Verfasser:	Thorsten Bödeker
Organisation:	Envicomp Systemlogistik GmbH
• Auftraggeber:	Envicomp Systemlogistik GmbH
• Prüfstelle:	T-Systems GEI GmbH Prüfstelle IT-Sicherheit Rabinstraße 8, 53111 Bonn
• Zertifizierungsstelle:	Bundesamt für Sicherheit in der Informationstechnik Godesberger Allee 185-189, 53175 Bonn

Zertifizierungskennung:	
• Zu zertifizierendes Objekt:	Envicomp Security System ESS 3.0
• Name des Auftraggebers:	Envicomp Systemlogistik GmbH

Dokumententyp:		
• Dokumententitel	00 90009 Sicherheitsvorgaben ESS 100111	
• Einzelbericht:	Bezug:	.....
• Evaluierungsbericht	Bezug:	.....
• Problembericht	Bezug:	.....
• Review zum		
▪ Prüfbericht	Bezug:	.....
▪ Problembericht	Bezug:	.....
• Meilensteinplan		

Versionsnummer:	3.2
Erstellungsdatum:	10.01.2011
Dateiname:	0090009 Sicherheitsvorgaben ESS100111.doc
Unterschriften	
• Verantwortlich:	
• Abnahme Prüfstelle:	
• Abnahme Zertifizierungsstelle:	

Inhalt

1 ST-Einführung 4
1.1 ST-Identifikation 4
1.2 ST-Übersicht 6
1.3 Postulat der Übereinstimmung mit den CC 7

2 EVG-Beschreibung 8

3 EVG-Sicherheitsumgebung 11
3.1 Subjekte 12
3.2 Angreifer 12
3.3 Annahmen 12
3.4 Bedrohungen 14
3.5 Organisatorische Sicherheitspolitik 14

4 Sicherheitsziele 15
4.1 Sicherheitsziele für den TOE (EVG) 15
4.2 Sicherheitsziele für die Umgebung 16
4.3 Erklärung der Sicherheitsziele 17
4.3.1 Abdeckung der Sicherheitsziele 17
4.3.2 Zulänglichkeit der Sicherheitsziele 18

5 IT-Sicherheitsanforderungen 20
5.1 Funktionale Sicherheitsanforderungen an den TOE (EVG) 20
5.1.1 Datenauthentisierung (FDP_DAU) 20
5.1.2 EVG-interner Transfer (FDP_ITT) 21
5.1.3 Integrität der gespeicherten Daten (FDP_SDI) 21
5.1.4 Fehlertoleranz (FRU_FLT) 21
5.1.5 Hinlänglichkeit der Sicherheitsanforderungen 22
5.2 EVG-Sicherheitsfunktionen 24
5.3 Anforderungen an die Vertrauenswürdigkeit des TOE (EVG) 25
5.3.1 Entwicklung (ADV) 25
5.3.2 Handbücher (AGD) 25
5.3.3 Lebenszyklus-Support (ALC) 26
5.3.4 Testen (ATE) 27
5.3.5 Prüfung der Schwachstellen (AVA_VAN) 27
5.4 Maßnahmen zur Vertrauenswürdigkeit 28
5.4.1 Konfigurations-Management 28
5.4.2 Entwicklung 28
5.4.3 Handbücher 29
5.4.4 Unabhängiges Testen 30
5.5 Sicherheitsanforderungen an die IT-Umgebung 31
5.6 Sicherheitsanforderungen an die Nicht-IT-Umgebung 31
5.7 Erklärung der Sicherheitsanforderungen 33
5.7.1 Abdeckung der Sicherheitsanforderungen 33
5.7.2 Erklärung der Abhängigkeiten 34
5.7.3 Erklärung der Auswahl der EAL-Stufe 34

5.8 Erklärung der PP-Postulate 35
5.9 PP-Verweis 35
5.10 PP-Anpassung 35

Anhang 36
5.11 Abkürzungen 36
5.12 Glossar 38
5.13 Literatur 40
5.14 Transponder 41

1 ST-Einführung

1.1 ST-Identifikation

Das vorliegende Dokument Sicherheitsvorgaben **Envicomp-Security System / Version 3.2**, vom 09.05.2011, Autor Thorsten Bödeker, Envicomp Systemlogistik GmbH, bildet die Sicherheitsvorgaben für den Evaluierungsgegenstand (EVG) „**Envicomp Security System, Version 3.0 (ESS)“** (im weiteren **„ESS 3.0“** genannt) im Zertifizierungsprozess nach der CC-Version 3.1 und Vertrauenswürdigkeitsstufe EAL1, genauer definiert in Abschnitt 5.3, Tabelle 6, erweitert um ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2 zu EAL1+.

Tabelle 1: ESS 3.0 Security Module und Betriebsdokumentation

Nr.	Typ	Bezeichnung	Release	Datum	Auslieferungs-name	Übergabeform
1	Dok	Handbuch „Technischer Benutzer“	V1.0	14.05.2009	0090009 Technischer Benutzer Handbuch	Handbuch
2	Dok	EnviCONVERT Dokumentation	V2.1	12.07.2010	0090009 EnviCONVERT Dokumentation	Handbuch
3	Dok	Handlungsanweisungen	V2.0	06.05.2010	00 90009 Handlungsanweisungen	Dokument
4	Dok	Handbuch BC04	V1.0	25.05.2009	0090009 Handbuch BC04	Handbuch
5	SW	EnviCONVERT	V1.0	09.07.2009	EnviCONVERT Secure V1.0	CD-ROM
6	HW	TAG-Varianten	-	01.03.2009	TAG (siehe Anhang Punkt 5.14, Tag-Varianten)	Hardware
7	HW	IO03	V3.0	01.03.2009	IO03	Hardware
7.1	Sw	Controller SW IO03	455510_0001_0020.bin	09.07.2009	455510_0001_0020.bin	Software

8	HW	Reader Multireader	-	01.03.2009	Multireader 134xx	Hardware
8.1	SW	Reader SW	SR_705 m.bin	-	705m	Software
9	HW	Reader Tiris	Series 2000	-	TI-Reader	Hardware
9.1	SW	Reader SW	1.50.bin	-	1.50	Software
10	HW	Reader TAGSys	P013	-	P013 Reader	Hardware
10.1	SW	Reader SW	LF11776 V2.1	-	V1.6	Software
11	HW	Mikron-Reader (HF-Teil)	RWDDH FE1 M11000 19	-	HF-Teil	Hardware

HW = Hardware, SW = Software, Dok = Dokumentation

Die SW für die Reader (Tiris, Multi, P013 und Mikron) wird vom Lieferanten installiert. Es kann lediglich eine Adresse (Parameter) zugeordnet werden.

Der EVG wird von Envicomp fertig personalisiert installiert und ausgeliefert.

1.2 ST-Übersicht

Der EVG ist das **ESS 3.0**. Dieses ist Bestandteil des Systems **EnviID** / **EnviWeight** , welches im Bereich der Abfallentsorgung und der damit verbundenen Gebührenerhebung eingesetzt wird. Nachfolgend beschrieben sind die Sicherheitsvorgaben des Evaluierungsgegenstandes (EVG) hinsichtlich der Erfassung, Übertragung und Speicherung von Abfallbehälter-Leerungsdaten. Auch wenn der EVG noch weitere Funktionen und Sicherheitsmaßnahmen bereitstellt, so sind diese nicht Gegenstand dieser Evaluierung.

Das **ESS 3.0** ist ein sog. „**Waste Bin Identification System (WBIS)**“, ein Abfallbehälter-Identifikationssystem welches Abfallbehälter mit einem **ID-Tag** (etwa dem Transponder, einem elektronischen Chip) identifiziert und über diesen die zugehörigen Leerungsdaten erfasst. Hierzu gehören etwa die Anzahl der Leerungen des Behälters sowie die Daten des Anwohners. Zu beachten ist, dass das System nur die Abfallbehälter identifiziert, und nicht die eigentlichen Abfälle.
Das Abfallbehälter-Ident-System kann zusätzlich mit einem Wiege- oder Volumenmeßsystem verbunden werden, welches anhand von Leerungsgewicht und –Häufigkeit eine verursacherbezogene Abrechnung ermöglicht.
Individuell abgestimmt auf jeden Kunden, etwa eine Stadt oder Gemeinde, kann so ein modulares System für optimale und vertrauenswürdige Gebührenabrechnung bereit gestellt werden.
Das **ESS 3.0** ist in jeder Phase des Entsorgungsprozesses gegen Datenmanipulation und Datenverlust geschützt und bietet so eine zuverlässige Funktionsfähigkeit im täglichen Einsatz für jede abgerechnete Leerung. Eine verbrauchergerechte und verursacherbezogene Rechnungserstellung durch die jeweiligen entsorgenden Kommunen ist somit seitens der Herstellerfirma jederzeit gewährleistet.
Die Leerungsdatensätze des EBICS-Systems werden an das Sicherheitsmodul des Bürorechners der Entsorgungsfirma übertragen. Nach genauer Prüfung und Validierung durch dieses Sicherheitsmodul **EnviCONVERT** können die Daten danach an die jeweiligen entsorgenden Körperschaften zur Rechnungsstellung übermittelt werden.

1.3 Postulat der Übereinstimmung mit den CC

Die Sicherheitsvorgaben sind

- Konform mit den Common Criteria Version 3.1, Teil 1 (Revision 1, September 2006), und Teil 3 (Revision 2, September 2007)
- Common Criteria Version 3.1 (Revision 2) Teil 2 erweitert
- EAL1 erweitert um ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2
- Konform mit der Evaluierungsmethodologie CEM Version 3.1 (Release 2, September 2007)
- Konform zum Schutzprofil Waste Bin Identification Systems (WBIS-PP) [BSI-PP0010]

2 EVG-Beschreibung

Der EVG, das **ESS 3.0**, besteht aus Teilen des Abfallbehälter-Identifizierungsystems (WBIS) „ESS“ der Envicomp Systemlogistik GmbH.

Das WBIS selber besteht aus folgenden Komponenten:

- **ID-Tag** mit den Identifizierungsdaten des Abfallbehälters
- **Fahrzeug Reader**
- **Fahrzeugrechner IO03** und einem optionalen Wiege-, Volumenmess- oder ähnlichem System. Die **Fahrzeugsoftware** ist installiert auf dem Fahrzeugrechner (**IO03**).
- **Sicherheitsmodul Software EnviCONVERT** auf dem Bürorechner (Bestehend aus der Software EnviCONVERT und beliebigem Ausgabemodul)

Das Ausgabemodul ist für den Betrieb des EVG erforderlich und hat die Aufgabe die Daten dem Benutzer in einer angemessenen Weise anzuzeigen.

Die folgende Abbildung gibt einen Überblick über das **ESS 3.0**:

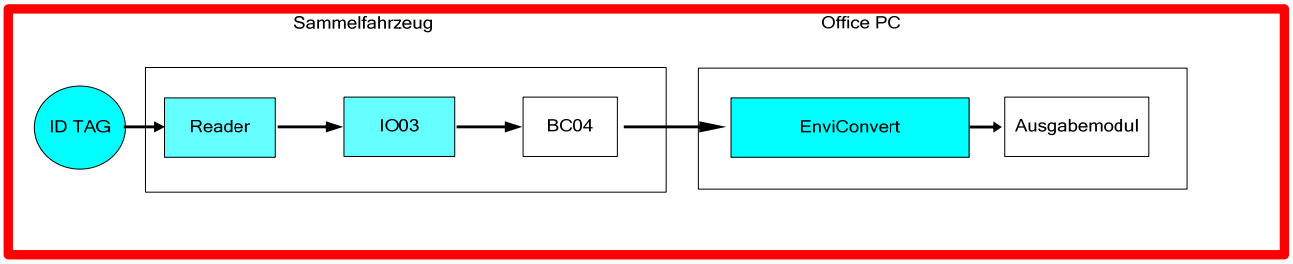

Bild 1: Abfallbehälter-Identifizierungssystem (WBIS)

Die in Bild 1 blau unterlegten Komponenten bilden den EVG. Damit stellt diese Abbildung gleichzeitig die Integration des EVG in das Abfallbehälter-Identifizierungssystem (WBIS) dar. Der BC04 ist als technische Schnittstelle zu betrachten.

Das Abfallbehälter-Identifizierungssystem dient der verursacherbezogenen Abrechnung und Veranlagung der Gebühren der Abfallwirtschaft. Das System kann außer im kommunalen Einsatz zur Gebührenveranlagung auch im privaten und gewerblichen Bereich eingesetzt werden.

Das System bietet die Möglichkeit, die Abrechnung über die Anzahl der Leerungen eines Abfallbehälters durchzuführen. Die Abfallbehälter werden mit einem Datenträger (**ID-Tag**) ausgestattet. Das **ID-Tag** speichert Identifizierungsdaten, die zur Identifizierung des Abfallbehälters herangezogen werden. Diese Daten sind einmalig und nicht vertraulich. Jedem Datensatz ist in der Regel ein Gebührenpflichtiger eindeutig zugeordnet. Die Identifizierungsdaten werden während (bzw. vor/nach) der Leerung eines Abfallbehälters durch den Reader ausgelesen. Die dabei möglichen Übertragungsfehler und eventuelle

Manipulationen werden erkannt. Die Identifizierungsdaten werden dann an die Fahrzeugsoftware weitergeleitet. Optional wird das Gewicht der Abfälle oder der Füllstand der Tonne durch eine entsprechende Sensorik im Fahrzeug ermittelt und parallel zu den Identifizierungsdaten an die Fahrzeugsoftware übermittelt. Die Fahrzeugsoftware ergänzt diese Daten um Datum- und Zeitangaben und bildet daraus einen **Leerungsdatensatz**.

Ein oder mehrere Leerungsdatensätze werden zu einem Leerungsdatenblock zusammengefasst. Es können auf diese Weise alle Leerungsdatensätze einer Tour zu einem **Leerungsdatenblock** zusammengefasst werden.

Die Leerungsdatenblöcke werden an das EnviCONVERT übermittelt welches sich aus der Software selbst und einem beliebigen Ausgabemodul zusammensetzt. Die Fahrzeugsoftware sorgt durch Backup der Daten in einem Speicher dafür, dass die Übermittlung auch nach einem Datenverlust oder nach dem Transport zum **EnviCONVERT** möglich ist. Bei der Übermittlung der Leerungsdatenblöcke an die EnviCONVERT Software wird sichergestellt, dass nur die in einem Fahrzeug des betreffenden Entsorgungsunternehmen erstellten Datenblöcke als gültig erkannt werden. Zusätzlich werden die bei einer Übertragung möglichen Fehler erkannt.

EnviCONVERT gestattet ein Überprüfen der Daten um z.B. weitere denkbare Angriffe (ungültige, kopierte Identifikationsdaten usw.) abzuwehren. Die Leerungsdatensätze, die in den Datenblöcken enthalten sind, oder die Datenblöcke selbst werden an externe Systeme (z.B. bei den Kommunen) zur Abrechnung mit dem Kunden weitergeleitet.

Das **ID-Tag** und die Datenübertragungsstrecke zwischen dem **ID-Tag** und der Fahrzeugsoftware, die im Fahrzeug gespeicherten Daten sowie die Übertragungstrecke zwischen der Fahrzeugsoftware und dem Sicherheitsmodul sind potenziellen Angriffen ausgesetzt. Bei der Betrachtung des Angriffspotenzials muss der potenzielle Wert der zu schützenden Daten in Betracht gezogen werden. Dieser Wert ist als gering zu sehen. Es wird deshalb ein niedriges Angriffpotential angenommen. Der Zugang zu der Fahrzeugsoftware und zum Sicherheitsmodul ist durch geeignete physikalische und organisatorische Maßnahmen nur autorisiertem Personal möglich. Dieser Schutz wird durch das Fahrzeug mit seinen Komponenten und durch das Büro mit dem Bürorechner realisiert.

Abgrenzung des Evaluierungsgegenstandes

Der Evaluierungsgegenstand ist ein Produkt im Sinne der Common Criteria. Der Evaluierungsgegenstand besteht aus dem **ID-Tag**, dem **Reader,** dem **IO03** und der **EnviCONVERT** Software und ist in Bild 2 blau unterlegt. Der Bordcomputer BC04 wird optional von der Firma Envicomp angeboten, gehört jedoch nicht zum EVG, er ist als technische Schnittstelle zu betrachten. Die wichtigsten Schnittstellen des Evaluierungsgegenstand sind folgende (in der Abbildung durch gelbe Rauten gekennzeichnet):

- eine logische interne Schnittstelle vom Tag zum Reader des Fahrzeugs (sicherheitsrelevant)
- eine logische interne Schnittstelle zwischen dem Reader und dem IO03 (sicherheitsrelevant)
- eine interne Schnittstelle zwischen dem IO03 und der Fahrzeugausstattung (nicht sicherheitsrelevant)
- eine externe Schnittstelle zwischen dem IO03 und dem Übertragungskanal (sicherheitsrelevant)
- eine externe Schnittstelle zwischen dem Übertragungskanal und EnviCONVERT (sicherheitsrelevant)
- eine externe Schnittstelle zwischen dem EnviCONVERT und dem Benutzer (sicherheitsrelevant)

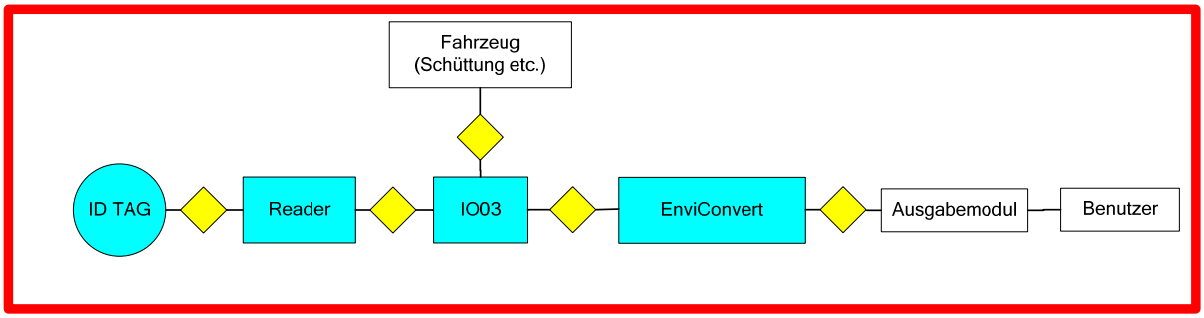

Bild 2: Evaluierungsgegenstand

3 EVG-Sicherheitsumgebung

Der folgende Abschnitt dient der Definition von Art und Umfang der Sicherheitsbedürfnisse, die der EVG adressiert. Daher enthält dieser Abschnitt alle Annahmen an die Umgebung des EVG, die zu schützenden Werte, die bekannten Angreifer und die Bedrohungen, die sie für die Werte darstellen sowie die organisatorischen Sicherheitspolitiken oder Regeln, die der EVG erfüllen muss, um den Sicherheitsbedürfnissen zu genügen.

Im folgenden werden zunächst die Werte, Subjekte und Angreifer definiert.

Schutzwürdige Objekte

AT Ein **Leerungsdatensatz** AT zu einer Leerung ist ein schutzwürdiges Objekt in einem WBIS. Ein Leerungsdatensatz AT besteht aus:

- Fortlaufender Nummer
- Mac des Vorgängerdatensatzes
- **Zeitstempel (AT2)**
- Verweis auf Schüttungsseite
- Verweis Datentyp
- **Status (AT3)**
- TAG-Typ
- **Chipnummer (AT1)**
- **Netto (AT4)**
- Mess-Identifier
- Mess-Signatur
- GPS
- Kilometerstand
- IAC-Code
- **MAC (AT5)**

AT1 Identifikationsdaten des Abfallbehälters

AT2 Zeitstempel (Datum und Uhrzeit) des Leerungsvorgangs.

Der **Leerungsdatensatz** AT entspricht im **ESS 3.0**-System dem **Leerungsdatensatz** und enthält in Übereinstimmung mit der Anwendungsbemerkung 1 des Schutzprofils WBIS-PP weitere zu schützende Datenfelder:

AT3	Statuscode des Leerungsvorganges (Kontrollziffer)
AT4	optional: Nettogewicht der entsorgten Abfälle
AT5	**Prüfsumme**

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.

3.1 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.

3.2 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.

3.3 Annahmen

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 Evaluierungsgegenstandes sicherzustellen.

A.Trusted *Vertrauenswürdiges Personal*

Die Besatzung des Fahrzeugs und die Benutzer des Bürorechners (S.Trusted) sind autorisiert und vertrauenswürdig. 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.

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.

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.

A.Backup *Datensicherung*

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

Hinweis: Für den EVG wird insbesondere angenommen, dass ein Angreifer keine Passwörter des **ESS 3.0**-Systems kennt.

3.4 Bedrohungen

Ein Angreifer nutzt die Schnittstellen des EVG mit dem Ziel Schwachstellen auszunutzen. Dies führt zu einer zunächst nicht näher spezifizierten Kompromittierung der Sicherheit des EVG. Die Bedrohungen adressieren alle Werte.

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.

T.Jam#1 *Gestörte Identifikationsdaten*

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

T.Jam#2 *Verfälschte Leerungsdatensätze und Leerungsdatenblöcke*

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 die Daten der Leerungsdatenblöcke (AT+) ausschließlich rein zufällig zu verfälschen.

T.Create *Ungültige Leerungsdatenblöcke*

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

3.5 Organisatorische Sicherheitspolitik

Die folgende Regel wird für den TOE (EVG) formuliert:

P.Safe *Fehlertoleranz*

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

4 Sicherheitsziele

Dieser Abschnitt identifiziert und definiert die Sicherheitsziele für den TOE (EVG) und seine Umgebung. Sicherheitsziele spiegeln die festgelegte Absicht wider und wirken den identifizierten Bedrohungen entgegen; genauso wie sie der identifizierten organisatorischen Sicherheitspolitik und den Annahmen entsprechen.
Mögliche Bedrohungen sind etwa

- Manipulation an den **Identifikationsdaten** AT1 oder **Leerungsdatenblöcke** AT+ über die am Abfallbehälter angebrachten Transponder (**T.Man**)
- Manipulation der Identifikationsdaten AT1 oder Leerungsdatenblöcke AT+ aufgrund eines Übertragungsfehlers zwischen Transponder und Fahrzeugrechner (**T.Jam**)
- Manipulation der Leerungsdatenblöcke AT+ bei der Übertragung zwischen Fahrzeugsoftware und Sicherheitsmodul des Bürorechners (**T.Jam 2**, **T.Create**)
- Verlust aller Leerungsdatenblöcke AT+ einer Tour durch Verlust oder Beschädigung während der Datenübertragung auf dem Bordrechner (**P.Safe**)

4.1 Sicherheitsziele für den TOE (EVG)

Die Sicherheitsziele für den TOE (EVG) sind exakt dem Schutzprofil WBIS-PP entnommen.

OT.Inv#1 *Erkennung von ungültigen Identifizierungsdaten*

Der TOE (EVG) soll manipulierte Identifizierungsdaten (AT1), die im **ID-Tag** gespeichert sind oder während der Übertragung zwischen **ID-Tag** und dem Reader im Fahrzeug verändert wurden erkennen.

OT.Inv#2 *Erkennung von ungültigen Leerungsdatensätzen*

Der TOE (EVG) soll jeden Versuch, willkürliche **Leerungsdatenblöcke** (AT+) an das Sicherheitsmodul zu übertragen, erkennen. Der TOE (EVG) soll Manipulationen eines **Leerungsdatensatzes** (AT) während der Verarbeitung und Speicherung im Sammelfahrzeug erkennen und Manipulationen von **Leerungsdatenblöcken** (AT+) durch zufällige Störung während der Übertragung vom Sammelfahrzeug an das Sicherheitsmodul erkennen.

OT.Safe *Fehlertoleranz*

Die **Bordrechner-Software**, als ein Teil des TOE (EVG), soll sicherstellen, dass die Daten der **Leerungsdatenblöcke** (AT+) durch eine redundante Speicherung in einem sekundären Speicher in der Art und Weise gesichert werden, dass die Übertragung der **Leerungsdatenblöcke** (AT+) von der **Bordrechner -Software** zum Sicherheitsmodul für den Fall möglich ist, dass **Leerungsdatenblöcke** (AT+) im primären Speicher der **Bordrechner -Software** verloren gegangen sind.

4.2 Sicherheitsziele für die Umgebung

OE.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 benutzt. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des TOE (EVG) sicherzustellen.

OE.Trusted *Vertrauenswürdiges Personal*

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

OE.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 Manipulation der internen Verbindungskanäle durch einen potenziellen Angreifer (S.Attack) innerhalb der IT-Struktur des Bürorechners muss aufgrund ausreichender Maßnahmen ausgeschlossen werden.

OE.Check *Überprüfung der Vollständigkeit*

Der Benutzer (S.Trusted) prüft in regelmäßigen Abständen, ob alle von dem Fahrzeugrechner zum Sicherheitsmodul im Büro übertragenen Daten vollständig sind. Erkannte Datenverluste werden vom Benutzer durch erneute Anforderung beim Fahrzeugrechner behoben. Der Zeitraum muss konsistent mit der Kapazität des entsprechenden Speichers am Fahrzeugrechner sein.

OE.Backup *Datensicherung*

Es soll sichergestellt sein, dass der Benutzer (S.Trusted) Sicherheitskopien der Daten, die vom TOE (EVG) erzeugt wurden, in regelmäßigen Zeitabständen erstellt.

4.3 Erklärung der Sicherheitsziele

4.3.1 Abdeckung der Sicherheitsziele

Tabelle 2: Zuordnung der Sicherheitsziele

Bedrohungen, Annahmen, Politik / Sicherheitsziele	OT. Inv#1	OT. Inv#2	OT. Safe	OE.Id	OE. Trusted	OE. Access	OE. Check	OE. Backup
T.Man	X							
T.Jam#1	X							
T.Create		X						
T.Jam#2		X						
A.Id				X				
A.Trusted					X			
A.Access						X		
A.Check							X	
A.Backup								X
P.Safe			X					

4.3.2 Zulänglichkeit der Sicherheitsziele

4.3.2.1 Politik und Zulänglichkeit der Sicherheitsziele

P.Safe (Fehlertoleranz) begründet die Verfügbarkeit von passenden Daten zur Übertragung von Leerungsdatenblöcke (AT+) von der Bordrechner-Software zum Sicherheitsmodul auch im Falle des Verlustes von diesen Daten in einem Primärspeicher der Bordrechner-Software durch Haltung dieser Daten in einem sekundären Speicher. Dies ist das exakt wiederholte Ziel OT.Safe, so dass dieses Ziel hinlänglich durch P.Safe abgedeckt ist.

4.3.2.2 Bedrohungen und Zulänglichkeit der Sicherheitsziele

T.Man (Manipulierte Identifizierungsdaten) handelt von Angriffen, bei denen die Identifizierungsdaten (AT1) innerhalb der Identifizierungseinheit ID-Tag manipuliert worden sind. Gemäß OT.Inv#1 werden die manipulierten Identifizierungsdaten (nach dem Lesen durch den Reader) durch den TOE erkannt, welcher hierdurch direkt die Bedrohung T.Man abwehrt.

T.Jam#1 (Zerstörte Identifizierungsdaten) handelt von Angriffen, bei denen gestörte Identifizierungsdaten (AT1) (durch zufällige Störung) dem Reader angeboten werden. Gemäß OT.Inv#1 werden die gestörten Identifizierungsdaten (nach dem Lesen durch den Reader) durch den TOE erkannt, welcher hierdurch direkt die Bedrohung T.Jam#1 abwehrt.

T.Create (Ungültige Leerungsdatensätze) handelt von Angriffen, bei denen Leerungsdatensätze willkürlich erzeugt werden und an das Sicherheitsmodul übertragen werden. Gemäß OT.Inv#2 werden jegliche Versuche von willkürlich übertragenen Leerungsdatensätzen (i. Allg. ungültige) an das Sicherheitsmodul erkannt, wodurch direkt der Angriff T.Create abgewehrt wird.

T.Jam#2 (Zerstörte Leerungsdatensätze) handelt von Angriffen, bei denen Leerungsdatensätze (AT) während ihrer Verarbeitung und Speicherung im Sammelfahrzeug zerstört werden oder deren Übertragung zum Sicherheitsmodul gestört wird. Gemäß OT.Inv#2 werden Leerungsdatensätze, deren Verarbeitung und Speicherung im Sammelfahrzeug gestört wird bzw. deren Übertragung zum Sicherheitsmodul gestört wird durch den TOE erkannt, welcher hierdurch die Bedrohung T.Jam#2 direkt abwehrt.

4.3.2.3 Annahmen und Hinlänglichkeit der Sicherheitsziele

A.Id (Identifizierungseinheit ID-Tag) stellt sicher, dass die Identifizierungseinheit am Abfallbehälter befestigt ist den sie identifiziert und dass ihre Daten eindeutig sind. Die Zuordnung zwischen der Identifizierungseinheit und dem Gebührenpflichtigen ist hergestellt durch organisatorische Maßnahmen. Weil das Ziel OE.Id exakt das gleiche bestätigt, ist es hinreichend für A.Id.

A.Trusted (Vertrauenswürdiges Personal) stellt sicher, dass alle Subjekte (mit Ausnahme des Angreifers) autorisiert und vertrauenswürdig sind. Das Ziel OE.Trusted bestätigt genau das Gleiche, so dass es hinlänglich für A.Trusted ist.

A.Access (Zugangsschutz) stellt sicher, dass der Zugang zum TOE (EVG), mit Ausnahme der Identifizierungseinheit, ausschließlich auf autorisiertes und vertrauens-würdiges Personal begrenzt ist. Es schließt auch die Fähigkeiten eines Angreifers aus, den interne Verbindungskanal innerhalb der IT-Struktur des Office-Computers zu beeinflussen. Das Ziel OE.Access bestätigt exakt das Gleiche, so dass es hinlänglich ist für A.Access.

A.Check (Überprüfung der Vollständigkeit) stellt sicher, dass der Benutzer in regelmäßigen Intervallen überprüft, ob die übertragenen Daten vom Sammelfahrzeug zum Büro vollständig sind. Erkannter Verlust von Daten kann wiederhergestellt werden durch wiederholte Übertragung der Daten. Die Intervalle sind konsistent mit der Kapazität des zugehörigen Speichers auf dem Bordrechner des Sammelfahrzeuges. Das Ziel OE.Check bestätigt exakt das Gleiche, so dass es hinlänglich ist für A.Check.

A.Backup (Datensicherung) stellt sicher, daß der Benutzer in regelmäßigen Zeitabständen Sicherheitskopien von den Daten erstellt, die der TOE (EVG) erzeugt hat, weil der TOE (EVG) über keine entsprechende Funktionalität verfügt. Das Ziel OE.Backup bestätigt exakt das Gleiche, so dass es hinlänglich für A.Backup ist.

5 IT-Sicherheitsanforderungen

Dieses Kapitel liefert die funktionalen Sicherheitsanforderungen und die Anforderungen an die Vertrauenswürdigkeit des TOE (EVG) und an dessen Umgebung.

Die Komponenten der funktionalen Sicherheitsanforderungen beschrieben in Abschnitt 5.1 „Funktionale Sicherheitsanforderungen an den TOE (EVG)" wurden von den Common Criteria abgeleitet; mit Ausnahme von der Komponente FDP_ITT.5, die im Schutzprofil [4] definiert worden ist. Die im Schutzprofil ausgeführten Operationen der Zuweisung und der Auswahl sind *kursiv* kenntlich gemacht.

Die Aufstellung der Anforderungen an die Vertrauenswürdigkeit des TOE beschrieben in Abschnitt 5.2 „Anforderungen an die Vertrauenswürdigkeit des TOE" wurde von den Komponenten der Vertrauenswürdigkeit der Common Criteria abgeleitet.

Abschnitt 5.3 identifiziert die IT-Sicherheitsanforderungen, die durch die IT-Umgebung einzuhalten sind.

Die Sicherheitsanforderungen an die Nicht-IT-Umgebung sind in Abschnitt 5.4 beschrieben.

5.1 Funktionale Sicherheitsanforderungen an den TOE (EVG)

5.1.1 Datenauthentisierung (FDP_DAU)

5.1.1.1 Einfache Datenauthentisierung (FDP_DAU.1)

FDP_DAU.1.1 Die TSF müssen die Fähigkeit zur Generierung von Nachweisen als Gültigkeitsgarantie von *Leerungsdatensätzen (AT) und Leerungs-datenblöcken (AT+)* bereitstellen.

FDP_DAU.1.2 Die TSF müssen *den Benutzern (S.Trusted)* die Fähigkeit zur Verifizierung des Gültigkeitsnachweises der angezeigten Information bereitstellen.

5.1.2 EVG-interner Transfer (FDP_ITT)

5.1.2.1 Integrität der internen Übertragung (FDP_ITT.5)

(Der Teil 2 der Common Criteria wurde im zugrunde liegenden Schutzprofil erweitert.)

FDP_ITT.5.1 Die TSF sollen die Einhaltung der *Datenintegritäts-Politik* erzwingen, um die Modifizierung der Benutzerdaten zu verhindern, wenn diese zwischen physisch getrennten Teilen des TOE (EVG) übertragen werden.

Die folgende Politik der Sicherheitsfunktionen (SFP) **Datenintegritäts-Politik** ist definiert für die Anforderung „Einfacher interner Übertragungsschutz (FDP_ITT.5)“:

> „Die Benutzerdaten (AT1 und AT+) sollen geschützt werden,
> um ihre Integrität sicherzustellen.“

5.1.3 Integrität der gespeicherten Daten (FDP_SDI)

5.1.3.1 Überwachung der Integrität der gespeicherten Daten (FDP_SDI.1)

FDP_SDI.1.1 Die TSF müssen die innerhalb von Blöcken gespeicherten und von den TSF kontrollierten Benutzerdaten auf *zufällige Manipulation* bei allen Objekten auf Basis folgender Attribute überwachen: *Identifizierungsdaten AT1 in der Identifizierungseinheit ID-Tag und den Leerungsdatensätzen AT während der Speicherung im Sammelfahrzeug*.

5.1.4 Fehlertoleranz (FRU_FLT)

5.1.4.1 Verminderte Fehlertoleranz (FRU_FLT.1)

FRU_FLT.1.1 Die TSF müssen den Betrieb von *der Übertragung der Leerungsdatenblöcke (AT+) von der Bordrechner-Software zum Sicherheitsmodul mit Hilfe der im sekundären Speicher gesicherten Daten* sicherstellen, wenn die folgenden Fehler auftreten: *Verlust der Benutzerdaten im primären Speicher des Sammelfahrzeuges.*

5.1.5 Hinlänglichkeit der Sicherheitsanforderungen

5.1.5.1 Hinlänglichkeit der Sicherheitsanforderungen des TOE und gegenseitige Unterstützung

OT.Inv#1 (Erkennung von zerstörten Identifizierungsdaten) behandelt die Erkennung von manipulierten Identifizierungsdaten (AT1) von Leerungsdatensätzen (AT) innerhalb der Identifizierungseinheit und während der Übertragung zwischen Identifizierungseinheit und der Bordrechner-Software, welche ein separater Teil des TOE (EVG) ist. Der Schutz der Integrität der Identifizierungsdaten (AT1), welche in der Identifizierungseinheit gespeichert sind, ist gefordert von FDP_SDI.1 und wehrt direkt zufällige Veränderungen von diesen Daten ab. Der Schutz der Benutzerdaten AT1 um ihre Integrität zu sichern ist gefordert von FDP_ITT.5 für die Übertragung zwischen physisch getrennten Teilen des TOE (EVG). Die Sicherung der Datenintegrität schützt also direkt vor Veränderungen der Daten während ihrer Übertragung.

OT.Inv#2 (Erkennung von ungültigen Datensätzen) behandelt die Erkennung von Manipulationen von Leerungsdatensätzen (AT), welche zwischen der Bordrechner-Software und dem Sicherheitsmodul übertragen werden; d.h. zwischen zwei physikalisch getrennten Teilen des TOE (EVG). Der Schutz dieser Benutzerdaten AT1 um ihre Integrität sicherzustellen ist gefordert von FDP_ITT.5 für die Datenübertragung zwischen physisch getrennten Teilen des TOE. Der Schutz der Datenintegrität schützt gleichzeitig gegen Manipulationen der Daten.

OT.Inv#2 behandelt also auch die Erkennung von ungültigen Leerungsdatensätzen AT während ihrer Verarbeitung und Speicherung im Sammelfahrzeug und Manipulationen der Leerungsdatensätze AT, die zum Sicherheitsmodul übertragen werden. Der TOE (EVG) liefert gemäß FDP_DAU.1 eine Fähigkeit einen Beweis zu erzeugen welcher durch den Anwender benutzt werden kann, um die Gültigkeit der Daten zu verifizieren. Der Schutz der Integrität der Benutzerdaten (AT) welche im Sammelfahrzeug gespeichert sind ist gefordert durch FDP_SDI.1 und wehrt direkt zufällige Veränderungen von diesen Daten ab. Die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 unterstützen sich gegenseitig für die Datenauthentisierung und Integrität. Deswegen decken die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 das Sicherheitsziel OT.Inv#2 hinlänglich ab.

OT.Safe (Fehlertoleranz) behandelt die Verfügbarkeit passender Daten zur Übertragung von Leerungsdatensätzen (AT) von der Bordrechner-Software zum Sicherheitsmodul für den Fall des Verlustes innerhalb des primären Speichers der Bordrechner-Software. Die Funktionalität für diese Datenübertragung mit Hilfe eines sekundären Speichers nach dem Verlust der Daten in einem primären Speicher wird durch den TOE realisiert gemäß FRU_FLT.1.

5.1.5.2 Hinlänglichkeit der Sicherheitsanforderungen der Umgebung des TOE

OE.Id (Identifizierungseinheit ID-Tag) wird bereitgestellt durch R.Id; so wie R.Id fordert, was das Ziel OE.Id bestätigt.

OE.Trusted (Vertrauenswürdiges Personal) wird bereitgestellt durch R.Trusted; so wie R.Trusted fordert, was das Ziel OE.Trusted bestätigt.

OE.Access (Zugangsschutz) wird bereitgestellt durch R.Access; so wie R.Access fordert, was das Ziel OE.Access bestätigt.

OE.Check (Überprüfung der Vollständigkeit) wird bereitgestellt durch R.Check; so wie R.Check fordert, was das Ziel OE.Check bestätigt.

OE.Backup (Datensicherung) wird bereitgestellt durch R.Backup; so wie R.Backup fordert, was das Ziel OE.Backup bestätigt.

5.2 EVG-Sicherheitsfunktionen

FDP_DAU.1.1 (Erzeugung einer Gültigkeitsgarantie)

Der EVG erzeugt durch den IO03 einen Message Authentication Code (MAC_{32}) über jeden Leerungsdatensatz AT bevor dieser in die Primärspeicher des IO03 geschrieben wird. Auch der BackUp-Speicher auf dem IO03 ist MAC_{32}-gesichert. Zusätzlich wird über jeden Leerungsdatenblock AT+ ein MAC_{32} gebildet.

FDP_DAU.1.2 (Verifizierung einer Gültigkeitsgarantie)

Der EVG prüft durch das EnviCONVERT den MAC_{32} über jeden Leerungsdatensatz AT beim Einlesen und zeigt die Ergebnisse in einer Logdatei an. Die AT+ werden nach ihrem fortlaufenden Counter, Fahrzeugnummer, Ein-und Ausschaltzeit verifiziert sowie deren MAC_{32} geprüft, die Ergebnissre werden in eine Logdatei geschrieben. Auch bei jedem durch ein Restore wiederhergestellten Leerungsdatensatz AT wird der MAC_{32} geprüft und die Ergebnisse werden in einer Logdatei angezeigt, ungültige Leerungsdatenblöcke AT+ oder Leerungsdatensätze AT werden abgelehnt.

FDP_ITT.5.1 (Integrität der internen Übertragung)

Die Übertragung der Identifikationsdaten des Abfallbehälters (AT1) erfolgt zwischen ID-Tag und Leser sowie zwischen Leser und IO03 mit einem CRC-Code gesichert, sowie durch Wiederholung und Vergleich der Übertragung.

Die Integrität von AT+ wird gewährleistet indem nach Ergänzung eines Datensatzes AT ein MAC_{32} berechnet wird. AT+ verfügt über einen Anfangs und einen End-Datensatz welcher in dieser Berechnung eingeschlossen ist, deshalb werden nur komplette Leerungsdatenblöcke AT+ übertragen.

FDP_SDI.1.1 (Überwachung der Integrität der gespeicherten Daten)

Die Identifikationsdaten des Abfallbehälters (AT1) werden im ID-Tag mit CRC-Code gesichert, durch den Leser gelesen und geprüft. Erkannte Modifizierungen führen zu Fehlermeldungen an die Bediener.

Der EVG erzeugt und speichert einen MAC_{32} über jeden Leerungsdatensatz AT im Primär- und Sekundärspeicher und prüft vor jeder Übertragung den MAC_{32} über jeden Leerungsdatensatz AT im Primär- und Sekundärspeicher. Nur als unverfälscht erkannte Leerungsdatensätze AT werden an EnviCONVERT übergeben.

FRU_FLT.1.1 (Datensicherung)

Treten Verluste von Leerungsdatensätzen AT oder Leerungsdatenblöcken AT+ im primären Speicher, USB Stick/GPRS oder im EnviCONVERT auf, so werden diese festgestellt und dem Bediener mitgeteilt. Für diesen Fall sind die Leerungsdatenblöcke AT+ ausreichend lange im sekundären Speicher des IO03 gespeichert, um diese Daten mit der Restore-Funktion wieder herstellen zu können. Somit sind die Daten zweimal auf den internen Speichern des IO03 vorhanden.

5.3 Anforderungen an die Vertrauenswürdigkeit des TOE (EVG)

Tabelle 6: Anforderungen an die Vertrauenswürdigkeit für Stufe EAL1+

Klasse der Vertrauenswürdigkeit	Komponente der Vertrauenswürdigkeit
ADV	ADV_FSP.1
AGD	AGD_OPE.1 AGD_PRE.1
ALC	ALC_CMC.1 ALC_CMS.1
ASE	ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.2 ASE_SPD.1 ASE_REQ.2 ASE_TSS.1
ATE	ATE_IND.1
AVA	AVA_VAN.1

5.3.1 Entwicklung (ADV)

Die Schutzklasse ADV definiert Anforderungen zur Bereitstellung von Informationen über das Design des TOE, seine Struktur und seine Schnittstellen. Diese Informationen dienen als Grundlage für die Durchführung von Analysen und Tests von Sicherheitslücken.

5.3.1.1 Funktionale Spezifikation (ADV_FSP)

Der Entwickler muss eine funktionale Spezifikation bereitstellen. Diese muss die TSF und ihre externen Schnittstellen in einem informellen Stil beschreiben. Sie muss in sich konsistent sein, den Zweck und die Methode des Gebrauchs aller externen TSF-Schnittstellen einschließlich Details der Wirkungen, Ausnahmen, und Fehlermeldungen beschreiben und die TSF vollständig darstellen.

5.3.2 Handbücher (AGD)

Die Schutzklasse AGD definiert Anforderungen an die Verständlichkeit, Abdeckung und Vollständigkeit der vorbereitenden und benutzerführenden Dokumentation, die die Entwickler für den Anwender verfassen. Ein Benutzer ist in diesem Zusammenhang eine Person, die befugt ist, den TOE im Einklang mit den funktionalen Sicherheitsanforderungen zu betreiben. Diese Dokumentation, die Informationen für alle Benutzer-Rollen, ist ein wichtiger Faktor für die sichere Bereitstellung und den Betrieb des TOE.

5.3.2.1 Benutzerführung (AGD_OPE)

Benutzer-Handbuch
Der Entwickler muss ein Benutzer-Handbuch bereitstellen. Dieses muss die Funktionen und Schnittstellen beschreiben, die den Benutzern des TOE (EVG) zur Verfügung stehen, die nicht für Systemverwaltung zuständig sind. Das Benutzer-Handbuch muss den Gebrauch der vom TOE (EVG) bereitgestellten Sicherheitsfunktionen, die für den Benutzer zugänglich sind, beschreiben. Es muss Warnungen bezüglich den Benutzern zugänglichen Funktionen und Privilegien enthalten, die in einer sicheren Verarbeitungsumgebung kontrolliert werden können. Das Benutzer-Handbuch muss alle Verantwortlichkeiten des Benutzers klar darstellen, die für den sicheren Betrieb des TOE (EVG) notwendig sind, einschließlich derjenigen, die mit den in der Darlegung der EVG-Sicherheitsumgebung enthaltenen Annahmen zum Benutzerverhalten zusammenhängen. Es muss konsistent mit allen anderen für die Prüfung und Bewertung gelieferten Dokumentationen sein und alle Sicherheitsanforderungen an die IT-Umgebung beschreiben, die für den Benutzer relevant sind.

5.3.2.2 Vorbereitende Prozeduren (AGD_PRE)

Konfigurations-Dokumentation
Der Entwickler muss eine Konfigurations-Dokumentation bereitstellen. Diese muss dem Benutzer alle Informationen vermitteln, die nötig sind um sicherzustellen, dass sein Exemplar des TOE akzeptiert, konfiguriert und aktiviert werden kann und um die Sicherheitsfunktionen während des Betriebs zu gewährleisten.

5.3.3 Lebenszyklus-Support (ALC)

Die Schutzklasse ALC definiert Anforderungen für die Qualitätssicherung durch die Annahme eines genau definierten Lebenszyklus-Modells für alle Schritte der TOE-Entwicklung, einschließlich der Fehlerbehebung, Sicherungsmaßnahmen und -Politik, der richtigen Verwendung von Werkzeugen und Techniken und Maßnahmen zur Gefahrenabwehr zum Schutz der Entwicklungsumgebung.

5.3.3.1 Konfigurations-Management-Einsatzmöglichkeiten (ALC_CMC)

Die Konfigurations-Management-Funktionen definieren die Eigenschaften des Konfigurations-Management-Systems.

5.3.3.2 Konfigurations-Management-Abgrenzung (ALC_CMS)

Dieses Kapitel befasst sich mit dem Geltungsbereich des Konfigurations-Management-Systems, das auf die TOE-Elemente verweist, die durch das Konfigurations-Management-System kontrolliert werden. Diese Angaben müssen sich auch im Inhalt der mitgelieferten Konfigurations-Dokumentation wiederfinden.

5.3.4 Testen (ATE)

5.3.4.1 Unabhängiges Testen (ATE_IND)

Der Entwickler muss den TOE (EVG) zum Testen bereitstellen, dieser muss sich zum Testen eignen.

5.3.5 Prüfung der Schwachstellen (AVA_VAN)

Diese Klasse beschreibt mögliche der Schwachstellen in der Entwicklung oder dem Betrieb des TOE. Es wird geprüft, ob potenzielle Schwachstellen, die bei der Evaluierung der zu erwartenden Entwicklung oder bei Betrieb des TOE oder durch andere Methoden (z. B. durch fehlerhafte Hypothesen oder quantitative oder statistische Analyse der Sicherheit von der zugrunde liegenden Mechanismen der Sicherheit) gefunden wurden, Angriffe gegen die funktionalen Sicherheitsanforderungen ermöglichen.
Die Klasse befasst sich mit der Gefahr, dass ein Angreifer in der Lage sein könnte Fehler zu entdecken, damit die den unbefugten Zugang zu Daten und Funktionen ermöglichen, oder die Fähigkeit erlangt sich durch Änderung der TSF oder mit Fähigkeiten anderer Benutzer Zugriff zu verschaffen.

5.4 Maßnahmen zur Vertrauenswürdigkeit

Es werden folgende Maßnahmen zur Vertrauenswürdigkeit ergriffen.

5.4.1 Konfigurations-Management

AGD_PRE Alle Programmteile mit Ihrer Version werden in einer aktuell gültigen **Konfigurationsliste** dargestellt.

- Alle Versionen des TOE (EVG) sind mit unterschiedlichen **Versionsnummern** gekennzeichnet.
- Jedes Programmteil des TOE (EVG) verfügt über eine **Info-Funktion**, mit der die Programmversion angezeigt werden kann.

Durch diese Anforderungen sind die allgemeinen Anforderungen abgedeckt.

5.4.2 Entwicklung

5.4.2.1 Informelle funktionale Spezifikation

Es ist ein Architekturentwurf mit einer informellen Beschreibung aller Sicherheitsfunktionen zu erstellen, der die externen Schnittstellen der Teilsysteme des TOE (EVG) beschreibt.

ADV_FSP Das Dokument „Funktionale Spezifikation“ enthält die Informelle Funktionale Spezifikation.

Durch diese Anforderung sind die allgemeinen Anforderungen abgedeckt.

5.4.2.2 Informeller Nachweis der Übereinstimmung

Es ist ein informeller Nachweis zu erstellen, dass die gelieferten Sicherheitsfunktionen, die geforderten Sicherheitsfunktionen abdecken.

Der informelle Nachweis der Übereinstimmung ist Bestandteil des Dokumentes zu ADV_FSP.

Durch diese Anforderung sind die allgemeinen Anforderungen abgedeckt.

5.4.3 Handbücher

Benutzerhandbuch
Es wird ein Benutzerhandbuch mit folgenden Eigenschaften erstellt und ausgeliefert:

AGD_OPE Dieses Dokument beinhaltet das Benutzer-Handbuch

- Beschreibung der Schnittstellen und Benutzerfunktionen
- Beschreibung der Bedienung der Sicherheitsfunktionen der Benutzer
- Warnungen bzgl. Funktionen, die in einer sicheren Verarbeitungsumgebung kontrolliert werden können.
- Beschreibung der Verantwortung des Benutzers
- Beschreibung aller sicherheitsrelevanten Ereignisse der Benutzer-Funktionen
- Konsistenz mit allen anderen Dokumenten
- Beschreibung der Sicherheitsanforderungen an die IT-Umgebung, die für den Benutzer relevant sind

Durch diese Anforderungen sind die allgemeinen Anforderungen abgedeckt.

5.4.4 Unabhängiges Testen

Der EVG wird in geeigneter Weise am Teststand von Envicomp Systems und einem geeigneten PC zum Testen durch den Evaluator zur Verfügung gestellt. Die Testprotokolle sind vorzulegen. Damit sind die Forderungen ATE_IND abgedeckt.

5.5 Sicherheitsanforderungen an die IT-Umgebung

Das Schutzprofil verlangt keine Sicherheitsanforderungen an die IT-Umgebung.

5.6 Sicherheitsanforderungen an die Nicht-IT-Umgebung

R.Id *ID-Tag*

Der Benutzer muss folgendes sicherstellen:

- Die Identifikationseinheit ID-Tag wird an dem Abfallbehälter befestigt, der durch die Identifikationsdaten in dieser Einheit identifiziert wird.
- Die Identifikationsdaten in dieser Einheit sind eindeutig.
- Die Zuordnung der Identifikationsdaten zu einem Gebührenpflichtigen erfolgen durch organisatorische Maßnahmen, welche sich nicht im Bereich des EVG befinden.

R.Trusted *Vertrauenswürdiges Personal*

Die Personen, die das Sammelfahrzeug und das Sicherheitsmodul bedienen, installieren und warten sollen autorisiert und vertrauenswürdig sein. Alle Personen, die für die Sicherheit der Umgebung verantwortlich sind sollen autorisiert und vertrauenswürdig sein.

R.Access *Zugangsschutz*

Die Umgebung soll durch geeignete Maßnahmen sicherstellen, dass nur die Benutzer und das Bedienpersonal direkten Zugang zu den Komponenten des TOE (EVG) haben (mit Ausnahme des Zugang zur Identifikationseinheit ID-Tag). Die Umgebung soll jede Art der Beeinflussung der internen Verbindungskanäle innerhalb des Office-Computers verhindern.

R.Check *Überprüfung der Vollständigkeit*

Der Benutzer soll in regelmäßigen Zeitabständen die Vollständigkeit der Übertragung der Leerungsdatenblöcke (AT+) von den Sammelfahrzeugen in das Büro überprüfen. Der Benutzer soll die Wiederherstellung und Übertragung der Daten anfordern, von denen er annimmt, dass sie noch nicht vom Sammelfahrzeug in das Büro übertragen worden sind.

Die Zeitintervalle dieser Überprüfung und Anforderungsaktionen müssen konsistent mit der verfügbaren Speicherkapazität auf dem Bordrechner sein, der die Leerungsdatenblöcke (AT+) sekundär zur Sicherheit für einen bestimmten Zeitraum speichert.

R.Backup *Datensicherung*

Der Benutzer soll die Daten, die vom TOE (EVG) erzeugt wurden, in regelmäßigen Abständen in einem angebrachten Archiv sichern.

5.7 Erklärung der Sicherheitsanforderungen

5.7.1 Abdeckung der Sicherheitsanforderungen

Tabelle 7: Zuordnung von Funktionalen Sicherheitsanforderungen zu Sicherheitszielen

TOE Funktionale Sicherheitsanforderungen / TOE Sicherheitsziele	OT.Inv#1	OT.Inv#2	OT.Save
FDP_DAU.1		X	
FDP_ITT.5	X	X	
FDP_SDI.1	X	X	
FRU_FLT.1			X

Tabelle 8: Zuordnung von Sicherheitsanforderungen der Umgebung zu Sicherheitszielen der Umgebung

Sicherheitsanforderungen der Umgebung / Sicherheitsziele der Umgebung	OE.Id	OE.Trusted	OE.Access	OE.Check	OE.Backup
R.Id	X				
R.Trusted		X			
R.Access			X		
R.Check				X	
R.Backup					X

Ausführliche Begründungen für Sufficiency of SFRs siehe [4] Abschnitt 6.3.2.

5.7.2 Erklärung der Abhängigkeiten

Tabelle 9: Funktionale Anforderungen und Abhängigkeiten

Anforderung	Abhängigkeit	Erfüllt
FDP_DAU.1	Keine Abhängigkeiten	unbedingt
FDP_ITT.5	Keine Abhängigkeiten	unbedingt
FDP_SDI.1	Keine Abhängigkeiten	unbedingt
FRU_FLT.1	FPT_FLS.1	Siehe nachfolgenden Text

FRU_FLT.1 benötigt das TOE um den Ablauf des Datentransfer von der Fahrzeugsoftware zum Sicherheitsmodul zu gewährleisten, auch wenn Daten in der Fahrzeug-Software verloren gehen. Diese Anforderung wird für die Erfüllung der organisatorischen Sicherheitspolitik, die sich mehr auf die Verfügbarkeit der Daten bezieht als auf die korrekte Funktionalität der Software, benötigt, und hängt nicht mit einem sicheren Stand des TOE in Bezug auf etwaige Bedrohungen auf das TOE zusammen. Da die Abhängigkeitskomponente FPT_FLS.1 sich lediglich auf einen solch sicheren Zustand des TOE (d.h. der Software) bezieht, ist sie nicht auf das TOE anwendbar.

5.7.3 Erklärung der Auswahl der EAL-Stufe

Die Vertrauenswürdigkeitsstufe für dieses Security Target ist EAL1+. Diese EAL bewirkt einen weitaus höheren Sicherheitsgrad gegenüber einem nicht-evaluierten IT-Produkt oder -System indem sie eine vertrauenswürdige Art der Bedienung vermittelt, während die Bedrohungen der Sicherheit nicht als ernst angesehen werden, was in direkter Beziehung zu dem eher niedrig anzusiedelnden Wert der vom EVG zu schützenden Daten steht. EAL1+ bietet unabhängige Sicherheit um unterstützend dafür Sorge zu tragen, dass im Umgang mit Informationen aus den Leerungsdatensätzen verantwortungsvoll umgegangen wird und dass der EVG einen, den Kundenanforderungen angemessenen Schutz gegenüber bekannten Bedrohungen bietet. Durch EAL1+ wird der EVG inklusive unabhängiger Tests der Sicherheitsfunktionalität und ausführlicher Untersuchung der bereitgestellten Anleitungen und Dokumentationen evaluiert.

Im Vergleich zur im zugrundeliegenden Schutzprofil verlangten Vertrauenswürdigkeitsstufe (EAL1 nach CC 2.3) wird der EVG nach CC 3.1 EAL1+ evaluiert.
Dabei wird EAL1 um die Komponenten ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2 erweitert.
Die Erweiterung von EAL1 um die o.a. Komponenten wurde vorgenommen, um die in Abschnitt 4 definierte Sicherheitsumgebung des EVG und die darauf aufbauenden Sicherheitsziele und Sicherheitsanforderungen angemessen zu prüfen, was bei einer Prüfung nach EAL1 der CC Version 3.1 noch nicht gefordert ist.

5.8 Erklärung der PP-Postulate

Diese Sicherheitsanforderungen decken das Schutzprofil vollständig ab, da alle

- Sicherheitsziele und
- Sicherheitsanforderungen

unverändert übernommen worden sind.

5.9 PP-Verweis

Der TOE (EVG) ist konform mit dem des zertifizierten Schutzprofiles (BSI-PP0010) und erfüllt somit alle Anforderungen des WBIS Protection Profiles.

5.10 PP-Anpassung

Die Sicherheitsvorgaben enthalten keine PP-Anpassung durch Operationen der Sicherheitsanforderungen.

Anhang

5.11 Abkürzungen

A.	Präfix für Annahmen
AGS	Amtlicher Gemeinde Schlüssel
AT	Abkürzung des Schutzprofils für engl. „record of clearance“, deutsch “Leerungsdatensatz”
AT+	Abkürzung des Schutzprofils: engl. „clearance data block”, deutsch “Leerungsdatenblock”
AT1	Identifikationsdaten des Abfallbehälters
AT2	Zeitstempel (Datum und Uhrzeit) des Leerungsvorganges
AT3	Statuscode der Leerungsvorganges (Kontrollziffer)
AT4	optional: Nettogewicht der entsorgten Abfälle
BCC	Block Check Code
BCP	Bord-Computer-Programm
CC	Common Criteria (Gemeinsame Kriterien)
EAL	Evaluation Assurance Level
ESS	Envicomp Security System
ESB	Envicomp System Box
EVG	Evaluationsgegenstand
F1	Manipulationssicherung der R-Leerungsdaten (AT)
F2	Backup-Funktion und Restore-Funktion der Leerungsdatensätze (AT)
F3	Erkennungsfunktion für gültige Identifizierungsdaten
ID-Tag	Abkürzung für TAG-Identifikationsnummer
IT	Information Technology (Informationstechnologie)
LRG	Dateikennung einer Leerungsdatei

MAC	Message Authentication Code
MAC_{32}	Message Authentication Code der Länge 32 bit
OE.	Präfix für Sicherheitsziele der Umgebung
OSP	Organisational Security Policy
OT.	Präfix von Sicherheitszielen
P.	Präfix für Politik
PP	Protection Profile (Schutzprofil)
R.	Präfix für Sicherheitsanforderungen an die Nicht-IT-Umgebung
SF	Security Function (Sicherheitsfunktion)
SFP	Security Function Policy (funktionale Sicherheitspolitik)
SOF	Strength of Function (Stärke der Funktionen)
ST	Security Target (Sicherheitsvorgaben)
T.	Präfix für Bedrohungen (threats)
TAG	Berührungslos lesbarer Datenträger (Transponder)
TK	Transport-Schlüssel
TOE	Target of Evaluation (= EVG)
TSC	TSF Scope Control (Anwendungsbereich der TSF-Kontrolle)
TSF	TOE Security Function (EVG-Sicherheitsfunktion)
TSFI	TSF Interface (TSF-Schnittstelle)
TSP	TOE Security Policy (EVG-Sicherheitspolitik)
WBIS	Waste Bin Identification System = Abfallbehälter-Identifizierungssystem

5.12 Glossar

ESS	Envicomp Security System Komplettes System zur Erfassung der Daten vom TAG bis zum Office
EBICS	Envicomp Behälter Identifications Car System
EnviCONVERT	Programm zur Entgegennahme und Überprüfung sowie Weitergabe und Backupfunktion der Leerungsdaten
BCC	Code zum Erkennen zufälliger Fehler, der aus der XOR-Summe aller Bytes besteht
BC04	Spezial-PC im Sammelfahrzeug mit abgesetztem Touch – Bedienteil / Hauptaufgabe ist die Bedienung des Systems am Müllsammelfahrzeug und der Datenübertragung.
IO03	Spezial-PC im Sammelfahrzeug. Er entspricht inhaltlich dem Bordrechner in der Terminologie des WBIS-PP
CRC-Code	Zyklischer linearer Code zum Erkennen zufälliger Fehler
Backup-Leerungsdatensatz	Leerungsdatensatz im Backup des EnviCONVERT-Systems mit Angaben zu den Leerungen der Abfallbehälter. Die Formate von Backup- und Leerungsdatensatz stimmen überein. Er entspricht inhaltlich dem Leerungsdatensatz AT in der Terminologie des WBIS-PP.
EC-Sicherheitsmodul	EnviCONVERT Sicherheitsmodul Programm zum Erzeugen der Schlüssel. Dieses Modul ist Bestandteil des EVG
ID-Tag	Transponder zur Speicherung der Identifikationsdaten des Abfallbehälters
Kfz-Ausstattung	Komponenten des Systems EBICS (Envicomp Behälter Identifications Car System) für die Abfall-Sammelfahrzeuge, bestehend aus: BC04, Reader, Enviomp System Box mit IO03, Kontrollschaltern, Alarmeinrichtung, Wägesystem und Antennen zum Lesen von TAGs. Der IO03 enthält die EVG-Komponente „IO03-Programm“.
Leerungsdatei	ASCII-Datei mit der Dateikennung „LRG“, die Leerungsdatensätze und deren Anzahl während einer Tour eines Fahrzeugs enthält. Sie entspricht dem Leerungsdatenblock AT+ in der Terminologie des WBIS-PP.
Message Authentication	Kryptographisches Integritätsmerkmal, das in Abhängigkeit

Code	von einem Schlüssel für Daten berechnet wird, kurz MAC. Der Absender der Daten berechnet den MAC für die Daten und fügt ihn den Daten bei. Der Empfänger berechnet den MAC für die empfangenen Daten neu. Die Daten werden als durch Dritte (die nicht über den Schlüssel verfügen) nicht verfälscht akzeptiert, wenn empfangener und neu berechneter MAC übereinstimmen.
USB / GPRS	USB / GPRS die einen möglichen Kommunikationskanal zwischen dem Bordcomputer der Kfz-Ausstattung und EnviCONVERT im Office ermöglicht
Leerungsdatensatz	Leerungsdatensatz mit Angaben zu den Leerungen der Müllgefäße. Sie entspricht dem Leerungsdatensatz AT in der Terminologie des WBIS-PP.
Sammelfahrzeug	Müllfahrzeug mit Spezialkippvorrichtung mit optionaler Wiegevorrichtung und TAG-Lese- und Schreibmodule
Sperrliste	Liste gesperrter Abfallbehälter
TAG	Berührungslos lesbarer Datenträger (Transponder) mit einem Speicher zwischen 32 und 64 bit. Der TAG ist an einem Abfallbehälter befestigt und dient der Identifzierung des Abfallbehälters.
TAG-Identifikationsnummer	Eindeutige und unveränderbare Nummer (read-only) zwischen 32 und 64 Bit Länge zur Identifizierung eines TAG, Kurzform TAG-ID. Sie entspricht in der Terminologie des WBIS-PP den Identifikationsdaten des Abfallbehälters AT+.

5.13 Literatur

[1] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 1: Einführung und allgemeines Modell, Version 3.1, September 2006, mit den Final Interpretations des CCIMB gemäß AIS 32

[2] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 2: Funktionale Sicherheitsanforderungen, Version 3.1, September 2007, mit den Final Interpretations des CCIMB gemäß AIS 32

[3] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 3: Anforderungen an die Vertrauenswürdigkeit, Version 3.1, September 2007, mit den Final Interpretations des CCIMB gemäß AIS 32

[4] Protection Profile - Waste Bin Identification Systems (WBIS-PP), Version 1.04, (registriert beim BSI unter BSI-PP-0010-2004 vom 27.05.2004)

[5] Dokumentencheck Sicherheitsvorgaben ESS 3.0, Version 2.12 vom 23.01.2009

5.14 Transponder

Nachfolgend aufgeführt sind die Transpondertypen und ihre Artikelnummern und technischen Spezifikationen, die mit dem unter der Kennung BSI-DSZ-CC-0618 zertifizierten ESS 3.0 betrieben werden können.

Hierzu zählen Transponder folgender Normen:

- **ISO 7816**
- **ISO 11784**
- **ISO 11785**
- **ISO 15693**
- **ISO 14443**
- **ISO 14803**
- **ISO 18000**

Folgende Hersteller/Typen werden vom ESS 3.0 unterstützt:

Frequenz 125 kHz

4101040, 4101054, 4100002, 4101043, 4101115, 4101008, 4100001, 4101166

Frequenz 128 kHz

4101025

Frequenz 134,2 kHz

4101149, 4101156, 4101066, 4101056, 4101036, 4101013, 4101073, 4101017, 4101165, 4101105

Frequenz 4 MHz

4101009, 4101145

Frequenz 13,56 MHz

4101205, 4101256, 4101248