_SDI Integrität der gespeicherten Daten (Kapitel 5.1.3),
- FRU_FLT Fehlertoleranz (Kapitel 5.1.4).

Sämtliche funktionalen Sicherheitsanforderungen sind aus dem WBIS-PP entnommen und wurden nicht ergänzt.

5.1.1 Einfache Datenauthentisierung (FDP_DAU.1)

FDP_DAU.1.1 Die TSF müssen die Fähigkeit zur Generierung von Nachweisen als Gültigkeitsgarantie von ***Leerungsdatensätzen AT und Leerungsdatenblöcken AT+*** bereitstellen.
(Siehe auch WBIS-PP, Kapitel 5.1.1.1, Seite 18.)

FDP_DAU.1.2 Die TSF müssen ***Benutzern (S.Trusted)*** die Fähigkeit zur Verifizierung des Gültigkeitsnachweises der angezeigten Information bereitstellen.
(Siehe WBIS-PP, Kapitel 5.1.1.1, Seite 18.)

5.1.2 EVG-interner Transfer (FDP_ITT)

Der Anforderung EVG-interner Transfer wird beschrieben durch die Familienkomponente FDP_ITT.5 Schutz der Integrität des internen Transfers in Kapitel 5.1.2.1. Die Common Criteria Teil 2 ist an dieser Stelle um eine fünfte Komponente erweitert (siehe WBIS-PP Kapitel 5.1.2.1, Seite 18, sowie Kapitel 6.4, Seite 26 und Kapitel 9, Seite 36).

5.1.2.1 Schutz der Integrität des internen Transfers (FDP_ITT.5) (CC Teil 2 erweitert)

FDP_ITT.5.1 Die TSF müssen die ***Datenintegritätspolitik*** durchsetzen, um Modifizierung von Benutzerdaten zu verhindern, wenn diese zwischen materiell getrennten Teilen des TOE (EVG) übertragen werden.
(Siehe WBIS-PP, Kapitel 5.1.2.1, Seite 18.)

Die folgende Sicherheitsfunktionspolitik (SFP) **Datenintegritätspolitik,** wird als Anforderung an „Schutz der Integrität des internen Transfers (FDP_ITT.5)“ definiert: Die Benutzerdaten (AT1 und AT+) müssen zur Aufrechterhaltung ihrer Integrität geschützt werden.

5.1.3 Integrität der gespeicherten Daten (FDP_SDI)

Die Anforderung Integrität der gespeicherten Daten wird beschrieben durch die Familienkomponente FDP_SDI.1 Überwachung der Integrität gespeicherter Daten in Kapitel 5.1.3.1.

5.1.3.1 Überwachung der Integrität gespeicherter Daten (FDP_SDI.1)

FDP_SDI.1.1 Die TSF müssen die innerhalb des TSC gespeicherten Benutzerdaten auf ***zufällige Verfälschung*** bei allen Objekten auf Basis folgender Attribute: ***Identifikationsdaten AT1 innerhalb der Identifikationseinheit und Leerungsdaten AT während der Speicherung innerhalb des Fahrzeugs*** überwachen.
(Siehe WBIS-PP, Kapitel 5.1.3.1, Seite 19.)

5.1.4 Fehlertoleranz (FRU_FLT)

Die Anforderung Fehlertoleranz, wird beschrieben durch die Familienkomponente FDP_FLT.1 Überwachung der Integrität gespeicherter Daten in Kapitel 5.1.4.1.

5.1.4.1 Verminderte Fehlertoleranz (FRU_FLT.1)

FRU_FLT.1.1 Die TSF müssen den Betrieb von ***Transfer der Leerungsdatenblöcke (AT+), von der Fahrzeugsoftware zum Sicherheitsmodul, mit Hilfe der gespeicherten Daten im Sekundärspeicher*** sicherstellen, wenn die folgenden Fehler auftreten: ***Verlust der Anwender Daten im Primärspeicher der Fahrzeugsoftware***.
(Siehe WBIS-PP, Kapitel 5.1.4.1, Seite 19.)

5.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Eine Tabelle mit den Klassen und Komponenten für die Vertrauenswürdigkeitsstufe EAL1 kann im WBIS-PP, Kapitel 5.2, Seite 19, Table 5.1, nachgeschlagen werden.

Daraus sind die Komponenten mit Anforderungen an die Vertrauenswürdigkeit des EVG entnommen und werden in den nächsten Kapiteln dargestellt.

Tabelle 5-1

Komponente	Komponenten Name
ACM_CAP.1	Versionsnummern
ADO_IGS.1	Installations-, Generierungs- und Anlaufprozeduren
ADV_FSP.1	Informelle, funktionale Spezifikation
ADV_RCR.1	Informeller Nachweis der Übereinstimmung
AGD_ADM.1	Systemverwalterhandbuch
AGD_USR.1	Benutzerhandbuch
ATE_IND.1	Unabhängiges Testen - Übereinstimmung

5.2.1 Konfigurationsmanagement (ACM)

Die Ziele dieser Familie sind u.a. folgende:

a) Sicherstellung der Korrektheit und Vollständigkeit des EVG vor dessen Lieferung an den Konsumenten;
b) Sicherstellung, dass bei der Prüfung und Bewertung keine Konfigurationsteile fehlen;
c) Vermeidung nicht-autorisierter Modifizierungen, Hinzufügungen oder Löschungen von EVG-Konfigurationsteilen.

5.2.1.1 Versionsnummern (ACM_CAP.1)

ACM_CAP.1.1D	Der Entwickler muss einen Verweisnamen für den EVG bereitstellen. (Siehe WBIS-PP, Kapitel 5.2.1.1, Seite 19.)
ACM_CAP.1.1C	Der Verweisname für den EVG muss für jede Version des EVG eindeutig sein. (Siehe WBIS-PP, Kapitel 5.2.1.1, Seite 19.)
ACM_CAP.1.2C	Der EVG muss mit seinem Verweisnamen gekennzeichnet sein. (Siehe WBIS-PP, Kapitel 5.2.1.1, Seite 20.)

5.2.2 Auslieferung und Betrieb (ADO)

Auslieferung und Betrieb enthält Anforderungen an die korrekte Auslieferung, Installation, Generierung und den Anlauf des EVG.

5.2.2.1 Installations-, Generierungs- und Anlaufprozeduren (ADO_IGS.1)

ADO_IGS.1.1D	Der Entwickler muss die für die sichere Installation und Generierung sowie den sicheren Ablauf des EVG erforderlichen Prozeduren dokumentieren. (Siehe WBIS-PP, Kapitel 5.2.1.1, Seite 20.)
ADO_IGS.1.1C	Die Dokumentation muss die für die sichere Installation und Generierung sowie die für den sicheren Ablauf des EVG erforderlichen Schritte beschreiben. (Siehe WBIS-PP, Kapitel 5.2.1.1, Seite 20.)

5.2.3 Entwicklung (ADV)

5.2.3.1 Informelle, funktionale Spezifikation (ADV_FSP.1)

ADV_FSP.1.1D	Der Entwickler muss eine funktionale Spezifikation bereitstellen. (Siehe WBIS-PP, Kapitel 5.2.3.1, Seite 20.)
ADV_FSP.1.1C	Die funktionale Spezifikation muss die TSF und ihre externen Schnittstellen in einem informellen Stil beschreiben. (Siehe WBIS-PP, Kapitel 5.2.3.1, Seite 20.)
ADV_FSP.1.2C	Die funktionale Spezifikation muss in sich konsistent sein. (Siehe WBIS-PP, Kapitel 5.2.3.1, Seite 20.)
ADV_FSP.1.3C	Die funktionale Spezifikation muss den Zweck und die Methode des Gebrauchs aller externen TSF Schnittstellen beschreiben, einschließlich der Details der Wirkungen, Ausnahmen und Fehlermeldungen, wie jeweils angemessen. (Siehe WBIS-PP, Kapitel 5.2.3.1, Seite 20.)
ADV_FSP.1.4C	Die funktionale Spezifikation muss die TSF vollständig Darstellen. (Siehe WBIS-PP, Kapitel 5.2.3.1, Seite 20.)

5.2.3.2 Informeller Nachweis der Übereinstimmung (ADV_RCR.1)

ADV_RCR.1.1D	Der Entwickler muss eine Analyse der Übereinstimmung aller benachbarten Paare der bereitgestellten TSF Darstellungen bereitstellen. (Siehe WBIS-PP, Kapitel 5.2.3.2, Seite 20.)
ADV_RCR.1.1C	Die Analyse muss für jedes Paar benachbarter TSF-Darstellungen nachweisen, dass die gesamte relevante Sicherheitsfunktionalität der abstrakteren TSF Darstellung in der weniger abstrakten TSF Darstellung korrekt und vollständig verfeinert wurde. (Siehe WBIS-PP, Kapitel 5.2.3.2, Seite 20.)

5.2.4 Handbücher (AGD)

Die Klasse Handbücher stellen die Anforderungen an die Benutzer- und Systemverwalterhandbücher bereit. Für eine sichere Verwaltung und einen sicheren Gebrauch des EVG ist es notwendig, alle für die sichere Anwendung des EVG relevanten Aspekte zu beschreiben.

5.2.4.1 Systemverwalterhandbuch (AGD_ADM.1)

AGD_ADM.1.1D	Der Entwickler muss ein Systemverwalterhandbuch bereitstellen, das an das für Systemverwaltung zuständige Personal gerichtet ist. (Siehe WBIS-PP, Kapitel 5.2.4.1, Seite 20.)
AGD_ADM.1.1C	Das Systemverwalterhandbuch muss die Systemverwalterfunktionen und Schnittstellen beschreiben, die dem Systemverwalter des EVG zur Verfügung stehen. (Siehe WBIS-PP, Kapitel 5.2.4.1, Seite 20.)
AGD_ADM.1.2C	Das Systemverwalterhandbuch muss beschreiben, wie der EVG auf sichere Art und Weise zu verwalten ist. (Siehe WBIS-PP, Kapitel 5.2.4.1, Seite 21.)
AGD_ADM.1.3C	Das Systemverwalterhandbuch muss Warnungen bezüglich Funktion und Privilegien enthalten, die in einer sicheren Verarbeitungsumgebung kontrolliert werden sollen. (Siehe WBIS-PP, Kapitel 5.2.4.1, Seite 21.)
AGD_ADM.1.4C	Das Systemverwalterhandbuch muss alle Annahmen zum Benutzerverhalten beschreiben, die für den sicheren Betrieb des EVG relevant sind. (Siehe WBIS-PP, Kapitel 5.2.4.1, Seite 21.)
AGD_ADM.1.5C	Das Systemverwalterhandbuch muss alle vom Systemverwalter kontrollierten Sicherheitsparameter beschreiben und dabei, wie jeweils angemessen, sichere Werte angeben. (Siehe WBIS-PP, Kapitel 5.2.4.1, Seite 21.)
AGD_ADM.1.6C	Das Systemverwalterhandbuch muss jede Art von sicherheitsrelevanten Ereignissen bezüglich der auszuführenden Systemverwalterfunktionen beschreiben, einschließlich der Änderungen der Sicherheitseigenschaften von Einheiten, die unter Kontrolle der TSF stehen. (Siehe WBIS-PP, Kapitel 5.2.4.1, Seite 21.)
AGD_ADM.1.7C	Das Systemverwalterhandbuch muss konsistent mit allen anderen für die Prüfung und Bewertung gelieferten Dokumentationen sein. (Siehe WBIS-PP, Kapitel 5.2.4.1, Seite 21.)
AGD_ADM.1.8C	Das Systemverwalterhandbuch muss alle Sicherheitsanforderungen an die IT Umgebung beschreiben, die für den Systemverwalter relevant sind. (Siehe WBIS-PP, Kapitel 5.2.4.1, Seite 21.)

5.2.4.2 Benutzerhandbuch (AGD_USR.1)

AGD_USR.1.1D	Der Entwickler muss ein Benutzerhandbuch bereitstellen. (Siehe WBIS-PP, Kapitel 5.2.4.2, Seite 21.)
AGD_USR.1.1C	Das Benutzerhandbuch muss die Funktionen und Schnittstellen beschreiben, die den Benutzern des TOE (EVG) zur Verfügung stehen, die nicht für Systemverwaltung zuständig sind. (Siehe WBIS-PP, Kapitel 5.2.4.2, Seite 21.)
AGD_USR.1.2C	Das Benutzerhandbuch muss den Gebrauch der vom EVG bereitgestellten Sicherheitsfunktionen, die für den Benutzer zugänglich sind, beschreiben. (Siehe WBIS-PP, Kapitel 5.2.4.2, Seite 21.)
AGD_USR.1.3C	Das Benutzerhandbuch muss Warnungen bezüglich den Benutzern zugänglichen Funktionen und Privilegien enthalten, die in einer sicheren Verarbeitungsumgebung kontrolliert werden sollen. (Siehe WBIS-PP, Kapitel 5.2.4.2, Seite 21.)
AGD_USR.1.4C	Das Benutzerhandbuch muss alle Verantwortlichkeiten des Benutzers klar darstellen, die für den sicheren Betrieb des EVG notwendig sind, einschließlich derjenigen, die mit den in der Darlegung der EVG Sicherheitsumgebung enthaltenen Annahmen zum Benutzerverhalten zusammenhängen. (Siehe WBIS-PP, Kapitel 5.2.4.2, Seite 21.)
AGD_USR.1.5C	Das Benutzerhandbuch muss konsistent mit allen anderen für die Prüfung und Bewertung gelieferten Dokumentationen sein. (Siehe WBIS-PP, Kapitel 5.2.4.2, Seite 21.)
AGD_USR.1.6C	Das Benutzerhandbuch muss alle Sicherheitsanforderungen an die IT Umgebung beschreiben, die für den Benutzer relevant sind. (Siehe WBIS-PP, Kapitel 5.2.4.2, Seite 21.)

5.2.5 Testen (ATE)

Testen hilft nachzuweisen, dass der EVG die funktionalen Sicherheitsanforderungen erfüllt. Testen schafft Vertrauenswürdigkeit, dass der EVG zumindest die funktionalen Sicherheitsanforderungen des EVG erfüllt. Es kann allerdings nicht feststellen, ob der EVG nicht mehr tut, als spezifiziert wurde.

Die Familie Unabhängiges Testen weist Abhängigkeiten von den anderen Familien auf, die Informationen bereitstellen, die zur Unterstützung der Anforderungen notwendig sind. Sie befasst sich aber vorrangig mit den unabhängigen Evaluatoraufgaben.

5.2.5.1 Unabhängiges Testen - Übereinstimmung (ATE_IND.1)

ATE_IND.1.1D	Der Entwickler muss den EVG zum Testen bereitstellen. (Siehe WBIS-PP, Kapitel 5.2.5.1, Seite 22.)
ATE_IND.1.1C	Der EVG muss sich zum Testen eignen. (Siehe WBIS-PP, Kapitel 5.2.5.1, Seite 22.)

5.3 Sicherheitsanforderungen an die IT Umgebung

Der IT Umgebung sind keine Sicherheitsanforderungen auferlegt.

5.4 Sicherheitsanforderungen an die nicht IT Umgebung

R.Id *ID-Tag*

Der Benutzer muss folgendes absichern: Das ID-Tag muss sich fest an dem Abfallbehälter befinden, welcher durch die Identifizierungsdaten, die in dem ID-Tag gespeichert sind, identifiziert werden soll. Die gespeicherten Identifizierungsdaten in den angebrachten ID-Tags sind eindeutig. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen muss organisatorisch außerhalb des EVG sichergestellt werden.

(Siehe WBIS-PP, Kapitel 5.4, Seite 22.)

R.Trusted *Vertrauenswürdiges Personal*

Die Personen, die das Fahrzeug und das Sicherheitsmodul betreiben, installieren und warten müssen autorisiert und vertrauensvoll sein. Alle Personen, die für die Sicherheit der Umgebung verantwortlich sind, müssen autorisiert und vertrauensvoll sein.

(Siehe WBIS-PP, Kapitel 5.4, Seite 22.)

R.Access *Zugangsschutz*

Die Umgebung muss durch geeignete Maßnahmen sicherstellen, dass nur Benutzer bzw. das Servicepersonal den direkten Zugang zu allen Komponenten des EVG haben (außer zum ID-Tag). Die Umgebung muss jede Beeinflussung der internen Datenkanäle innerhalb der IT Struktur des Bürorechners vorbeugen.

(Siehe WBIS-PP, Kapitel 5.4, Seite 22.)

R.Check *Überprüfung der Vollständigkeit*

Der Benutzer muss in regelmäßigen Abständen prüfen, ob die Leerungsdatenblöcke (AT+) vollständig von dem Fahrzeugrechner übertragen worden sind. Der Benutzer muss bei Feststellung von noch nicht übertragenen Daten vom Fahrzeug zum Büro, diese zwecks Wiederherstellung anfordern. Der Zeitraum der Prüfungen und Anforderungen muss konsistent mit der Kapazität des entsprechenden Speichers am Fahrzeugrechner sein, der zur Speicherung der Leerungsdatenblöcke (AT+) zur Verfügung steht.

(Siehe WBIS-PP, Kapitel 5.4, Seite 22.)

R.Backup *Datensicherung*

Der Benutzer (S.Trusted) muss die vom EVG erzeugten Daten regelmäßig in entsprechenden Archiven sichern.

(Siehe WBIS-PP, Kapitel 5.4, Seite 22.)

R.Installation *Systeminstallation*

Das Servicepersonal stellt bei Installation, Service oder Wartung des Identifikationssystems sicher, dass eine eindeutige Fahrzeug-Identifikation im Fahrzeugrechner hinterlegt ist.

(WBIS-PP erweitert.)

6 EVG Übersichtsspezifikation

Dieses Kapitel beschreibt, wie der EVG die definierten Sicherheitsanforderungen bezüglich der funktionalen Sicherheitsanforderungen aus Kapitel 5.1 und den Anforderungen an die Vertrauenswürdigkeit aus Kapitel 5.2 implementiert.

6.1 EVG Sicherheitsfunktionen (TSF)

Die Beschreibung der Sicherheitsfunktionen nimmt die Gliederung des Kapitels 5.1 auf.

6.1.1 Datenauthentisierung (TSF_DAU.1)

TSF_DAU.1.1 Der EVG stellt eine Funktion zur Verfügung, welche einen Nachweis zur Gültigkeit der Leerungsdatensätze AT, als auch der Leerungsdatenblöcke AT+ generiert. Jedem Leerungsdatensatz AT wird die im System hinterlegte, eindeutige Fahrzeug-Identifikation (Fahrgestellnummer, etc.) hinzugefügt. Jeder Leerungsdatenblock AT+ wird ebenfalls mit dieser Fahrzeug-ID gekennzeichnet. Diese Kennzeichnung ist Teil des sogenannten Tourkopfes und wird für jeden einzelnen Leerungsdatenblock AT+ angelegt. Mittels dieser Kennzeichnung ist die Gültigkeit der Daten nachweisbar.

TSF_DAU.1.2 Mit Hilfe der Funktion einen Nachweis zur Gültigkeit zu generieren und anzuzeigen, wird der Anwender befähigt, die Leerungsdatensätze AT, als auch die Leerungsdatenblöcke AT+, zu prüfen. Jeder Leerungsdatensatz AT+ ist mit einem Tourkopf gekennzeichnet und enthält die eindeutige Fahrzeug-Identifikation als Nachweis der Gültigkeit der Daten, sowie weitere Daten wie Tournummer, Tourname, Gültigkeitsdatum, usw., die als sogenannter Tourplan vom Anwender bzw. vom EVG als Tourbericht generiert wurden. Jeder Leerungsdatenblock AT+ wird mit seinem Tourkopf dem Anwender angezeigt. Übertragungsfehler des Leerungsdatenblocks AT+ werden ebenfalls angezeigt. Weiterhin wird jeder einzelne Leerungsdatensatz AT, mit darin enthaltener Fahrzeug-Identifikation als Nachweis der Gültigkeit der Daten, angezeigt.

6.1.2 EVG-interner Transfer (TSF_ITT.5)

TSF_ITT.5.1 Die Anwender Daten AT1 und AT+ (Tourbericht) sowie die Tourpläne werden mittels Prüfsummenverfahren bei allen Transfers zwischen physikalisch getrennten Teilen des EVG geschützt. Der EVG ergänzt zu jedem Leerungsdatenblock AT+, einen über die Daten berechneten Prüfwert, zum Schutz der Integrität. Nachfolgend sind die 3 vorhandenen Transferwege dieser Daten beschrieben.

1. Transfer von AT1 vom ID-Tag zum Reader

Die Daten AT1 und der Prüfwert 1, beide im ID-Tag gespeichert (read only), werden vom Reader ausgelesen, anschließend der Prüfwert 1 über AT1 berechnet und mit dem eingelesenen Prüfwert verglichen. Nur Daten AT1 mit korrektem Prüfwert 1, werden an die Fahrzeugsoftware weitergegeben.

2. Transfer von AT1 vom Reader zur Fahrzeugsoftware

Nach der Lese-Aufforderung durch die Fahrzeugsoftware an den Reader, erfolgt der beschriebene Transfer aus 1. Die Antwort des Readers (ggf. mit AT1) erhält die Fahrzeugsoftware anschließend mit angehängtem Prüfwert 2. Die Fahrzeugsoftware berechnet aus der Antwort den Prüfwert 2 und vergleicht diesen mit dem erhaltenen Prüfwert. Sind die Werte unterschiedlich, so wird ein Lesefehler angezeigt.

3. Transfer von AT+ von der Fahrzeugsoftware zum Sicherheitsmodul

Vor dem Transfer wird über den Leerungsdatenblock AT+ ein Prüfwert 3 berechnet und diesem angehängt. Das Sicherheitsmodul liest den Leerungsdatenblock ein, berechnet den Prüfwert 3 und vergleicht ihn mit dem angehängten Prüfwert. Sind diese Unterschiedlich, so wird der Leerungsdatenblock (Tourbericht) verworfen und eine entsprechende Meldung ausgegeben. Jeder Leerungsdatensatz AT ist ebenfalls mit einem Prüfwert versehen, der im Sicherheitsmodul mit dem dort berechneten Wert verglichen wird. Sind die Werte unterschiedlich, so wird dies gemeldet und der entsprechende Leerungsdatensatz gekennzeichnet.

6.1.3 Integrität der gespeicherten Daten (TSF_SDI.1)

TSF_SDI.1.1. Die Leerungsdatensätze AT werden mittels Prüfsummenverfahren auf zufällige Verfälschung bei der Speicherung überwacht. D.h. die Leerungsdatensätze AT werden mit einem Prüfwert 4 ergänzt und somit überwacht. Die im ID-Tag fest gespeicherten Identifikationsdaten AT1 enthalten einen Prüfwert 1 eines Prüfsummenverfahrens. Mit Hilfe des Prüfwertes 1, werden die Identifikationsdaten AT1, auf zufällige Verfälschung innerhalb des ID-Tags überwacht.

6.1.4 Fehlertoleranz (TSF_FLT.1)

TSF_FLT.1.1 Der EVG verfügt über zwei Hauptdatenspeicher. Den Primärspeicher in Form einer kontaktlosen Speicherkarte im Laufwerk des Bedienterminals und dem Sekundärspeicher in Form einer handelsüblichen Compact Flash Speicherkarte im Laufwerk des Fahrzeugrechners. Die Leerungsdatensätze AT und Leerungsdatenblöcke AT+ werden in beiden Speichern festgehalten. Über das Bedienterminal ist es möglich, im Falle eines Verlustes der Daten aus dem Primärspeicher, die Daten aus dem Sekundärspeicher abzurufen und in den Primärspeicher zu übertragen.

6.2 Maßnahmen zur Vertrauenswürdigkeit

In diesem Abschnitt werden die Maßnahmen bezüglich der Anforderungen an die Vertrauenswürdigkeit des EVG aus Kapitel 5.2 dargestellt.

Tabelle 6-1

Komponente	Maßnahmen
ACM_CAP.1	Jeder EVG ist mit einem Verweisnamen und einer Versionsnummer gekennzeichnet. Die Angaben können über ein frei zugängliches Benutzermenü angezeigt werden.
ADO_IGS.1	Die erforderlichen Prozeduren für die Installation, den Anlauf und den Betrieb des EVG sind im Systemverwalterhandbuch dokumentiert.
ADV_FSP.1	Im Dokument „Funktionale Spezifikation“ werden die sichtbaren TSF Schnittstellen und das Verhalten der TSF beschrieben.
ADV_RCR.1	Im Dokument „Analyse und Vergleich von funktionalen Anforderungen und Sicherheitsfunktionen des EVG“ werden die entsprechenden Übereinstimmungen nachgewiesen.
AGD_ADM.1	Im Systemverwalterhandbuch sind alle für die sichere Verwaltung und den sicheren Betrieb notwendigen Informationen beschrieben.
AGD_USR.1	Im Benutzerhandbuch sind alle für den sicheren Betrieb notwendigen Informationen beschrieben.
ATE_IND.1	Der Entwickler stellt den EVG am entsprechenden Ort und einschließlich benötigter Komponenten für die Evaluation bereit. Die beauftragte Prüfstelle prüft nach ihren Vorgaben bei technischer Unterstützung des Entwicklers.

7 Postulate

7.1 PP Verweis

Die Sicherheitsvorgaben stimmen mit den Anforderungen des WBIS-PP vollständig überein.

Das Schutzprofil „Waste Bin Identification Systems (WBIS-PP)“, Version 1.04 ist in der Liste zertifizierter und registrierter Schutzprofile des BSI enthalten, welche regelmäßig publiziert wird (siehe auch Internet: http://www.bsi.bund.de). Dort ist auch das PP als Download verfügbar.

7.2 PP Anpassung

Das Schutzprofil WBIS-PP wurde in diesen Sicherheitsvorgaben um A.Installation (Kapitel 3.2), OE.Installation (Kapitel 4.2) und R.Installation (Kapitel 5.4) erweitert.

7.3 PP Ergänzungen

Das Schutzprofil WBIS-PP wurde in diesen Sicherheitsvorgaben um A.Installation (Kapitel 3.2), OE.Installation (Kapitel 4.2) und R.Installation (Kapitel 5.4) erweitert.

8 Erklärung

Dieses Kapitel stellt den Nachweis zur Prüfung und Bewertung der Sicherheitsvorgaben dar.

8.1 Erklärung zu den Sicherheitszielen

Die Erklärung soll zeigen, dass die festgelegten Sicherheitsziele (Kapitel 4), die Annahmen, Politiken und Bedrohungen aus der EVG Sicherheitsumgebung (Kapitel 3), abdecken und erfüllen.

Tabelle 8-1

Annahmen	Sicherheitsziele
A.Id	OE.Id Die Annahme stellt sicher, dass der ID-Tag am Abfallbehälter befestigt ist und das die installierten ID-Tags eindeutig sind. Die Zuordnung der Identifikationsdaten zum Gebührenpflichtigen ist organisatorisch bewerkstelligt. Da das Sicherheitsziel exakt das gleiche aussagt, genügt es der Annahme.
A.Trusted	OE.Trusted Die Annahme stellt sicher, dass alle Subjekte (außer der Angreifer) vertrauensvoll sind. Da das Sicherheitsziel exakt das gleiche aussagt, genügt es der Annahme.
A.Access	OE.Access Die Annahme stellt sicher, dass der Zugang zum EVG, außer zum ID-Tag, begrenzt auf vertrauensvolles Personal beschränkt ist. Es schließt die Möglichkeit derBeeinflussung interner Kommunikationskanäle innerhalb der IT Struktur des Bürorechners aus. Da das Sicherheitsziel exakt das gleiche aussagt, genügt es der Annahme.
A.Check	OE.Check Die Annahme stellt sicher, dass der Bediener die Vollständigkeit der übertragenen Daten vom Fahrzeug zum Büro überprüft. Erkannte Datenverluste werden durch erneute Anforderung wiederhergestellt. Der Zeitraum der Überprüfung ist konsistent mit der Größe des entsprechenden Speichers des Fahrzeugrechners. Da das Sicherheitsziel exakt das gleiche aussagt, genügt es der Annahme.
A.Backup	OE.Backup Die Annahme stellt sicher, dass der Anwender die durch den EVG erzeugten Daten regelmäßig als Kopie sichert, da der EVG eine solche Funktionalität nicht zur Verfügung stellt. Da das Sicherheitsziel exakt das gleiche aussagt, genügt es der Annahme.
A.Installation	OE.Installation Die Annahme stellt sicher, dass bei Installation, Service oder Wartung des Identifikationssystems eine eindeutige Fahrzeug-Identifikation im Fahrzeugrechner hinterlegt ist. Da das Sicherheitsziel exakt das gleiche aussagt, genügt es der Annahme.

Tabelle 8-2

Politiken	Sicherheitsziele
P.Safe	OT.Safe Die Politik legt die Verfügbarkeit der Übertragung von Leerungsdatenblöcken (AT+) zwischen der Fahrzeugsoftware und dem Sicherheitsmodul fest, im Falle eines Datenverlustes im primären Speicher der Fahrzeugsoftware durch Halten der Daten in einem sekundären Speicher. Da das Sicherheitsziel exakt das gleiche aussagt, genügt es der Politik.

Tabelle 8-3

Bedrohungen	Sicherheitsziele
T.Man	OT.Inv#1 Die Bedrohung befasst sich mit Angriffen, bei denen die Identifikationsdaten (AT1) innerhalb des ID-Tags manipuliert sind. Entsprechend des Sicherheitszieles werden die beschädigten Daten (wie vom Reader nach dem lesen empfangen) vom EVG erkannt, welches der Bedrohung entgegenwirkt.
T.Jam#1	OT.Inv#1 Die Bedrohung befasst sich mit Angriffen, bei dem gestörte Identifikationsdaten (AT1) (durch zufällige Störungen) dem Reader übergeben werden. Entsprechend des Sicherheitszieles werden die gestörten Daten (wie vom Reader nach dem lesen empfangen) vom EVG erkannt, welches der Bedrohung entgegenwirkt.
T.Jam#2	OT.Inv#2 Die Bedrohung behandelt Angriffe, bei denen Leerungsdaten (AT) während der Bearbeitung und Speicherung beschädigt werden oder der Transfer der Leerungsdatenblöcke zum Sicherheitsmodul gestört wird. Entsprechend des Sicherheitszieles werden Beschädigungen während der Bearbeitung und Speicherung der Leerungsdaten und gestörte Transfers der Leerungsdatenblöcke zum Sicherheitsmodul vom EVG erkannt, welches der Bedrohung entgegenwirkt.
T.Create	OT.Inv#2 Die Bedrohung befasst sich mit Angriffen, bei dem willkürliche Leerungsdatensätze erzeugt werden und anschließend an das Sicherheitsmodul übergeben werden. Entsprechend des Sicherheitszieles werden alle Versuche der Übertragung von willkürlichen (z.B. ungültigen) Leerungsdatenblöcken zum Sicherheitsmodul entdeckt, welches der Bedrohung entgegenwirkt.

8.2 Erklärung zu den Sicherheitsanforderungen

Die Erklärung soll zeigen, dass die festgelegten Sicherheitsziele (Kapitel 4), durch die Sicherheitsanforderungen an den EVG und seine Umgebung (Kapitel 5) abdeckt und erfüllt werden.

8.2.1 Erklärung zu den funktionalen Sicherheitsanforderungen des EVG

Tabelle 8-4

Funktionale Sicherheitsziele	Funktionale Sicherheitsanforderungen
OT.Inv#1 Erkennung gestörter Identifikationsdaten	FDP_ITT.5, FDP_SDI.1 Das Sicherheitsziel behandelt die Erkennung von Manipulationen der Identifikationsdaten (AT1) der Leerungsdatensätze (AT) innerhalb des ID-Tags und während der Übertragung vom ID-Tag zur Fahrzeugsoftware, die getrennte Teile des EVG darstellen. Der Schutz der Unversehrtheit der Identifizierungsdaten (AT1), welche im ID-Tag gespeichert sind, wird von FDP_SDI.1 gefordert und wirkt zufälligen Manipulationen der Daten direkt entgegen. Der Schutz der Anwender Daten AT1 zur Absicherung der Unversehrtheit beim Transfer zwischen physikalisch getrennten Teile des EVG, wird durch FDP_ITT.5 gefordert. Die Absicherung der Unversehrtheit schützt direkt gegen die Manipulation der Daten während des Transfers.
OT.Inv#2 Erkennung ungültiger Leerungsdatensätze	FDP_DAU.1, FDP_ITT.5, FDP_SDI.1 Das Sicherheitsziel behandelt die Erkennung von Manipulationen der Leerungsdatenblöcke (AT+), welche zwischen der Fahrzeugsoftware und dem Sicherheitsmodul transferiert werden, die physikalisch getrennte Teile des EVG darstellen. Der Schutz der Anwender Daten AT1 zur Absicherung der Unversehrtheit beim Transfer zwischen physikalisch getrennten Teile des EVG, wird durch FDP_ITT.5 gefordert. Die Absicherung der Unversehrtheit schützt direkt gegen die Manipulation der Daten. Das Sicherheitsziel behandelt ebenso die Erkennung ungültiger Leerungsdaten AT während der Bearbeitung und Speicherung im Fahrzeug und die Manipulation der übertragenen Leerungsdatenblöcke AT+ zum Sicherheitsmodul. Der EVG stellt entsprechend FDP_DAU.1 dem Anwender eine Möglichkeit zu Verfügung, einen Nachweis zu erstellen, um die Gültigkeit der Daten prüfen zu können. Der Schutz der Unversehrtheit der Anwender Daten (AT), die im Fahrzeug gespeichert sind, wird durch FDP_SDI.1 gefordert und wirkt direkt zufälliger Manipulationen entgegen. Die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 unterstützen sich bezüglich Authentizität und Unversehrtheit der Daten gegenseitig. Deshalb decken die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 das Sicherheitsziel ausreichend ab.
OT.Safe Fehlertoleranz	FRU_FLT.1 Das Sicherheitsziel behandelt die Verfügbarkeit der relevanten Daten für den Transfer der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul auch im Falle eines Verlustes der Daten im primären Speicher der Fahrzeugsoftware. Die Funktion dieses Datentransfers mit Hilfe eines sekundären Speichers durch Verlust der Daten im primären Speicher, ist vom EVG entsprechend FRU_FLT.1 umgesetzt.

Tabelle 8-5

Sicherheitsziele Umgebung	Sicherheitsanforderungen Umgebung
OE.Id	R.Id Die Sicherheitsanforderung wird durch das Sicherheitsziel bereitgestellt, da die Sicherheitsanforderung bedingt, was das Ziel von OE.Id festlegt.
OE.Trusted	R.Trusted Die Sicherheitsanforderung wird durch das Sicherheitsziel bereitgestellt, da die Sicherheitsanforderung bedingt, was das Ziel von OE.Trusted festlegt.
OE.Access	R.Access Die Sicherheitsanforderung wird durch das Sicherheitsziel bereitgestellt, da die Sicherheitsanforderung bedingt, was das Ziel von OE.Access festlegt.
OE.Check	R.Check Die Sicherheitsanforderung wird durch das Sicherheitsziel bereitgestellt, da die Sicherheitsanforderung bedingt, was das Ziel von OE.Check festlegt.
OE.Backup	R.Backup Die Sicherheitsanforderung wird durch das Sicherheitsziel bereitgestellt, da die Sicherheitsanforderung bedingt, was das Ziel von OE.Backup festlegt.
OE.Installation	R.Installation Die Sicherheitsanforderung wird durch das Sicherheitsziel bereitgestellt, da die Sicherheitsanforderung bedingt, was das Ziel von OE.Backup festlegt.

8.2.2 Erklärung zu den Anforderungen an die Vertrauenswürdigkeit des EVG

Die Vertrauenswürdigkeitsstufe dieser Sicherheitsvorgaben ist EAL1. Dies entspricht der Stufe im WBIS-PP. Eine höhere Stufe ist nicht erforderlich, da wie im PP erwähnt, das Hauptziel des Produktes die korrekte Funktion und nicht der Schutz der Sicherheit ist und somit die unterste Vertrauenswürdigkeitsstufe ein ausreichendes Vertrauen in das Produkt zur Verfügung stellt, ganz im Gegensatz zu einem nicht evaluierten Produkt.

(Siehe auch WBIS-PP, Kapitel 6.6, Seite 27)

Die Erfüllung der Maßnahmen zur Vertrauenswürdigkeit bezüglich der Anforderungen an die Vertrauenswürdigkeit des EVG ist bereits in Tabelle 6-1 dargestellt. Der geforderte einfache Schutz der Identifikationsdaten, Leerungsdatensätze und Leerungsdatenblöcke, mit der Annahme unbeabsichtigter und rein zufälliger Bedrohungen, sowie der einfachen organisatorischen durchzusetzenden Sicherheitspolitiken, die hauptsächlich vor zufälligen Veränderungen und Verlust der Daten schützen sollen, ermöglichen eine Evaluierung nach der untersten Stufe EAL1, die für den EVG als völlig angemessen und ausreichend anzusehen ist.

8.2.3 Erklärung zu der Anforderung an die Stärke der EVG-Sicherheitsfunktionen

Ein Postulat zur Stärke der EVG-Sicherheitsanforderungen sowie der Stärke der EVG-Sicherheitsfunktionen wird nicht formuliert. Eine Vorgabe seitens der WBIS-PP ist nicht gegeben.

8.2.4 Erklärung zu der gegenseitigen Unterstützung der funktionalen Anforderungen und der Anforderung an die Vertrauenswürdigkeit des EVGs

Die Sicherheitskomponenten sind exakt der Spezifikation der Vertrauenswürdigkeitsstufe EAL1 entnommen. Alle Abhängigkeiten sind somit erfüllt.

Die Abhängigkeiten der funktionalen Anforderungen des EVG und die für die Umgebung sind nicht vollständig erfüllt. Die folgende Abweichung der Abhängigkeit ergibt sich:

FRU_FLT.1 erfordert vom EVG die Absicherung der Funktion Datentransfer von der Fahrzeugsoftware zum Sicherheitsmodul, selbst wenn die Daten in der Fahrzeugsoftware verloren gegangen sind. Diese Anforderung ist angetrieben, die organisatorische Sicherheitspolitik zu erfüllen, was sich mehr auf die Verfügbarkeit der Daten bezieht, als auf die korrekte Funktionsweise der Software und bezieht sich nicht auf einen sicheren Zustand des EVG bezüglich der vom EVG entgegneten Bedrohungen. Da sich die abhängige Komponente FPT_FLS.1 lediglich auf den sicheren Zustand des EVG (z.B. die Software) bezieht, ist sie nicht anwendbar für den EVG.

Die funktionalen Anforderungen FDP_DAU.1, FDP_ITT.5 und FDP_SDI.1 besitzen keine Abhängigkeiten.

Zu den beschriebenen Abhängigkeiten der funktionalen Anforderungen folgende Übersicht.

Tabelle 8-6

Funktionale Anforderung	Abhängigkeiten	Erfüllung
FDP_DAU.1	Keine	Bedingungslos erfüllt.
FDP_ITT.5	Keine	Bedingungslos erfüllt.
FDP_SDI.1	Keine	Bedingungslos erfüllt.
FDP_FLT.1	FDP_FLS.1	Erfüllt, da nicht anwendbar (siehe obige Erläuterung)

(Siehe auch WBIS-PP, Kapitel 6.5, Seite 26/27)

8.3 Erklärung zu der EVG Übersichtsspezifikation

Die Erklärung soll zeigen, dass die aus den Sicherheitszielen (Kapitel 4) abgeleiteten Sicherheitsanforderungen (Kapitel 5) durch entsprechende Sicherheitsfunktionen (Kapitel 6) erfüllt werden.

Tabelle 8-7

Sicherheitsanforderung	Sicherheitsfunktion
FDP_DAU.1.1	TSF_DAU.1.1 Die Sicherheitsfunktion entspricht der Sicherheitsanforderung und erfüllt diese somit vollständig. Durch das Hinzufügen der eindeutigen Fahrzeug-Identifikation zu jedem Leerungsdatenblock AT+ und jedem Leerungsdatensatz AT, erhält der Anwender einen Gültigkeitsnachweis der Daten.
FDP_DAU.1.2	TSF_DAU.1.2 Die Sicherheitsfunktion entspricht der Sicherheitsanforderung und erfüllt diese somit vollständig. Durch die Anzeige der Gültigkeitsnachweise der Leerungsdatenblöcke AT+ und Leerungsdatensätze AT, wird der Anwender befähigt, die Gültigkeit der Daten zu verifizieren.
FDP_ITT.5.1	TSF_ITT.5.1 Die Sicherheitsfunktion entspricht mindestens der Sicherheitsanforderung und erfüllt diese somit vollständig. Die Übertragung von AT1 und AT+ zwischen materiell getrennten Teilen des TOE (EVG) wird grundsätzlich mittels Prüfsummenverfahren geschützt. Zusätzlich werden hier die Daten von AT geprüft und das Ergebnis angezeigt.
FDP_SDI.1.1	TSF_SDI.1.1 Die Sicherheitsfunktion entspricht der Sicherheitsanforderung und erfüllt diese somit vollständig. Zufällige Manipulationen von AT1 innerhalb der Identifikationseinheit werden durch Prüfsummenverfahren während der Übertragung zur Fahrzeugsoftware, sowie durch Prüfung der korrekten Länge der ID überwacht. Zufällige Manipulationen von AT während des Speicherns werden durch Prüfsummenverfahren überwacht.
FRU_FLT.1.1	TSF_FLT.1.1 Die Sicherheitsfunktion entspricht der Sicherheitsanforderung und erfüllt diese somit vollständig. Durch das Vorhandensein eines Primär- und Sekundärspeichers, sowie synchrones Speichern der Leerungsdatensätze AT und der Leerungsdatenblöcke AT+ hierauf, sind die Benutzerdaten vor Verlust im Primärspeicher geschützt.

Die Funktionen TSF_DAU.1.1, TSF_DAU.1.2, TSF_ITT.5.1, TSF_SDI.1.1 und TSF_FLT.1.1 unterstützen sich gegenseitig und wirken so zusammen, dass die Sicherheitsanforderungen an den EVG abgedeckt sind, weil:

- neue Leerungsdatenblöcke AT+ und Leerungsdatensätze AT durch die Funktion TSF_DAU.1.1 (Auslesen der Fahrzeug-Identifikation und hinzufügen zu den Daten) sofort einen Gültigkeitsnachweis erhalten,
- die Identifikationsdaten AT1 durch TSF_SDI.1.1 als unversehrt erkannt werden,
- die Identifikationsdaten AT1 sofort mit einem Zeitstempel AT2 versehen werden und optional mit weiteren Daten AT3 zum Leerungsdatensatz AT ergänzt werden,
- nach Abschluss des Leerungsdatensatzes AT, dieser zum Leerungsdatenblock AT+ hinzugefügt und beide durch TSF_DAU.1.1 mit einer Prüfsumme versehen werden,
- die Leerungsdatensätze AT und Leerungsdatenblöcke AT+ mit TSF_FLT.1.1 redundant im Primär- und Sekundärspeicher abgelegt werden,
- die Datenintegrität von AT und AT+ mittels der durch TSF_DAU.1.1 hinzugefügten Prüfsummen im Sicherheitsmodul der Bürosoftware mit Hilfe von TSF_ITT.5.1 festgestellt und angezeigt wird,
- die Gültigkeit von AT und AT+ mittels der durch TSF_DAU.1.1 hinzugefügte Fahrzeug-Identifikation im Sicherheitsmodul der Bürosoftware mit Hilfe von TSF_ITT.5.1 angezeigt wird.

Somit sind die Sicherheitsanforderungen an den EVG durch die dargestellte gegenseitige Unterstützung und Zusammenwirkung der Sicherheitsfunktionen TSF_DAU.1.1, TSF_DAU.1.2, TSF_ITT.5.1, TSF_SDI.1.1 und TSF_FLT.1.1 erfüllt.

8.3.1 Erklärung der EVG-Sicherheitsmaßnahmen

Die in Kapitel 6.2 formulierten Maßnahmen zur Vertrauenswürdigkeit erfüllen alle in Kapitel 5.2 identifizierten Anforderungen an die Vertrauenswürdigkeit des EVG.

Tabelle 8-8

Anforderung	Maßnahmen des Herstellers
ACM_CAP.1	Die Verweisnamen und Versionsnummern der EVG Komponenten sind in Tabelle 2-1 aufgeführt. Alle EVG Komponenten sind entsprechend und für jede weitere Version eindeutig am Produkt gekennzeichnet.
ADO_IGS.1	Die erforderlichen Prozeduren für die Installation, den Anlauf und den Betrieb des EVG sind im bereitgestellten Systemverwalterhandbuch dokumentiert.
ADV_FSP.1	Im bereitgestellten Dokument „Funktionale Spezifikation“ werden die sichtbaren TSF Schnittstellen und das Verhalten der TSF beschrieben.
ADV_RCR.1	Im bereitgestellten Dokument „Analyse und Vergleich von funktionalen Anforderungen und Sicherheitsfunktionen des EVG“ werden die entsprechenden Übereinstimmungen nachgewiesen.
AGD_ADM.1	Im bereitgestellten Systemverwalterhandbuch sind alle für die sichere Verwaltung und den sicheren Betrieb notwendigen Informationen beschrieben.
AGD_USR.1	Im bereitgestellten Benutzerhandbuch sind alle für den sicheren Betrieb notwendigen Informationen beschrieben.
ATE_IND.1	Der Entwickler stellt den EVG am entsprechenden Ort und einschließlich benötigter Komponenten für die Evaluation bereit. Hiezu ist ein Testaufbau mit allen benötigten Komponenten im Labormaßstab verfügbar. Die beauftragte Prüfstelle prüft nach ihren Vorgaben bei technischer Unterstützung des Entwicklers.

8.4 Erklärung zu den PP Postulate

Da die Sicherheitsvorgaben, abgesehen von den Anpassungen A.Installation (Kapitel 3.2), OE.Installation (Kapitel 4.2) und R.Installation (Kapitel 5.4), keinerlei Ergänzungen zum WBIS-PP enthalten und sich strikt an dieses Profil halten, besteht absolute Konformität zum WBIS-PP.

9 Anhang

9.1 Abkürzungen

BDE	Bundesverband der Deutschen Entsorgungswirtschaft
CC	Common Criteria
CF	Compact Flash
CRC	cyclic redundancy check (Prüfsummenverfahren)
EAL	Evaluation Assurance Level
EVG	Evaluierungsgegenstand (siehe TOE)
ID	Identification
IT	Informationstechnik
ME	Mobil Elektronik GmbH
ME_TTSC	ME-TourdataTransferSecurityComponent
ME_VDSC	ME-VehicleDataSecurityComponent
PC	Personal Computer
PP	Protection Profile (Schutzprofil)
ST	Security target (siehe SV)
SV	Sicherheitsvorgaben (siehe ST)
TOE	Target of evaluation (siehe EVG)
TSF	Sicherheitsfunktion des Evaluierungsgegenstandes (TOE Security Function)
V-CNT-125ISO	Veridat-Chipnesttransponder-125kHz nach ISO
V-CNT-134BDE	Veridat-Chipnesttransponder-134kHz nach BDE
WBIS	Waste Bin Identification System
MEVOS	Mobil Elektronik – Veridat Office Schnittstelle

9.2 Glossar

ID-Tag:

Transponder mit gespeicherten Identifikationsdaten (z.B. Transpondernummer).

Veridat Ident, Volumen, Verwiegung 4.0:

Produktbezeichnung des Herstellers für ein Abfallbehälter-Identifikationssystem.

Tourplan:

Datensatz, der Informationen zu einer geplanten Entsorgungstour enthält (Tourname, Tourdatum, Fahrzeug-ID, Behälterliste etc.). Er muss vor jeder neuen Tour in das Entsorgungsfahrzeug geladen werden. Tourpläne sind immer eindeutig, da sie sich immer auf ein bestimmtes Fahrzeug beziehen, nur dort geladen werden können und zwei identische Tourpläne vom Fahrzeug nicht angenommen werden.

Tourbericht:

Datensatz, der Informationen zu einer durchgeführten Entsorgungstour enthält (Tourname, Tourdatum, Fahrzeug-ID, Leerungsdatenblock AT+, etc.). Damit ist der Tourbericht eindeutig einem Tourplan zugeordnet. Somit sind über das Büro nicht eingeholte Tourberichte, mittels der Tourpläne identifizierbar.

Office-Box:

Laufwerk für kontaktlose Speicherkarten (MEMO-Karte), zum Anschluss an den Bürorechner. Dies erfolgt entweder über den seriellen COM Port oder die parallele Schnittstelle LPT des Rechners.

MEMO-Karte:

Kontaktlose Speicherkarte, die einen Tourplan und einen Tourbericht abspeichert. Somit stellt der Teil der Karte, der den Tourbericht enthält, den Primärspeicher dar.