Gefäßidentifikationssystem Gassner (GWBIS)

Version V-GWBIS-1.50

Sicherheitsvorgaben (ST)

Version 2.0 vom 25.03.2010

Evaluierungsgrundlage:

Common Criteria, Vers. 3.1

Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

Vertrauenswürdigkeitsstufe: EAL1+

Hersteller/Antragsteller:

GASSNER Wiege und Messtechnik GmbH

Robinigstraße 26a, 5020 Salzburg

INHALTSVERZEICHNIS

1 Aufbau des Dokuments 4

2 ST-Einführung 5

2.1 Identifikation ST und EVG 5

2.2 EVG-Übersicht (WBIS) 5

2.2.1 Übersicht Abfallbehälter-Identifikations-Systeme 5
2.2.2 Übersicht Gassner Gefäß-Identifikations-System 6
2.2.3 Lieferumfang des Gassner Gefäß-Identifikations-Systems 6

2.3 EVG-Beschreibung 8

2.3.1 Beschreibung des Gesamtsystems 8
2.3.2 Definition des EVG 11
2.3.3 Abgrenzung des EVG 12

3 Postulat der Übereinstimmung mit den CC 14

4 Definition der Sicherheitsumgebung 15

4.1 Einleitung 15

4.1.1 Schutzwürdige Objekte 15
4.1.2 Subjekte 15
4.1.3 Angreifer 15

4.2 Bedrohungen 16

4.3 Organisatorische Sicherheitspolitik 16

4.4 Annahmen 17

5 Sicherheitsziele 18

5.1 EVG-Sicherheitsziele 18

5.2 Umgebungssicherheitsziele 18

5.3 Erläuterung der Sicherheitsziele 19

5.3.1 Abdeckung der Sicherheitsziele 19
5.3.2 Hinlänglichkeit der Sicherheitsziele 20

5.4 Sicherheitsanforderungen an die Nicht-IT-Umgebung 21

6 IT-Sicherheitsanforderungen 22

6.1 Funktionale Sicherheitsanforderungen an den EVG 22

6.1.1 Datenauthentisierung (FDP_DAU) 22

6.1.2 EVG-interner Transfer (FDP_ITT) ... 22
6.1.3 Integrität der gespeicherten Daten (FDP_SDI) ... 23
6.1.4 Fehlertoleranz (FRU_FLT) ... 23
6.2 Anforderungen an die Vertrauenswürdigkeit des EVG ... 23
6.3 Erläuterung der Sicherheitsanforderungen ... 24
6.3.1 Abdeckung der Sicherheitsanforderungen ... 24
6.3.2 Hinlänglichkeit der Sicherheitsanforderungen ... 24
6.3.3 Explizit dargelegte Sicherheitsanforderungen ... 25
6.3.4 Vertrauenswürdigkeitsmaßnahmen und Vertrauenswürdigkeitsstufe ... 25
6.4 Erläuterung der Abhängigkeiten ... 26

7 EVG-Übersichtsspezifikation ... 27

7.1 EVG-Sicherheitsfunktionen ... 27
7.2 Maßnahmen zur Vertrauenswürdigkeit ... 27
7.3 Erklärung der EVG-Übersichtsspezifikation ... 29
7.3.1 Zusammenwirken der IT-Sicherheitsfunktionen ... 30

8 Anhang ... 32

8.1 Literaturangaben ... 32
8.2 Abkürzungen ... 32
8.3 Mnemocodes der EVG-Übersichtsspezifikation ... 32
8.4 Glossar ... 33

Tabellenverzeichnis

Tabelle 1- GFE-Bestandteile und Versionen ... 7
Tabelle 2 - Darstellung der Sicherheitsziele ... 19
Tabelle 3 - Anforderungen der angestrebten Vertrauenswürdigkeitsstufe EAL1+ ... 23
Tabelle 4 - Gegenüberstellung: Funktionale Sicherheitsanforderungen – Sicherheitsziele ... 24
Tabelle 5 - Gegenüberstellung: Sicherheitsanforderungen – Umgebungssicherheitsziele ... 24
Tabelle 6 - Abhängigkeiten der funktionalen Anforderungen ... 26
Tabelle 7 - Maßnahmen zur Vertrauenswürdigkeit ... 28
Tabelle 8 - Gegenüberstellung: Funktionale Sicherheitsanforderungen - Sicherheitsfunktionen ... 30

Abbildungsverzeichnis

Abbildung 1 - Abfallbehälter-Identifikations-System ... 9

1 Aufbau des Dokuments

Zur Vereinfachung des Vergleichs mit dem diesem ST zu Grunde liegenden Schutzprofil „Protection Profile - Waste Bin Identification Systems WBIS-PP, Version 1.04“ [3] sind die dem PP direkt übernommenen oder direkt aus dem Englischen übersetzten Teile durch grüne Schrift gekennzeichnet; für die Sicherheitsvorgaben neu entstandene Passagen wurden in schwarzer Schrift gehalten.

Das Dokument ist wie folgt unterteilt:

- Abschnitt 2 enthält einführendes Material für die Sicherheitsvorgaben. Abschnitt 2.3 beschreibt den typischen Einsatzbereich und die Definition des EVG.
- Abschnitt 3 enthält Aussagen zur Konformität zu den Common Criteria und zu Schutzprofilen.
- Abschnitt 4 enthält eine Erörterung bezüglich der angenommenen EVG-Sicherheitsumgebung. Dieser Abschnitt definiert ebenfalls die Bedrohungen, die entweder von den technischen Gegenmaßnahmen in der EVG-Hardware, der EVG-Software, oder durch Kontrollen aus der Umgebung angesprochen werden.
- Abschnitt 5 enthält die Sicherheitsziele sowohl für den EVG als auch die EVG-Umgebung.
- Abschnitt 6 enthält die Funktionalen Sicherheitsanforderungen und Anforderungen an die Vertrauenswürdigkeit, abgeleitet aus den Common Criteria (CC), Teil 2 [1] und Teil 3 [2], die vom EVG erfüllt werden müssen.
- Abschnitt 7 gibt die einzelnen Sicherheitsfunktionen des EVG und Maßnahmen zur Vertrauenswürdigkeit wieder.
- In Abschnitt 8 wird ein Verzeichnis mit Literaturangaben bereitgestellt. Listen mit Abkürzungen, Mnemocodes und ein Glossar dienen zur Definition von wiederholt gebrauchten Kurzbezeichnungen.

Die Abschnitte 5 und 6 enthalten zusätzliche Erläuterungen. Abschnitt 5.3 enthält eine Erklärung, um ausführlich zu demonstrieren, dass die IT-Sicherheitsziele die Politiken und Bedrohungen erfüllen. Beweise erfolgen durch die Abdeckung jeder Politik und Bedrohung. Der Abschnitt erläutert, wie die Anforderungen relativ zu den Zielen komplettiert werden, sowie dass jedes Sicherheitsziel durch eine oder mehr Anforderungen an die Bestandteile angesprochen wird. Beweise erfolgen durch die Abdeckung jedes Zieles. Abschnitt 6.3 enthält einige Argumente für die Adress-Abhängigkeitsanalyse und die interne Folgerichtigkeit und gegenseitige Unterstützung der Anforderungen.

2 ST-Einführung

Dies sind die Sicherheitsvorgaben (Security Target, ST) für die Zertifizierung des Gefäßidentifikationssystems Gassner (GWBIS) nach den Common Criteria (CC).

2.1 Identifikation ST und EVG

Eigenschaft	Wert
Sicherheitsvorgaben (ST)	
Titel:	Sicherheitsvorgaben zum Gefäßidentifikationssystem Gassner(GWBIS)
Version:	2.0
Datum:	25.03.2010
Autoren:	Helmut Strauß, Gerald Krummeck
CC-Version	3.1R2
Vertrauenswürdigkeitsstufe	EAL1, ergänzt um ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2
Evaluationsgegenstand (EVG)	
Produktname	Gefäßidentifikationssystem Gassner (GWBIS)
Version	V-GWBIS-1.50

2.2 EVG-Übersicht (WBIS)

2.2.1 Übersicht Abfallbehälter-Identifikations-Systeme

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

Aufgabe von Systemen dieser Art ist es z.B. zu zählen, wie oft die Behälter geleert worden sind, um auf diese Art eine verursacherbezogene Abrechnung der Abfallgebühren zu ermöglichen. Häufig werden solche Systeme auch mit zum Beispiel einem Wiege- oder einem Volumenmesssystem kombiniert, um die Entsorgungsleistungen nach Häufigkeit, nach Gewicht oder Menge abrechnen zu können. Es sind in Zukunft auch andere Verfahren denkbar und mit dem System einsetzbar.

Abfallbehälter-Identifikations-Systeme (WBIS) beinhaltende Gebühren- bzw. Abrechnungssysteme umfassen die elektronische Erfassung, Übertragung und Speicherung von Leerungsdaten (u.a. auch als Leistungsnachweise des Entsorgungsunternehmens) bis hin zur Erstellung eines Abfall-Gebührenbescheides durch die entsorgungspflichtigen Körperschaften (Städte und Landkreise) bzw. Rechnungsstellung durch den Entsorger.

Weil aufgrund der Masse der anfallenden Daten eine manuelle Detailprüfung jeder abgerechneten Leerung ausgeschlossen ist, benötigen solche Systeme ein hohes Maß an Vertrauen in die technische Funktionsfähigkeit des Systems, dass z.B. nur genau die tatsächlich durchgeführten Leerungen abgerechnet werden. In diesem Zusammenhang sind daher die für die Abrechnung relevanten Daten (Identifikationsdaten, Zeitstempel) vor Manipulation und Verlust zu schützen.

Diese Daten entstehen bei der Leerung eines Abfallbehälters auf einem Sammelfahrzeug, in dem ausgehend von der Identifikationsnummer des Behälters ein Leerungsdatensatz gebildet wird.

Nach Abschluss einer Entleerungstour werden alle gesammelten Daten mit unterschiedlichen Medien (Datenträger, Kabel, drahtlos) vom Abfallsammelfahrzeug in eine stationäre Software übertragen, um sie dort in einem zentralen Datenbestand zu speichern.

Dabei kann es sich zum Beispiel um die Software im Büro des kommunalen oder privatwirtschaftlichen Entsorgers handeln. Die abrechnungsrelevanten Daten (Identifikationsdaten, Zeitstempel) gelangen in die entsorgungspflichtige Körperschaft über den kommunalen bzw. privatwirtschaftlichen Entsorger oder direkt vom Abfallsammelfahrzeug.

2.2.2 Übersicht Gassner Gefäß-Identifikations-System

Bei Gassner werden Transponderinformationen zu einem Lesegerät übertragen. Von dort werden sie zu dem Fahrzeugrechner (GFE) weitergeleitet. Daraus werden auf dem GFE Leerungsdatensätze erstellt. Die Leerungsdatensätze werden im Fahrzeugrechner redundant in Speichern abgelegt und verwaltet. Von dem Fahrzeugrechner aus werden die Datensätze in Leerungsdatenblöcke gruppiert über den GFE-Speicher bis in eine Bürosoftware übertragen. Die ins Büro übermittelten Leerungsdaten werden wiederum mit Hilfe des Sicherheitsmoduls auf Datenintegrität und Gültigkeit (Authentisierung) überprüft.

Der Datentransfer in die Bürosoftware kann mit unterschiedlichen Datenträgern bzw. Datentransfermethoden erfolgen. So ist z.B. ein dienstleistungsnaher (wie täglicher) Datentransfer zum jeweiligen privatwirtschaftlichen oder kommunalen Entsorgungsunternehmen möglich. Von da aus können die Daten – je nach regionaler bzw. formaler Notwendigkeit – der entsorgungspflichtigen Körperschaft zeitnah oder in definierten Intervallen übergeben werden.

Darüber hinaus bietet Gassner zusätzlich die Möglichkeit, die beschriebenen Daten mit einem weiteren Datenträger z. B. direkt vom Abfallsammelfahrzeug bis in die entsorgungspflichtige Körperschaft zu übertragen ohne dass sie zuvor die Rechentechnik eines z.B. privatwirtschaftlichen Unternehmens durchlaufen müssen. Auf diese Weise erstreckt sich bei Gassner der EVG bis in die entsorgungspflichtige Körperschaft! Dies geschieht durch den Datentransfer mit einem in der GFE vorhandenen und entnehmbaren Langzeitdatenspeicher. Dieser Langzeitdatenspeicher kann direkt in der entsorgungspflichtigen Körperschaft ausgelesen werden und darüber hinaus – je nach Wunsch – auch dort archiviert werden.

Dabei kommt der EVG innerhalb des Gefäß-Identifikations-Systems überall dort zum Einsatz, wo die Datenintegrität und Gültigkeit bei der Übertragung von Daten zwischen den einzelnen Komponenten sichergestellt werden muss. Wie diese EVG Bestimmungen in Art und Umfang umgesetzt werden, wird in den nachfolgenden Kapiteln ausführlich behandelt. In Abschnitt 2.3 werden die Aufgaben des EVG behandelt und die Komponenten beschrieben.

2.2.3 Lieferumfang des Gassner Gefäß-Identifikations-Systems

Im folgenden Diagramm ist eine Übersicht zusammengestellt, die den Lieferumfang des Gassner Gefäß-Identifikations-Systems beschreibt. Beachten Sie bitte, dass eine eingehende Beschreibung der Komponenten und die Anwendung der Komponenten im Abschnitt 2.3 ‚EVG-Beschreibung' erfolgt.

Darstellung und Übersicht des Lieferumfangs des Gassner Gefäß-Identifikations-Systems inklusive aller Versionen:

Name	Versionsnummer	Lieferumfang	Bestandteil des EVG
Transponder	Stifttransponder EnvicompTI-134 2Khz-HDX-R/O-Wedge 23mm Glastransponder Texas InstrumentsRI-TRP-REHP-30	Transponder (EVG-konforme Transponder)	ja

Name	Versionsnummer	Lieferumfang	Bestandteil des EVG
	32mm Glastransponder Texas InstrumentsRI-TRP-RE2B-30 120mm Kunststoffrohr Texas InstrumentsRI-TRP-R9TD-16 Schlüsselanhänger Texas InstrumentsRI-TRP-RFoB		
Lesegerät	Version POWER TIRIS TI-RFID Standard Ausführung	Lesegerät Texas Instruments	nein
Firmware in der GFE und Applikation am Fahrzeugrechner	SWE-BLK-1.01 (für Balkenschütte) SWE-DS-1.01 (für Doppelschütte)	GFE Fahrzeugsoftware GFE mit Firmware (Teil des EVG) für die Gerätegeneration DMA02 Junior	ja
Handbücher GFE	Handbuch_Junior.pdf: Juni 2007 User.pdf: Juni 2009	Installations- und Benutzerhandbücher DMA02 Junior: Handbuch_Junior.pdf user.pdf	ja
Bürosoftware mit Sicherheitsmodul (nur das Sicherheitsmodul ist Teil des EVG)	1.6.0.1	Bürosoftware und Sicherheitsmodul (Teil des EVG) Communicator.exe	ja
Handbücher Bürosoftware	1.6.0.1 letzte Änderung: 25.03.2010	Installations- und Benutzerhandbuch Communicator	ja
Optionale Eingabegeräte	Keine bzw. spezifisch vom Projekt abhängig	Eingabegeräte Pro Manual	nein

Tabelle 1- GFE-Bestandteile und Versionen

Anmerkung zu den Versionsständen:

Die genannten Versionsnummern entsprechen den Versionsständen zum Zeitpunkt der BSI Zertifizierung!

Die weiteren Abschnitte dieser Sicherheitsvorgaben beschreiben den EVG, seine Sicherheitsumgebung mit Annahmen und Sicherheitspolitiken sowie die Sicherheitsziele und Sicherheitsanforderungen.

Bitte beachten: Bezüglich des Begriffes ‚Bürosoftware' ist nur das darin enthaltene Sicherheitsmodul Teil des EVG. Das Sicherheitsmodul selbst ist Bestandteil der Bürosoftware am PC. (siehe auch Abbildung 1 - Abfallbehälter-Identifikations-System im Abschnitt 2.3.1.2)

2.3 EVG-Beschreibung

2.3.1 Beschreibung des Gesamtsystems

2.3.1.1 Übersicht des Gassner Gefäß-Identifikations-Systems (GWBIS)

Bei GWBIS werden Transponderinformationen (Identifikationsdaten AT1) von einem Transponder (ID-Tag) an einem Abfallgefäß zu einem Leser übertragen. Von dort werden sie zu dem Fahrzeugrechner (GFE) weitergeleitet und auf Datenintegrität geprüft.

Bei der GFE handelt es sich um eine von Gassner Wiege und Messtechnik GmbH entwickelte Mikroprozessor gesteuerte Hardware. Die GFE verfügt über weitere Schnittstellen zu anderen Komponenten des Abfallsammelfahrzeuges, wie einem Wiegesystem, die jedoch nicht Teil des EVG sind. Die Firmware auf dieser GFE bildet aus den Identifikationsdaten (AT1) zusammen mit dem Zuordnungsteil (GFE Identifizierung/Zeitstempel AT2), optionalen Daten und einem neu ermittelten CRC-Wert einen Leerungsdatensatz (AT).

Zur Authentisierung der Leerungsdatensätze wird jeweils im Zuordnungsteil AT2 die Kennung der im Fahrzeug befindlichen GFE gespeichert. Die Generierung und Verwendung dieser Kennung wird im Rahmen der Funktionalen Spezifikation (FSP) näher beschrieben.

Die Leerungsdatensätze werden im Fahrzeugrechner in unterschiedlichen Speichern (Primär- und Sekundärspeicher) abgelegt und verwaltet. Die optionalen Daten sind von der Applikation, also von den über Schnittstellen mit der GFE verbundenen Komponenten, abhängig. Für diese optionalen Daten werden im Leerungsdatensatz entsprechende Speicherplätze freigehalten. Der Aufbau eines Leerungsdatensatzes (AT) wird im Rahmen der Funktionalen Spezifikation (FSP) näher beschrieben.

Von dem Fahrzeugrechner aus werden die Daten in Leerungsdatenblöcken[1] über den GFE-Speicher bis in eine Bürosoftware übertragen. Die ins Büro übermittelten Leerungsdatenblöcke (AT+), die darin enthaltenen Leerungsdatensätze (AT) sowie die Gesamtheit der in die Bürosoftware übertragenen Gruppen werden wiederum mit Hilfe des Sicherheitsmoduls auf Datenintegrität und Gültigkeit überprüft.

Der Datentransfer in die Bürosoftware kann bei Gassner mit unterschiedlichen Datenträgern bzw. Datentransfermethoden erfolgen. Die Hardware-Schnittstelle des Bürorechners (siehe Beschreibung 2.3.1.3) und der Teil des GFE der für den Transfer zuständig ist, werden entsprechend der zum Einsatz kommenden Datentransfer Methode, adaptiert.

Des Weiteren kommen aus der Sicht des Gassner-Systems (und im Sinne des EVG) nur „ReadOnly“ Transponder zum Einsatz. Verwendet der Kunde beschreibbare Transponder, so ist der beschreibbare Teil des Transponders und die daraus folgenden Implikationen jedenfalls nicht Teil des EVG.

Der EVG Teil des Gefäß-Identifikations-Systems prüft die Datenintegrität und Gültigkeit bei der Übertragung von Daten zwischen den Komponenten:

- Alle Identifikationsdaten des Abfallbehälters (AT1) werden auf Integrität geprüft.
- Jeder Leerungsdatensatz (AT) ist durch einen CRC gesichert.
- Die Gültigkeit der Leerungsdatensätze (AT) wird durch die eindeutige Kennung und Identifizierung des Fahrzeugrechners (GFE) sichergestellt.
- Die Leerungsdatensätze werden jeweils auf einem Primär- und Sekundärspeicher gespeichert.
- Bei der Übergabe an die Bürosoftware wird mit Hilfe des Sicherheitsmoduls die Datenintegrität der gesamten Übertragung, der Leerungsdatenblöcke (AT+) und der Leerungsdatensätze (AT) überprüft und entsprechend gekennzeichnet.

[1] Ein Leerungsdatenblock fasst mehrere Leerungsdatensätze zusammen und ist durch einen CRC gesichert

- Ein autorisierter Benutzer kann die Gültigkeits- und Integritätsüberprüfung verifizieren.

Neben der Identifikation von Abfallgefäßen kann das Gassner-System auch bei anderen Behältern angewendet werden.

2.3.1.2 Definition und Beschreibung der Komponenten

Das Abfallbehälter-Identifikations-System besteht aus folgenden Komponenten:

- ID-Tag mit den Identifizierungsdaten des Abfallbehälters.
- Fahrzeug mit dem (ID-Tag-) Reader, Fahrzeugrechner und einem optionalen Wiege-, Volumenmess- oder ähnlichem System. Die Fahrzeugsoftware ist installiert auf dem Fahrzeugrechner. Der Fahrzeugrechner an dem auch die genannten optionalen Komponenten angeschlossen werden können und auf dem die Fahrzeugsoftware installiert ist, wird in weiterer Folge als GFE (Gassner Fahrzeug Einheit) bezeichnet.
- Bürorechner im Büro. Das Sicherheitsmodul und die Bürosoftware auf dem Bürorechner sind installiert.

Die folgende Abbildung gibt einen Überblick über das Abfallbehälter-Identifikations-System.

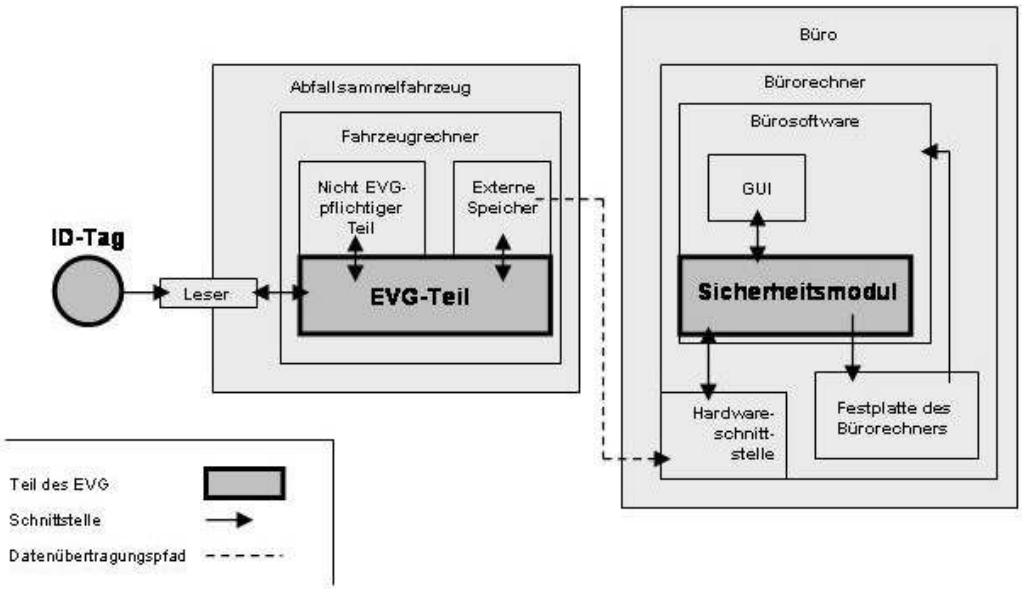

Abbildung 1 - Abfallbehälter-Identifikations-System

Das Abfallbehälter-Identifikations-System 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. Das System kann optional z.B. ein Wiege- oder Volumenmesssystem enthalten, um auch zur gewichtsbezogenen Abrechnung benutzt zu werden. Andere ergänzende Verfahren sind in der Zukunft möglich.

Die Abfallbehälter werden mit einem Datenträger (ID-Tag) ausgestattet. Der 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 Leser ausgelesen. Die dabei möglichen Übertragungsfehler und eventuelle Manipulationen werden von der Fahrzeugsoftware 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.

2.3.1.3 Anmerkungen zu der eingesetzten Hardware

Bürorechner:

Der Bürorechner ist ein handelsüblicher PC mit jeweils aktuellem Windows Betriebssystem.

Bürorechner – Externer Speicher:

Handelsübliche Festplatte des Bürorechners. Optional mit angeschlossenen Backup Systemen (RAID oder externe Festplatte etc.)

Bürorechner – Hardwareschnittstelle:

Die Übertragung der Daten von der Fahrzeugsoftware zum Bürorechner kann mit unterschiedlicher Hardware durchgeführt werden. Die Daten können z.B. drahtlos über GSM bzw. GPRS oder auch durch eine Einheit übertragen werden, die robuste Speicherkarten beschreiben und lesen kann. Wichtig ist, dass unabhängig von der eingesetzten Hardwareschnittstelle, die Daten immer über das Sicherheitsmodul laufen müssen. Das Sicherheitsmodul ist daher verantwortlich, dass der Vorgang der Generierung von Leerungsdaten im Sinne der EVG sicher durchgeführt werden kann. Siehe auch 2.3.1.4 ‚Generierung von Leerungsdatensätzen' bzw. 2.3.3. ‚Abgrenzung des EVG'.

Fahrzeugrechner – Speicher

Der Fahrzeugrechner besitzt sowohl interne als auch externe Speicherbereiche. Diese werden sinngemäß auch als Primärer Speicher und Sekundärer Speicher bezeichnet. Der interne und externe Speicher ist außerdem dafür verantwortlich, die Leerungsdaten redundant zu speichern. Der EVG Teil der Fahrzeugsoftware implementiert alle Voraussetzungen um das redundante Speichern der Leerungsdatensätze im Speicher zu gewährleisten. Damit wird unter anderen den Sicherheitsrichtlinien P.SAVE und TSF_SAFE entsprochen. Die Fahrzeugsoftware stellt außerdem, zusammen mit der Sicherheitssoftware am PC, sicher dass bei Übertragung der Leerungsdatensätze kein Datenverlust auftreten kann. Damit wird der Sicherheitsrichtlinie FRU_FLT.1 entsprochen.

Art und Typ des Primären Speichers und des Sekundären Speichers

Primärspeicher: PCMCIA SMRAM CARD mit Kapazitäten von 64KB bis 1MB

Sekundärspeicher: kontaktlose MEMO CARD 2MB oder SD CARD > 128MB

Art der Transponder (ID-Tags) bzw Art des Lesegerätes

Punkt 2.3.2 ‚Definition des EVG' (Transponder ID-Tag) definiert die Art der verwendeten Transponder bzw. die Art des zugehörigen Lesegerätes.

2.3.1.4 Generierung von Leerungsdatensätzen

Zum Nachweis der Gültigkeit eines Leerungsdatensatzes wird sofort bei dessen Erstellung die Kennung der im Fahrzeug befindlichen GFE eingefügt.

Die Leerungsdatensätze werden in Leerungsdatenblöcken vom Fahrzeugrechner über das Sicherheitsmoduls an die Bürosoftware übermittelt. Die Fahrzeugsoftware sorgt durch geeignete Maßnahmen (z.B. Backup der Daten) dafür, dass die Übermittlung auch nach einem Datenverlust im Primärspeicher möglich ist. Bei der Übermittlung der Leerungsdatenblöcke an die Bürosoftware wird durch das Sicherheitsmodul

sichergestellt, dass nur die in einem registrierten Fahrzeug erstellten Leerungsdatensätze als gültig erkannt werden. Zusätzlich werden die bei einer Übertragung möglichen Fehler erkannt.

Die Leerungsdatensätze können von der Bürosoftware in dem Bürorechner gespeichert werden. Sie können optional ausgewertet werden, um z.B. weitere denkbare Angriffe (ungültige, kopierte Identifikationsdaten usw.) abzuwehren. Die Leerungsdatensätze, die in den Leerungsdatenblöcken enthalten sind, werden an externe Systeme (z.B. bei den Kommunen) zur Abrechnung mit dem Kunden weitergeleitet. Solche externen Systeme können neben der Abrechnungs- auch andere Funktionalitäten (z.B. das Erkennen von möglichem Missbrauch durch Wiedereingespielte Leerungsdatensätze usw.), die die Sicherheitsfunktionalität des Evaluierungsgegenstands ergänzen, bereitstellen.

Der 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 Angriffspotential 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.

2.3.2 Definition des EVG

Der EVG setzt sich aus folgenden Komponenten zusammen:

Transponder (ID-Tag) bzw. Art des Lesegerätes:

Bei den ID-Tags handelt es sich um passive Transponder, die am oder im zu identifizierenden Gegenstand befestigt werden. Alle Transponder besitzen eine Unique ID mit einer Datenstruktur von mind. 64 Bit und sind im Gassner System und im Sinne des EVG nur lesbar (Read Only und OTP).

Der Markt bietet sowohl ReadOnly Transponder als auch beschreibbare Transponder an. Technisch gesehen steht es dem Kunden offen, beide Arten von Transponder einzusetzen. Der beschreibbare Teil eines Transponders vom Typ Read/Write ist aber nicht Teil des EVG. Deshalb wird in diesem Dokument und im Sinne des EVG nur auf Transponder vom Typ ReadOnly verwiesen. Weitere Angaben zu den Transpondern erfolgen im Rahmen der Funktionalen Spezifikation (FSP).

In der evaluierten Version können folgende Transponder zum Einsatz kommen:

Typ	Lieferant	Bezeichnung
Stifttransponder	Envicomp	TI-134 2Khz-HDX-R/O-Wedge
23mm Glastransponder	Texas Instruments	RI-TRP-REHP-30
32mm Glastransponder	Texas Instruments	RI-TRP-RE2B-30
120mm Kunststoffrohr	Texas Instruments	RI-TRP-R9TD-16
Schlüsselanhänger	Texas Instruments	RI-TRP-RFoB

Art des Lesers: Das Lesegerät ist nicht Teil des EVG. Gassner liefert zurzeit ein Lesegerät von Texas Instruments vom Typ (TIRIS) TI-RFID in normaler Ausführung, in der Version POWER-TIRIS, oder ein ähnliches Fabrikat. Der EVG-Teil der Fahrzeugsoftware interpretiert die übergebenen Daten vom Lesegerät im Sinne des EVG.

EVG-Teil der Fahrzeugsoftware:

Die Fahrzeugsoftware besteht aus Teilen die EVG-pflichtig sind und aus Teilen die nicht EVG-pflichtig sind [siehe auch Abbildung 1 im Abschnitt 2.3.1.2]. Bei dem EVG Teil der Fahrzeugsoftware handelt es sich namentlich um folgende Datei bzw. Dateiversion der Gassner Fahrzeugsoftware: DMA02 JUNIOR-V2.04. Zusätzlich werden die Handbücher zu DMA02 Junior mitgeliefert.

In der Tabelle ‚GFE-Bestandteile und Versionen' im Abschnitt 2.2.3 sind alle Versionen übersichtlich zusammengefasst bzw. gelistet.

Sicherheitsmodul:

Bei dem Sicherheitsmodul handelt es sich um den EVG-Anteil der Bürosoftware [siehe Tabelle Bestandteile und Versionen des Sicherheitsmoduls im Abschnitt 2.2.3.], inklusive Installations- und Benutzerhandbuch.

Der EVG hat folgende Aufgaben:

- Überprüfen der eingelesenen Identifikationsdaten (AT1) mit angehängtem CRC auf Integrität.
- Generieren des Leerungsdatensatzes AT durch Einfügen der Identifikationsdaten AT1 und der Zuordnung (GFE Kennung, Zeitstempel) AT2. Anhängen des CRC über den Leerungssatz AT mit Prüfung auf Integrität.
- Speichern der Leerungsdatensätze AT im GFE Speicher.
- Auslesen der Leerungsdatensätze AT vom GFE Speicher und Bildung von Leerungsdatenblöcken zur Übertragung in das Sicherheitsmodul des Bürorechners über die im Sicherheitsmodul ausgewählte Hardwareschnittstelle.
- Prüfen der Integrität der Gesamtübertragung zwischen GFE Speicher und Sicherheitsmodul durch das Sicherheitsmodul
- Prüfen des Zuordnungsteils AT2 auf Gültigkeit der Leerungsdatensätze AT
- Prüfen des CRC Wertes auf Integrität der AT Datensätze durch das Sicherheitsmodul.

  Dies beinhaltet auch die Möglichkeit die Datensätze und insbesondere den CRC Wert sowohl manuell bzw. visuell zu überprüfen.

  Die Sicherheitssoftware am Bürorechner stellt dazu (= automatische und manuelle Überprüfung der Daten auf Integrität) ein geeignetes Interface zur Verfügung um unter anderem die Sicherheitsrichtlinie TSF_AT_CHK zu erfüllen.
- Prüfen des CRC-Wertes auf Integrität der Leerungsdatenblöcken AT+ durch das Sicherheitsmodul.
- Kennzeichnung der Leerungsdatensätze AT bezüglich Gültigkeit und Integrität durch das Sicherheitsmodul.
- Die Leerungsdatensätze werden im Fahrzeugrechner in unterschiedlichen Speichern (Primär- und Sekundärspeicher) redundant abgelegt und verwaltet.
- Verifizierbarkeit der Gültigkeits- und Integritätsprüfung durch einen autorisierten Benutzer

2.3.3 Abgrenzung des EVG

Der Evaluierungsgegenstand ist ein Produkt im Sinne der Common Criteria. Der Evaluierungsgegenstand besteht aus dem ID-Tag, dem „EVG-Teil der Fahrzeugsoftware" und dem Sicherheitsmodul am PC. Alle anderen Komponenten (siehe auch Abbildung 1) sind nicht Bestandteil des Evaluierungsgegenstands und gehören zu dessen Umgebung.

Der EVG ist verantwortlich und allein in der Lage dafür zu sorgen, dass die Daten direkt vom Leser des Fahrzeugs in den EVG-Teil der Fahrzeugsoftware gelangen und dort die Sicherheitsfunktionalität des EVG durchlaufen, bevor sie in den GFE Speicher des Fahrzeugs geschrieben werden.

Der EVG ist verantwortlich und allein in der Lage dafür zu sorgen, dass alle Leerungsdaten, die in den Bürorechner gelangen, als erstes die Funktionalität (Integritäts- und Gültigkeitsüberprüfung) des Sicher-

heitsmoduls durchlaufen, bevor sie im Bürorechner weiterverarbeitet werden können.

Der Evaluierungsgegenstand hat folgende externe Schnittstellen:

- Eine unidirektionale Schnittstelle zwischen dem ID-Tag und dem Leser. Sie ist unidirektional, da nur Daten vom Transponder zum Leser gelangen.
- Eine bidirektionale Schnittstelle zwischen dem Leser und dem EVG-Teil der Fahrzeugsoftware. Sie ist bidirektional, da der Leser vom EVG angesprochen wird und Identifikationsdaten vom Leser zum EVG geschickt werden.
- Eine bidirektionale Schnittstelle zwischen dem EVG-Teil der Fahrzeugsoftware und den Nicht-EVG Teilen der Fahrzeugsoftware. Sie ist bidirektional, da Parameter sowie optionale Daten und Steuerkommandos zwischen den beiden Teilen ausgetauscht werden.
- Eine bidirektionale Schnittstelle zwischen EVG-Teil der Fahrzeugsoftware und den externen Speichern. Sie ist bidirektional, da die Leerungsdatenblöcke AT+ auf die externen Speicher übertragen werden und anschließend durch ein Read after Write der Erfolg des Speichervorganges überprüft wird.
- Eine bidirektionale Schnittstelle zwischen der Hardwareschnittstelle des Bürorechners und dem Sicherheitsmodul. Sie ist bidirektional, da der Aufruf durch das Sicherheitsmodul erfolgt und die Daten via Hardwareschnittstelle am PC aus dem externen Speicher der Fahrzeugsoftware gelesen werden.
- Eine unidirektionale Schnittstelle zwischen dem Sicherheitsmodul und dem externen Speicher des Bürorechners. Sie ist unidirektional, da die geprüften Daten lediglich auf dem externen Speicher abgelegt werden.
- Eine birektionale Schnittstelle zwischen der Bürosoftware (GUI) und dem Sicherheitsmodul des Bürorechners. Sie ist bidirektional, da Integritätverletzungen in der Bürosoftware angezeigt werden, und Daten manuell aus der Sicherungsdatei importiert werden können.

Die physischen Kanäle ID-Tag - Fahrzeugsoftware und Fahrzeugsoftware - Sicherheitsmodul sind nicht Bestandteil des Evaluierungsgegenstands. Nur die externen Schnittstellen werden betrachtet. Weitere Schnittstellen, insbesondere die zu den kommunalen Abrechnungsstellen, sind nicht Bestandteil der Evaluierung. Die Bürosoftware ist auch kein Bestandteil des Evaluierungsgegenstandes.

3 Postulat der Übereinstimmung mit den CC

Die Evaluierung des EVG erfolgt auf Basis der Common Criteria (CC)

- Common Criteria for Information Technology Security Evaluation, Part 1, Version 3.1 Revision 1, CCMB-2007-09-001 September 2007
- Common Criteria for Information Technology Security Evaluation, Parts 2 and 3, Version 3.1 Revision 2, CCMB-2007-09-002/003 September 2007
- Common Evaluation Methodology for Information Technology Security Evaluation,
- Version 3.1 Revision 2, CCMB-2007-09-004, September 2007

Diese Sicherheitsvorgaben sind CC Teil 2 erweitert. Bei den funktionalen Sicherheitsanforderungen wurde die Komponente FDP_ITT.5 konform zum Schutzprofil „Protection Profile Waste Bin Identification Systems WBIS-PP, Version 1.04“ (PP) ergänzt.

Diese Sicherheitsvorgaben sind CC Teil 3 konform.

Die Sicherheitsvorgaben postulieren nachweisbare Konformität (demonstrable conformance) zum Schutzprofil „Protection Profile Waste Bin Identification Systems WBIS-PP, Version 1.04“ [3].

Zusätzlich zu den beschriebenen IT-Sicherheitsanforderungen sind in Absprache mit der Zertifizierungsbehörde folgende Annahmen, Ziele und Anforderungen in diesen Sicherheitsvorgaben hinzugekommen:

Annahmen	A.Installation: Korrekte Inbetriebnahme	siehe Abschnitt 4.4
Umgebungssicherheitsziele	OE.Installation: Korrekte Inbetriebnahme	siehe Abschnitt 5.2
Sicherheitsanforderungen an die Nicht-IT-Umgebung	R.Installation: Korrekte Inbetriebnahme	siehe Abschnitt 5.4

Die angestrebte Vertrauenswürdigkeitsstufe ist EAL1 erweitert um ASE_SPD.1, ASE_REQ.2 und ASE_OBJ.2.

4 Definition der Sicherheitsumgebung

4.1 Einleitung

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.

4.1.1 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 Zuordnungsteil (GFE Kennung), Zeitstempel (Datum und Uhrzeit)) des Leerungsvorgangs

AT+ Bei der Übertragung der Leerungsdatensätze AT von der Fahrzeugsoftware zum Sicherheitsmodul im Büro werden die Leerungsdatensätze zu Leerungsdatenblöcken AT+ zusammengefasst, wobei jeder Leerungsdatenblock AT+ einen oder mehrere Leerungsdatensätze AT enthält. Der Leerungsdatenblock AT+ ist ein schutzwürdiges Objekt in GWBIS bei der Kommunikation zwischen der Fahrzeugsoftware und dem Sicherheitsmodul.

Es gibt zwei Arten von Leerungsdatensätzen:

a) abrechnungsrelevante Datensätze (bzw. für die Abrechnung geeignete Daten)

b) nicht abrechnungsrelevante Datensätze (das sind Datensätze zur Information, Steuerung oder als fehlerhaft gekennzeichnete Daten)[2]. Ein solcher Datensatz enthält möglicherweise keine Identifikationsdaten AT1.

Ein abrechnungsrelevanter Datensatz muss zwingend gültige Identifikationsdaten AT1 und die Zuordnung AT2 enthalten[3]. Im Gassner-System sind abrechnungsrelevante bzw. nicht abrechnungsrelevante Datensätze als solche eindeutig gekennzeichnet.

4.1.2 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.

4.1.3 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.

[2] Der nicht abrechnungsrelevanten Datensatz wird als solcher gekennzeichnet und dem Benutzer zur Verfügung gestellt.
[3] Und kann zusätzliche, optionale Daten enthalten.

4.2 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. Denkbar sind hier folgende Beispiele:

- ein direkt ausgeführter Schlag auf den Transponder (z.B. durch einen Hammerschlag auf das Transpondergehäuse) oder
- das Fehlen eines Transponders (durch Entfernen des Transponders vom Gefäß).

T.Jam#1 ***Gestörte Identifikationsdaten***

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

Diese elektromagnetische Strahlung resultiert zum Beispiel von

- elektrischen Geräten, wie Mobiltelefone, deren Strahlung einer Sendequelle im gleichen Frequenzbereich des Lesers entspricht,
- weiteren Transponder im Lesefeld, die die Übertragung stören können

T.Create ***Ungültige Leerungsdatenblöcke***

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

- Eine solche Manipulation kann auch. durch eine elektromagnetische Entladung an einem elektromagnetischen Speicher (z.B. Speichermodul) verursacht werden.

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

4.3 Organisatorische Sicherheitspolitik

Die folgende Regel wird für den EVG formuliert:

P.Safe ***Fehlertoleranz***

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

4.4 Annahmen

A.Id ***ID-Tag***

Der ID-Tag befindet sich fest am Abfallbehälter. Die Identifizierungsdaten (AT1) des Abfallbehälters sind in dem ID-Tag gespeichert und werksseitig durch einen CRC geschützt. 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, initialisieren[4] 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 der Benutzer bzw. das Wartungspersonal (S.Trusted) direkten Zugang zu allen Komponenten des Evaluierungsgegenstands, ausgenommen der ID-Tag, haben. Die Beeinflussung der internen Verbindungskanäle innerhalb der IT-Struktur des Bürorechners durch einen potenziellen Angreifer (S.Attack) ist aufgrund geeigneter Maßnahmen ausgeschlossen.

A.Check ***Überprüfung der Vollständigkeit***

Der Benutzer (S.Trusted) prüft in regelmäßigen Abständen, ob alle Leerungsdatensätze (AT) von dem Fahrzeugrechner übertragen worden sind (Vollständigkeit der Übertragungen). Erkannte Datenverluste werden vom Benutzer in einem bestimmten Zeitraum durch erneutes Abrufen beim Fahrzeugrechner behoben. Dieser Zeitraum entspricht der Kapazität des jeweiligen Speichers im Fahrzeugrechner, der zur Speicherung der Leerungsdatensätze (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.

A.Installation ***Korrekte Inbetriebnahme***

Bei der Inbetriebnahme des Identifikationssystems auf dem Fahrzeug wird sichergestellt, dass die GFE-Kennung und die Adressen der Leser richtig konfiguriert und zugeordnet sind. Dieses gilt sowohl bei der Neuinstallation, als auch im Service- / Wartungsfall.

[4] Die Inbetriebnahme beinhaltet unter anderem sämtliche Parametrisierungsdaten, wie GFE-Kennung, Adressen der Leser, Schüttungsparameter

5 Sicherheitsziele

Dieser Abschnitt benennt und definiert die Sicherheitsziele für den EVG und seine Umgebung. Die Sicherheitsziele spiegeln die angegebene Absicht wider und begegnen den identifizierten Bedrohungen ebenso, wie sie den identifizierten organisatorischen Sicherheitspolitiken und Annahmen entsprechen.

5.1 EVG-Sicherheitsziele

Die Sicherheitsziele für den EVG müssen (in der gewünschten Stufe) festlegen, in welcher Weise der EVG Bedrohungen begegnet und die OSPs unterstützt. Jedes Ziel muss auf Aspekte von ermittelten Bedrohungen zurückgeführt werden, um vom EVG durchgesetzt zu werden, sowie auf Aspekte der OSPs, die durch den EVG erfüllt werden müssen. So besehen bilden die Sicherheitsziele für den Leser eine Verbindung von den identifizierten Sicherheitsbedürfnissen zu den IT-Sicherheitsanforderungen.

OT.Inv#1 ***Erkennen ungültiger Identifikationsdaten***

Der EVG muss Manipulationen an Identifikationsdaten erkennen (AT1), die in einem ID-Tag gespeichert sind, oder während sie zwischen ID-Tag und Leser im Fahrzeug übertragen werden.

OT.Inv#2 ***Erkennen von ungültigen Leerungsdatenblöcken***

Der EVG muss jeden Versuch einer Übermittlung willkürlicher (z.B. ungültiger) Leerungsdatenblöcke (AT+) an das Sicherheitsmodul erkennen. Der EVG muss Manipulationen an empfangenen Leerungsdatensätzen (AT) während des Leerungsprozesses und Speicherns im Fahrzeug erkennen, sowie Manipulationen der Leerungsdatenblöcke (AT+) bei zufälligen Störungen während des Transfers von der Fahrzeugsoftware zum Sicherheitsmodul.

OT.Safe ***Fehlertoleranz***

Die Fahrzeugsoftware als Teil des EVG muss sicherstellen, dass die Daten der Leerungsdatensätze (AT) durch eine redundante Sicherung in einem sekundären Speicher gesichert werden, auf eine Weise, dass der Transfer der Leerungsdatensätze (AT) von der Fahrzeugsoftware zum Sicherheitsmodul möglich ist, sofern Leerungsdatensätze (AT) im Primärspeicher der Fahrzeugsoftware verloren gehen.

5.2 Umgebungssicherheitsziele

OE.Id ***ID-Tag***

Der ID-Tag ist an einem Abfallgefäß befestigt. Die Identifikationsdaten (AT1) des Abfallgefäßes sind im ID-Tag gespeichert und werksseitig durch einen CRC geschützt. Ausschließlich ID-Tags mit einmaligen Identifikationsdaten dürfen benutzt werden. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des Evaluierungsgegenstandes sicherzustellen.

OE.Trusted ***Vertrauenswürdiges Personal***

Durch organisatorische Mittel muss sichergestellt sein, dass die Besatzung des Sammelfahrzeuges und der Benutzer des Bürorechners autorisiert und vertrauenswürdig sind (S.Trusted). Alle Personen, die das System installieren, initialisieren und warten, müssen ermächtigt und vertrauenswürdig sein (S.Trusted). Alle Personen, die für die Sicherheit der EVG-Umgebung verantwortlich sind, müssen ermächtigt und vertrauenswürdig sein (S.Trusted).

OE.Access ***Zugangsschutz***

Die Umgebung muss durch angemessene Mittel sicherstellen (Verschluss, Passwort zur Zugangskontrolle usw.), dass lediglich Benutzer oder Servicemitarbeiter (S.Trusted) direkten Zugang zu den Komponenten des EVG haben, der ID-Tag ist davon ausgenommen. Die Manipulation von internen Kommunikationswegen durch potentielle Angreifer (S.Attack) innerhalb der IT-Struktur von Bürorechnern, muss durch ausreichende Maßnahmen ausgeschlossen werden.

OE.Check ***Vollständigkeitsprüfung***

Es muss sichergestellt werden, dass Benutzer (S.Trusted) in regelmäßigen Abständen prüfen, ob die von der Fahrzeugsoftware zum Sicherheitsmodul im Büro übermittelten Daten vollständig sind. Der festgestellte Verlust von Daten muss durch eine erneute Datenübermittlung wiederhergestellt werden. Die Intervalle müssen der Kapazität des entsprechenden Speichers vom Fahrzeugrechner angepasst sein.

OE.Backup ***Datensicherung***

Es muss sichergestellt werden, dass der Benutzer (S.Trusted) in regelmäßigen Abständen Sicherungskopien von den durch den EVG erzeugten Daten macht.

OE.Installation ***Korrekte Inbetriebnahme***[5]

Es muss sichergestellt werden, dass bei Installation des Identifikationssystemes auf dem Fahrzeug die GFE-Kennung und die Adressen der Leser richtig konfiguriert und zugeordnet sind. Dieses gilt sowohl bei der Neuinstallation, als auch im Service- / Wartungsfall.

5.3 Erläuterung der Sicherheitsziele

5.3.1 Abdeckung der Sicherheitsziele

Bedrohungen – Annahmen – Politiken Sicherheitsziele	OT.Inv#1	OT.Inv#2	OT.Safe	OE.Id	OE.Trusted	OE.Access	OE.Check	OE.Backup	OE.Installation
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	
A.Installation									x
P.Safe			x						

Tabelle 2 - Darstellung der Sicherheitsziele

[5] Dieses Umgebungssicherheitsziel ist nicht im PP [3] enthalten. Es wurde hier neu definiert.

5.3.2 Hinlänglichkeit der Sicherheitsziele

5.3.2.1 Hinlänglichkeit der Politiken und Sicherheitsziele

P.Safe (Fehlertoleranz) setzt die Verfügbarkeit von den wichtigen Daten für die Übertragung der Leerungsdatensätze (AT) von der Fahrzeugsoftware zum Sicherheitsmodul durch, ebenso wie im Falle des Verlustes dieser Daten im Primärspeicher der Fahrzeugsoftware, indem die Daten im Sekundärspeicher behalten werden. Dies wiederholt sich exakt im Ziel OT.Safe, somit ist dieses Ziel hinlänglich für P.Safe.

5.3.2.2 Hinlänglichkeit der Bedrohungen und Sicherheitsziele

T.Man (Manipulierte Identifikationsdaten) behandelt Angriffe, in denen Identifikationsdaten (AT1) innerhalb der Identifikationseinheit manipuliert sind. Entsprechend OT.Inv#1 werden die beschädigten Identifikationsdaten (AT1) durch den EVG erkannt, was der Bedrohung T.Man direkt entgegen wirkt.

T.Jam#1 (Gestörte Identifikationsdaten) behandelt Angriffe, in denen (durch zufällige Störung) verfälschte Identifikationsdaten (AT1) dem Leser übergeben werden. Entsprechend OT.Inv#1 werden die gestörten Identifikationsdaten durch den EVG erkannt, was der Bedrohung T.Jam#1 direkt entgegen wirkt.

T.Create (Ungültige Leerungsdatenblöcken) behandelt Angriffe, in denen willkürlich Leerungsdaten kreiert und anschließend in das Sicherheitsmodul eingebracht werden. Entsprechend OT.Inv#2 wird jeder Versuch, willkürliche (z.B. ungültige) Leerungsdatenblöcke in das Sicherheitsmodul einzubringen erkannt, was der Bedrohung T.Create direkt entgegen wirkt.

T.Jam#2 (Verfälschte Leerungsdatensätze) richtet sich auf Angriffe in denen gespeicherte Leerungsdatensätze (AT) während der Bearbeitung und Speicherung innerhalb des Fahrzeuges verfälscht werden oder die Übertragung der Leerungsdatenblöcke zum Sicherheitsmodul gestört ist. Entsprechend OT.Inv#2 werden Verfälschungen von gespeicherten Leerungsdatensätzen während der Bearbeitung und Speicherung innerhalb des Fahrzeuges, sowie der Leerungsdatenblöcke, die während der Übertragung zum Sicherheitsmodul verfälscht werden, durch den EVG erkannt, was der Bedrohung T.Jam#2 direkt entgegen wirkt.

5.3.2.3 Hinlänglichkeit der Annahmen und Sicherheitsziele

A.Id (ID-Tag) stellt sicher, dass die Identifikationseinheit am Abfallgefäß befestigt ist, welches sie identifiziert, und dass die Daten der installierten Identifikationseinheit einmalig und werksseitig durch einen CRC geschützt sind. Die Übereinstimmung zwischen den Identifikationsdaten und dem Gebührenpflichtigen wird über organisatorische Mittel durchgesetzt. Da das Ziel OE.Id die exakt gleichen Angaben enthält, ist es hinlänglich für A.Id.

A.Trusted (Vertrauenswürdiges Personal) stellt sicher, dass alle Personen (außer dem Angreifer) vertrauenswürdig sind. Das Ziel OE.Trusted enthält exakt die gleiche Angaben, und ist somit hinlänglich für A.Trusted.

A.Access (Zugangsschutz) stellt sicher, dass der Zugang zum EVG, mit Ausnahme der Identifikationseinheit, ausschließlich auf vertrauenswürdiges Personal beschränkt ist. Sie schließt ebenfalls die Fähigkeit des Angreifers aus, die internen Verbindungskanäle innerhalb der IT-Struktur des Bürorechners zu beeinflussen. Das Ziel OE.Access enthält exakt die gleichen Angaben, und ist somit hinlänglich für A.Access.

A.Check (Überprüfung der Vollständigkeit) stellt sicher, dass der Benutzer in regelmäßigen Intervallen prüft, ob die vom Fahrzeug zum Büro übertragenen Daten vollständig sind. Erkannte Datenverluste werden durch eine erneute Übertragung der Daten abgedeckt. Dieser Zeitraum stimmt überein mit der Kapazität des entsprechenden Speichers im Fahrzeugrechner. Das Ziel OE.Check enthält exakt die gleichen Angaben, und ist somit hinlänglich für A.Check.

A.Backup (Datensicherung) stellt sicher, dass der Benutzer in regelmäßigen Abständen Sicherungskopien der vom EVG erzeugten Daten anlegt, da der EVG keine entsprechende Funktion anbietet. Das Ziel OE.Backup enthält exakt die gleichen Angaben, und ist somit hinlänglich für A.Backup.

A.Installation (Korrekte Inbetriebnahme) stellt sicher, dass bei der Inbetriebnahme und beim Service-/ Wartungsfall die richtige GFE-Kennung im Fahrzeug korrekt und vollständig gesetzt wird. Sie stellt außerdem sicher, dass bei Inbetriebnahme und beim Service-/ Wartungsfall die Adressen der Leser richtig gesetzt sind. Das Ziel OE.Installation enthält exakt die gleichen Angaben und ist somit hinlänglich für A.Installation.

5.4 Sicherheitsanforderungen an die Nicht-IT-Umgebung

R.Id ***Identifikationseinheit***

Der Benutzer muss folgendes sicherstellen: Die Identifikationseinheit sollte am Abfallgefäß, das durch die enthaltenen Identifikationsdaten erkannt werden soll, befestigt sein. Die in den installierten Identifikationseinheiten gespeicherten Identifikationsdaten sind einmalig d.h. immer eindeutig. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des Evaluierungsgegenstandes sicherzustellen.

R.Trusted ***Vertrauenswürdiges Personal***

Personen, die das Fahrzeug und das Sicherheitsmodul bedienen, installieren, initialisieren und warten, müssen autorisiert und vertrauenswürdig sein. Alle für die Sicherheit der Umgebung verantwortlichen Personen sind autorisiert und vertrauenswürdig.

R.Access ***Zugriffsschutz***

Die Umgebung muss durch geeignete Maßnahmen sicherstellen, dass nur der Benutzer und das Wartungspersonal direkten Zugang zu den Komponenten des EVG haben, ausgenommen die Identifikationseinheit. Die Umgebung muss jede Art von Beeinflussung der internen Kommunikationswege in den Bürorechnern verhindern.

R.Check ***Überprüfung der Vollständigkeit***

Der Benutzer muss in regelmäßigen Abständen die vollständige Übertragung der Leerungsdatensätze (AT) zwischen Fahrzeug und Büro prüfen. Der Benutzer muss jene Daten abrufen, die er als noch nicht vom Fahrzeug zum Büro übertragen festgestellt hat, um sie von hier aus wiederherzustellen. Der Zeitraum der Prüf- und Abrufaktionen muss mit der vorhandenen Speicherkapazität des Fahrzeugrechners übereinstimmen, mit dem Ziel, Leerungsdatensätze (AT) zu speichern.

R.Backup ***Datensicherung***

Der Benutzer soll die vom EVG erzeugten Daten regelmäßig in geeigneten Archiven sichern.

R.Installation ***Korrekte Inbetriebnahme***[6]

Bei Installation des Identifikationssystems auf dem Fahrzeug müssen die GFE-Kennung und die Adressen der Leser richtig konfiguriert und zugeordnet werden. Die korrekte Installation ist anschließend auf Richtigkeit und Vollständigkeit zu überprüfen. Dieses gilt sowohl bei der Neuinstallation, als auch im Service- / Wartungsfall.

[6] Diese Sicherheitsanforderung ist nicht in den PP [3] enthalten. Es wurde hier neu definiert.

6 IT-Sicherheitsanforderungen

Dieses Kapitel enthält die funktionalen Sicherheitsanforderungen und Anforderungen an die Vertrauenswürdigkeit des EVG und seine Umgebung.

6.1 Funktionale Sicherheitsanforderungen an den EVG

In diesem Kapitel sind Komponenten der funktionalen Sicherheitsanforderungen angegeben. Sie wurden aus den Common Criteria Teil 2 [1] entnommen, mit Ausnahme der Komponente FDP_ITT.5, die im Schutzprofil „Protection Profile Waste Bin Identification Systems WBIS-PP, Version 1.04“ [3] definiert wird.

6.1.1 Datenauthentisierung (FDP_DAU)

6.1.1.1 Einfache Datenauthentisierung (FDP_DAU.1)

FDP_DAU.1.1 Die TSF müssen die Fähigkeit zur Generierung von Nachweisen als Gültigkeitsgarantie von *Aufzeichnungen von Leerungsdatensätzen AT und Leerungsdatenblöcken AT+* bereitstellen.

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

Anwendungshinweis: Jeder vom EVG generierte Leerungsdatensatz AT enthält ein Gültigkeitsmerkmal welches vom EVG für jeden einzelnen Leerungsdatensatz explizit geprüft wird. Das Gültigkeitsmerkmal eines jeden Leerungsdatensatzes stellt somit gleichzeitig das Gültigkeitsmerkmal für den umfassenden Leerungsdatenblock dar.

6.1.2 EVG-interner Transfer (FDP_ITT)

6.1.2.1 Schutz der internen Transferintegrität (FDP_ITT.5) (Ergänzung zu CC Teil 2)

FDP_ITT.5.1 Die TSF müssen die *Datenintegritätspolitik* durchsetzen, um die Modifikation von Benutzerdaten zu verhindern, wenn diese zwischen materiell getrennten Teilen des TOE (EVG) übertragen werden.

Die folgende funktionale Sicherheitspolitik (SFP) formuliert die ‚Datenintegritätspolitik’ mit der Anforderung “Schutz der internen Transferintegrität (FDP_ITT.5)” wie folgt:

- *Benutzerdaten (AT1 und AT+) müssen geschützt werden, um ihre Integrität zu wahren.*

Anwendungshinweis: Sowohl der EVG Teil der Fahrzeugsoftware GFE als auch das Sicherheitsmodul am PC schützen die Benutzerdaten (AT1 und AT+) in geeigneter Weise, um ihre Integrität zu wahren. Die zu schützenden Daten können weder verändert noch verfälscht werden und nur von authorisierten Benutzern eingesehen werden.

Anwendungshinweis: Die Übertragung von Leerungsdatenblöcken zwischen dem EVG Teil der Fahrzeugsoftware und dem Sicherheitsmodul am PC wird durch geeignete Maßnahmen geschützt, um sicherzustellen, dass die Integrität der gesamten Übertragung gewährleistet ist.

6.1.3 Integrität der gespeicherten Daten (FDP_SDI)

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

FDP_SDI.1.1 Die TSF müssen die in Containern, welche von der TSF kontrolliert werden, gespeicherten Benutzerdaten auf *zufällige Manipulation* bei allen Objekten auf Basis folgender Attribute überwachen:

- *Die Identifikationsdaten AT1 innerhalb der Identifikationseinheit und die Aufzeichnung von Leerungsdatensätzen AT während der Speicherung im Fahrzeug.*

Anwendungshinweis: Sowohl der EVG Teil der Fahrzeugsoftware GFE als auch das Sicherheitsmodul am PC stellen sicher, dass Identifikationsdaten in geeigneter Weise überwacht werden und vor Manipulation geschützt werden.

6.1.4 Fehlertoleranz (FRU_FLT)

6.1.4.1 Verminderte Fehlertoleranz (FRU_FLT.1)

FRU_FLT.1 Die TSF müssen den Betrieb von dem Transfer von Leerungsdatenblöcken (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul mit Hilfe der im sekundären Speicher gespeicherten Daten sicherstellen, wenn die folgenden Fehler auftreten:

- *Verlust von Benutzerdaten im Primärspeicher der Fahrzeugsoftware*

Anwendungshinweis: Sowohl der EVG Teil der Fahrzeugsoftware GFE als auch das Sicherheitsmodul am PC stellen sicher dass Benutzerdaten nach Verlust im Primärspeicher jederzeit rekonstruiert werden. Dies geschieht u.a. durch redundante Speicherung der Daten im Primärspeicher und Sekundärspeicher.

6.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Die folgende Tabelle enthält die Vertrauenswürdigkeitsklassen mit den Vertrauenswürdigkeitskomponenten für die angestrebte Evaluierungsstufe EAL1+. Sie entstammen allesamt den Common Criteria (CC), Teil 3 [2].

Klassen	Vertrauenswürdigkeitskomponenten
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_REQ.2, ASE_SPD.1, ASE_TSS.1
ATE	ATE_IND.1
AVA	AVA_VAN.1

Tabelle 3 - Anforderungen der angestrebten Vertrauenswürdigkeitsstufe EAL1+

6.3 Erläuterung der Sicherheitsanforderungen

6.3.1 Abdeckung der Sicherheitsanforderungen

EVG Sicherheitsziele Funktionale Sicherheitsanforderungen an den EVG	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 4 - Gegenüberstellung: Funktionale Sicherheitsanforderungen – Sicherheitsziele

Umgebungssicherheitsziele Sicherheitsanforderungen an die Umgebung	OE.ID	OE.Trusted	OE.Access	OE.Check	OE.Backup	OE.Installation
R.Id	x					
R.Trusted		x				
R.Access			x			
R.Check				x		
R.Backup					x	
R.Installation						x

Tabelle 5 - Gegenüberstellung: Sicherheitsanforderungen – Umgebungssicherheitsziele

6.3.2 Hinlänglichkeit der Sicherheitsanforderungen

6.3.2.1 Hinlänglichkeit der EVG Sicherheitsanforderungen und gegenseitige Unterstützung

OT.Inv#1 (Erkennen ungültiger Identifikationsdaten) zielt auf das Erkennen von manipulierten Identifikationsdaten (AT1) ab. Dies betrifft sowohl den Transfer von Identifikationsdaten von der Identifikationseinheit zum Fahrzeug bzw. der Fahrzeugsoftware als auch den Transfer von Identifikationsdaten zwischen der Fahrzeugeinheit und dem Sicherheitsmodul am PC. Bei dem Transfer zum Sicherheitsmodul am PC werden die Identifikationsdaten als Bestandteil des Leerungsdatensatzes (AT) transferiert.

Die Sicherung der Integrität von den Identifikationsdaten (AT1), die in der Identifikationseinheit gespeichert sind, wird durch FDP_SDI.1 gefordert und begegnet direkt zufälligen Manipulationen dieser Daten. Der Schutz der Benutzerdaten AT1, um ihre Integrität sicherzustellen, wird durch FDP_ITT.5 für den

Transfer zwischen physisch getrennten Teilen des EVG gefordert. Die Datenintegrität sicherzustellen, schützt direkt vor Manipulationen der Daten während des Transfers.

OT.Inv#2 (Erkennen von ungültigen Leerungsdatenblöcken) zielt auf das Erkennen von manipulierten Leerungsdatenblöcken (AT+), die zwischen der Fahrzeugsoftware und dem Sicherheitsmodul übertragen werden, wobei es sich um physisch getrennte Teile des EVG handelt. Der Schutz der Benutzerdaten AT+, um ihre Integrität sicherzustellen, wird durch FDP_ITT.5 für den Transfer zwischen physisch getrennten Teilen des EVG gefordert. Die Datenintegrität sicherzustellen, schützt direkt vor Manipulationen der Daten. OT.Inv#2 spricht auch die Erkennung von ungültigen Leerungsdaten AT während der Bearbeitung und Speicherung im Fahrzeug an, sowie Manipulationen von Leerungsdatenblöcken AT+, die zum Sicherheitsmodul übertragen werden.

Der EVG bietet bezüglich FDP_DAU.1 eine Möglichkeit, einen Nachweis zu kreieren, der vom Benutzer gebraucht werden kann, um die Gültigkeit der Daten nachzuweisen. Der Integritätsschutz der Benutzerdaten (AT), die im Fahrzeug gespeichert sind, wird durch FDP_SDI.1 gefordert und begegnet direkt zufälligen Manipulationen dieser Daten. Die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 unterstützen sich gegenseitig bezüglich der Datenechtheit und Integrität. Daher decken die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 hinlänglich das Sicherheitsziel OT.Inv#2.

OT.Safe (Fehlertoleranz) zielt auf die Verfügbarkeit der für den Transfer der Leerungsdatenblöcke (AT+) wichtigen Daten von der Fahrzeugsoftware zum Sicherheitsmodul, selbst bei Datenverlust im primären Speicher der Fahrzeugsoftware. Die Durchführung dieses Datentransfers mit Hilfe eines sekundären Speichers nach Verlust der Daten im Primärspeicher, wird mit Bezug auf FRU_FLT.1 durch den EVG ermöglicht.

6.3.2.2 Hinlänglichkeit der Anforderungen an die EVG-Umgebung

OE.Id (ID-Tag) wird bereitgestellt durch R.Id, da R.Id fordert, was das Ziel OE.Id anführt.

OE.Trusted (Vertrauenswürdiges Personal) wird bereitgestellt durch R.Trusted, da R.Trusted fordert, was das Ziel OE.Trusted anführt.

OE.Access (Zugriffsschutz) wird bereitgestellt durch R.Access, da R.Access fordert, was das Ziel OE.Access anführt.

OE.Check (Vollständigkeitsprüfung) wird bereitgestellt durch R.Check, da R.Check fordert, was das Ziel OE.Check anführt.

OE.Backup (Datensicherung) wird bereitgestellt durch R.Backup, da R.Backup fordert, was das Ziel OE.Backup anführt.

OE.Installation (Korrekte Inbetriebnahme) wird bereitgestellt durch R.Installation, da R.Installation fordert, was das Ziel OE.Installation anführt.

6.3.3 Explizit dargelegte Sicherheitsanforderungen

Es wurde beschlossen, FDP_ITT.5 umfassend zu definieren, da Teil 2 der Common Criteria keine allgemeine funktionale Sicherheitsanforderung enthält, zur Integritätssicherung von Benutzerdaten während der Übertragung zwischen physisch getrennten Teilen des EVG. Darüber hinaus ist FDP_ITT.5 enger gefasst als FDP_ITT.1, denn es ist nicht unbedingt notwendig, den TOE funktionale Sicherheitspolitiken (SFPs) für Zugriffskontrolle und/oder Informationsflusskontrolle ausführen zu lassen, auch richtet er sich lediglich gegen Manipulationen von Daten.

6.3.4 Vertrauenswürdigkeitsmaßnahmen und Vertrauenswürdigkeitsstufe

Die Vertrauenwürdigkeitsstufe für den EVG ist EAL1 ergänzt um ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2. Diese EAL liefert eine bedeutsame Verbesserung zur Qualitätssicherung eines nicht-evaluierten IT-Produktes oder Systems, indem es eine Absicherung zum korrekten Ablauf bereitstellt,

wobei die Bedrohungen der Sicherheit nicht als ernst angesehen werden, die sich direkt auf den eher geringen Wert des EVG beziehen.

In Tabelle 7 in Abschnitt 7.2 ist nachgewiesen, dass die Maßnahmen zur Vertrauenswürdigkeit die diesbezüglichen Anforderungen erfüllen.

Für einen EVG, der zum Schutz von Identifikationsdaten, Leerungsdatensätzen und Leerungsdatenblökken mit einfachem Schutzbedarf dient, und der nur gegen unabsichtliche oder rein zufällig gegen den EVG gerichtete Bedrohungen schützt, sowie eine einfache organisatorische Sicherheitspolitik umsetzt, die primär Veränderungen und Verluste, z.B. durch technische Effekte oder Defekte basierend auf den in Abschnitt 4.2 beschriebenen Bedrohungen, feststellt, ist eine Evaluation nach der Einstiegsstufe EAL1 erweitert um die Komponenten ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2 ausreichend und angemessen.

Die Erweiterung von EAL1 um die o.a. Komponenten wurde vorgenommen, um eine angemessene Prüfung der in Abschnitt 4 definierten Sicherheitsumgebung des EVG und der darauf aufbauenden Sicherheitsziele und Anforderungen durchzuführen, welche auf Stufe EAL1 der CC Version 3.1 noch nicht gefordert ist.

6.4 Erläuterung der Abhängigkeiten

Die Komponenten der Sicherheitsanforderungen wurden genau wie durch das EAL1 spezifiziert übernommen. Alle Abhängigkeiten sind dadurch komplett erfüllt.

Durch die Ergänzung der Evaluationsstufe um die Vertrauenswürdigkeitskomponenten ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2 entstehen keine weiteren Abhängigkeiten.

Die Abhängigkeiten der funktionalen Anforderungen an den EVG und an seine Umgebung sind nicht vollständig erfüllt. Die nachstehende Tabelle bietet einen Überblick über die Abhängigkeiten und zeigt wie sie erfüllt sind.

Anforderungen	Abhängigkeiten	Erfüllt
FDP_DAU.1	keine Abhängigkeiten	stillschweigend
FDP_ITT.5	keine Abhängigkeiten	stillschweigend
FDP_SDI.1	keine Abhängigkeiten	stillschweigend
FRU_FLT.1	FPT_FLS.1	siehe Besprechung unten

Tabelle 6 - Abhängigkeiten der funktionalen Anforderungen

FRU_FLT.1 fordert vom EVG die sichere Übertragung von der Fahrzeugsoftware zum Sicherheitsmodul, selbst wenn die Daten innerhalb der Fahrzeugsoftware verloren gehen. Diese Anforderung wird verfolgt, um die organisatorische Sicherheitspolitik zu erfüllen, welche sich mehr auf die Verfügbarkeit von Daten richtet, als auf korrekte Funktion der Software, und sich nicht auf einen sicheren Zustand des EVG bezieht, bezüglich der Bedrohungen, denen der EVG begegnet. Da sich die abhängige Komponente FPT_FLS.1 lediglich auf einen solchen sicheren Status des EVG (z.B. der Software) bezieht, ist sie für den EVG nicht anwendbar.

7 EVG-Übersichtsspezifikation

7.1 EVG-Sicherheitsfunktionen

Die EVG-Übersichtsspezifikationen beschreiben die Sicherheitsmechanismen, die die Sicherheitsanforderungen aus Kapitel 6 erfüllen und abdecken.

TSF_IDCHK Funktion, die aufgrund von übergebenen Identifikationsdaten (AT1) aus dem Transponder (ID-Tag) mit anhängendem CRC-Wert den CRC-Wert berechnet und das Ergebnis (gültig/ungültig) übergibt. Bei diesem Ergebnis handelt es sich um eine Information, ob der aus dem Transponder eingelesene CRC-Wert mit dem aktuellen, durch den EVG (Fahrzeugrechner) berechneten CRC-Wert übereinstimmt.

TSF_GFE-KEN Funktion, die in einen Leerungsdatensatz (AT) die Kennung des angeschlossenen Fahrzeugrechners (GFE) schreibt.

TSF_AT+CRC Funktion, die über einen gültigen Leerungsdatensatz (AT) und Leerungsdatenblock (AT+) den CRC-Wert berechnet und diesen durch Anhängen an den Leerungsdatensatz bzw. Leerungsdatenblock zur Verfügung stellt.

TSF_SAFE Funktion, die die Leerungsdatensätze (AT) im primären und sekundären Speicher ablegt und wieder ausliest. Leerungsdatensätze (AT) werden im Sekundärspeicher redundant gehalten, damit bei Verlust von Daten im Primärspeicher die Leerungsdatensätze (AT) vollständig wiederhergestellt werden können.

TSF_GFE-CHK Funktion, die die Gültigkeit der vom Fahrzeugrechner an das Sicherheitsmodul übergebenen Leerungsdatensätze (AT) überprüft. Die Funktion überprüft AT2 auf eine gültige Fahrzeugkennung und verwendet die Sicherheitsfunktion TSF_AT+CHK um die Integritätsprüfung durchzuführen. Gegenüber TSF_AT+CHK erlaubt es die Funktion einem autorisierten Benutzer (S.Trusted) die durchgeführten Gültigkeitsnachweise zu verifizieren, und weist durch Warnmeldungen auf Fehler hin.

TSF_AT+CHK Funktion, die aufgrund der vom Fahrzeugrechner an das Sicherheitsmodul übergebenen Leerungsdatensätze (AT) und Leerungsdatenblöcke (AT+) mit jeweils beigefügtem CRC-Wert den CRC-Wert berechnet und das Ergebnis (gültig/ungültig) im Falle des AT CRC anzeigt und im Falle eines ungültigen AT+ CRC eine erneute AT+ Übertragung anstößt. Bei diesem Ergebnis handelt es sich um eine Information, ob der auf dem Fahrzeugrechner für den Leerungsdatenblock und die darin enthaltenen Leerungsdatensätze AT erzeugte CRC-Wert mit dem aktuellen durch den EVG berechneten CRC-Wert übereinstimmt. Die aus dem Vergleich resultierende Information über Integrität und Vollständigkeit wird vom Sicherheitsmodul für die korrekte Weiterverarbeitung genutzt.

7.2 Maßnahmen zur Vertrauenswürdigkeit

Die Vertrauenswürdigkeitskomponenten mit den Vertrauenswürdigkeitsstufen für die Evaluierungsstufe EAL1+ werden in der folgenden Tabelle dargestellt.

Vertrauenswürdigkeits-Komponente	Maßnahmen
ADV_FSP.1	Im Dokument "Funktionale Spezifikation" werden die relevanten TSF-Schnittstellen und deren Parameter beschrieben. Im „Nachweis der Übereinstimmung" von Sicherheitsvorgaben und Funktionaler Spezifikation wird die Übereinstimmung von SFR und

Vertrauenswürdigkeits-Komponente	Maßnahmen
	TSFI nachgewiesen.
AGD_OPE.1	Im Benutzerhandbuch des EVG sind alle für den sicheren Betrieb notwendigen Informationen dokumentiert.
AGD_PRE.1	Die erforderlichen Prozeduren für die Installation, den Anlauf und den Betrieb des EVG sind im Benutzerhandbuch für den EVG dokumentiert.
ALC_CMC.1 ALC_CMS.1	Die Firmware- und Software-Komponente des EVG ist mit einem eindeutigen Verweisnamen und einer Versionsnummer gekennzeichnet. Die Angaben befinden sich auch im Benutzerhandbuch für den EVG.
ATE_IND.1	Der Entwickler stellt den EVG einschließlich spezieller Testgeräte bereit. Die Prüfstelle prüft den EVG bei technischer Unterstützung des Entwicklers.
AVA_VAN.1	Die Prüfstelle führt eine unabhängige Schwachstellenanalyse durch.
ASE_*	Die Prüfstelle führt eine Evaluierung der vom Entwickler bereitgestellten Sicherheitsvorgaben nach EAL1 ergänzt um ASE_SPD.1, ASE_REQ.2 und ASE_OBJ.2 durch.

Tabelle 7 - Maßnahmen zur Vertrauenswürdigkeit

Die einzelnen Vertrauenswürdigkeitsmaßnahmen[7] werden wie folgt erfüllt:

ADV_FSP.1 Basic functional specification fordert eine *"[…] characterisation of all TSFIs and a high level description of SFR-enforcing and SFR-supporting TSFIs. To provide some assurance that the "important" aspects of the TSF have been correctly characterised at the TSFIs, the developer is required to provide the purpose and method of use, parameters for the SFR-enforcing and SFR-supporting TSFIs."*

Diese Forderung wird erfüllt, dadurch dass die relevanten TSF-Schnittstellen und deren Parameter in dem separaten Dokument "Funktionale Spezifikation" beschrieben werden.

Darüber hinaus wird eine *"[…] correspondence between the SFRs and the functional specification; that is, an indication of which interfaces are used to invoke each of the claimed SFRs."* vom Hersteller gefordert.

Diese Forderung wird dadurch erfüllt, dass im separaten Dokument „Nachweis der Übereinstimmung" die entsprechenden Übereinstimmungen zwischen Sicherheitsvorgaben und Funktionaler Spezifikation nachgewiesen werden.

AGD_OPE.1 Operational user guidance fordert ein Handbuch mit folgenden Beschreibungen:

> *"[…] for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.";*
>
> *"[…] for each user role, how to use the available interfaces provided by the TOE in a secure manner.";*
>
> *"[…] for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.";*
>
> *"[…] for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.";*
>
> *"[…] all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation."*

[7] Aufgrund einer derzeit noch ausstehenden, verbindlichen Übersetzung des Teils 3 der CC wurde hier der englischsprachige Text des Teils 3 zitiert.

Diese Forderung wird erfüllt, dadurch dass im Benutzerhandbuch des EVG alle für den sicheren Betrieb notwendigen Informationen dokumentiert sind.

AGD_PRE.1 Preparative procedures fordert eine Dokumentation aller *"[…] steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST."* sowie aller *"[…] steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST."*

Diese Forderung wird erfüllt, dadurch dass die erforderlichen Prozeduren für die Installation, den Anlauf und den Betrieb des EVG im Benutzerhandbuch für den EVG dokumentiert sind.

ALC_CMC.1 Labelling of the TOE fordert einen eindeutigen Verweisnamen, um sicherzustellen, dass Mehrdeutigkeit darüber ausgeschlossen ist, welche Version des TOE (EVG) geprüft und bewertet wird. Die Kennzeichnung des TOE (EVG) mit seinem Verweisnamen stellt sicher, dass die EVG-Benutzer wissen, welche Fassung des TOE (EVG) sie benutzen.

ALC_CMS.1 TOE CM coverage fordert zusätzlich, dass *"Placing the TOE itself and the evaluation evidence required by the other SARs in the ST under CM provides assurance that they have been modified in a controlled manner with proper authorisations."*

Diese Forderungen werden dadurch erfüllt, dass die Firmware- und Software-Komponenten des EVG mit einem eindeutigen Verweisnamen und einer Versionsnummer gekennzeichnet werden, die sich auch im Handbuch wieder finden.

ATE_IND.1 Unabhängiges Testen – Übereinstimmung fordert, dass die Sicherheitsfunktionen entsprechend ihrer Spezifikation wirken. Dazu muss ein TOE (EVG) zum Test bereitgestellt werden, der sich dazu eignet. Diese Forderung wird erfüllt, dadurch dass der Entwickler den EVG einschließlich spezieller Testgeräte der Prüfstelle bereitstellt. Der Entwickler hält sich zur technischen Unterstützung bereit.

AVA_VAN.1 Vulnerability survey fordert, dass die Prüfstelle eine Untersuchung von Schwachstellen basierend auf *„information available in the public domain […] to ascertain potential vulnerabilities that may be easily found by an attacker.*" durchführt. Außerdem wird gefordert, dass von der Prüfstelle "*penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE […] assuming an attack potential of Basic.*" durchgeführt wird.

Diese Forderung wird durch die Tätigkeiten der Prüfstelle im Rahmen der Evaluierung erfüllt.

ASE_*. Security Target evaluation fordert die Prüfung aller in den CC aufgeführten Aspekte der vom Hersteller bereitgestellten Sicherheitsvorgaben durch die Prüfstelle.

Diese Forderung wird durch die Tätigkeiten der Prüfstelle im Rahmen der Evaluierung erfüllt.

Die Maßnahmen in der Tabelle 7 sind ausreichend, weil sie den Anforderungen an die Vertrauenswürdigkeit aus den CC [2] für EAL1 erweitert um die Vertrauenswürdigkeitskomponenten ASE_SPD.1, ASE_OBJ.2 und ASE_REQ.2 entsprechen.

7.3 Erklärung der EVG-Übersichtsspezifikation

Die Erklärung soll zeigen, dass die aus den Sicherheitszielen (Abschnitt 5) abgeleiteten Sicherheitsanforderungen (Abschnitt 6) durch entsprechende Sicherheitsfunktionen (Abschnitt 7) erfüllt werden.

7.3.1 Zusammenwirken der IT-Sicherheitsfunktionen

Funktionale Sicherheitsanforderungen an den EVG Sicherheitsfunktionen	TSF_IDCHK	TSF_GFE_KEN	TSF_AT+CRC	TSF_SAFE	TSF_GFE-CHK	TSF_AT+CHK
FDP_DAU.1		X			X	
FDP_ITT.5	X		X			X
FDP_SDI.1	X					X
FRU_FLT.1				X		

Tabelle 8 - Gegenüberstellung: Funktionale Sicherheitsanforderungen - Sicherheitsfunktionen

FDP_DAU.1 wird durch die Funktion TSF_GFE-KEN erfüllt, weil durch das sofortige Auslesen der Kennung aus dem Fahrzeugrechner (GFE) und das sofortige Einfügen in einen neu angelegten Leerungsdatensatz AT die notwendige Voraussetzung geschaffen wird, dass der Benutzer die Fähigkeit zur Verifizierung des Gültigkeitsnachweises erhält. FDP_DAU.1 wird durch die Funktion TSF_GFE-CHK erfüllt, weil durch die Prüfung der Kennung für den Fahrzeugrechner (GFE) der Benutzer die Fähigkeit zur Verifizierung des Gültigkeitsnachweises erhält.

FDP_ITT.5 bezüglich des Datentransfers zwischen Fahrzeugrechner und Sicherheitsmodul wird durch die Funktion TSF_AT+CRC und TSF_AT+CHK erfüllt: Durch die Erzeugung des CRC-Wertes im Fahrzeugrechner als Integritätsmerkmal für einen Leerungsdatenblock AT+, und dessen Überprüfung im Sicherheitsmodul, wird der Schutz der Benutzerdaten (AT+) vor Modifikation durch Benutzer durchgesetzt, wenn diese zwischen materiell getrennten Teilen des EVG übertragen werden. Bezüglich des Datentransfers zwischen Transponder und Fahrzeugrechner wird FDP_ITT.5 durch TSF_IDCHK erfüllt. Durch die CRC-Prüfung der ID-Tags sind die Identifikationsdaten (AT1) vor Modifikation geschützt und können ihre Integrität bewahren.

FDP_SDI.1 wird durch die Funktion TSF_IDCHK erfüllt, weil durch die Prüfung des CRC-Wertes der Identifikationsdaten (AT1) die notwendige Voraussetzung geschaffen wird, dass der Benutzer die Fähigkeit zur Feststellung der zufälligen Manipulation der Identifikationsdaten AT1 innerhalb der Identifikationseinheit erhält. **FDP_SDI.1** wird durch die Funktion TSF_AT+CHK erfüllt, weil durch die Prüfung des CRC-Wertes der Leerungsdatenblöcke AT+ und der Leerungsdatensätze AT die notwendige Voraussetzung geschaffen wird, dass der Benutzer die Fähigkeit zur Feststellung der zufälligen Manipulation bei Aufzeichnung von Leerungsdatensätzen AT während des Speicherns innerhalb des Fahrzeuges erhält.

FRU_FLT.1 wird durch die Funktion TSF_SAFE erfüllt, weil durch das Ablegen der Leerungsdatensätze im Primär- und Sekundärspeicher die notwendige Voraussetzung geschaffen wird, dass bei einem Verlust von Benutzerdaten im Primärspeicher der Fahrzeugsoftware durch den Transfer von Leerungsdatensätzen von der Fahrzeugsoftware zum Sicherheitsmodul mit Hilfe der im sekundären Speicher gespeicherten Daten der Betrieb sichergestellt wird.

Die Funktionen TSF_IDCHK, TSF_GFE-KEN, TSF_AT+CRC, TSF_SAFE, TSF_GFE-CHK und TSF_AT+CHK arbeiten in der für den EVG intendierten Weise zusammen, weil

- neu gebildete Leerungsdatensätze AT durch die Funktion TSF_GFE-KEN (Auslesen der GFE Seriennummer und Abspeichern in AT) sofort einen eindeutigen Gültigkeitsnachweis erhalten,
- die Identifikationsdaten AT1 durch TSF_IDCHK als integer erkannt werden,
- die Identifikationsdaten AT1 sofort zusammen mit dem Zuordnungsteil AT2, sowie weiteren optionalen Daten in einem Leerungsdatensatz AT zusammengefasst werden,

- anschließend die Leerungsdatensätze AT sofort mittels der Funktion TSF_AT+CRC durch einen CRC-Wert gesichert werden
- diese Leerungsdatensätze AT durch die Funktion TSF_SAFE sowohl im Primär-, als auch im Sekundärspeicher der Fahrzeugsoftware abgelegt werden,
- im Sicherheitsmodul der Bürosoftware entsprechend TSF_AT+CHK der CRC-Wert der Leerungsdatensätze (AT) und Leerungsdatenblöcke (AT+) geprüft wird
- durch die Funktion TSF_GFE-CHK im Sicherheitsmodul der Bürosoftware die Gültigkeit der Leerungsdatenblöcke AT+ durch Prüfung des Gültigkeitsmerkmals jedes einzelnen im Leerungsdatenblock enthaltenen Leerungsdatensatzes AT festgestellt wird.

Somit sind die Sicherheitsanforderungen an den EVG durch das Zusammenwirken der Funktionen TSF_IDCHK, TSF_GFE-KEN, TSF_AT+CRC, TSF_SAFE, TSF_GFE-CHK und TSF_AT+CHK erfüllt.

8 Anhang

8.1 Literaturangaben

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, Part 2: Security functional components, CCMB-2007-09-002, September 2007

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, Part 3: Security assurance components, CCMB-2007-09-003, September 2007

[3] Schutzprofil (PP) Protection Profile Waste Bin Identification Systems WBIS-PP, Version1.04 nach Common Criteria, Vers. 2.1

8.2 Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
GFE	Gassner Fahrzeug Einheit
CC	Common Criteria (Gemeinsame Kriterien)
CRC	Cyclic Redundancy Check
EAL	Evaluation Assurance Level (Vertrauenswürdigkeitsstufe)
EVG	Evaluierungsgegenstand
FSP	Funktionale Spezifikation
IT	Informations-Technologie
OSP	Organisatorische Sicherheitspolitiken
OTP	One Time Programmable
PP	Protection Profile (Schutzprofil)
SFP	Security Function Policy (funktionale Sicherheitspolitik)
TOE	Target of Evaluation (Evaluationsgegenstand)
TSC	TSF Scope of Control (Anwendungsbereich der TSF-Kontrolle)
TSF	TOE Security Functions (EVG-Sicherheitsfunktionen)
WBIS	Waste Bin Identification Systems (Abfallbehälter-Identifikations-System)

8.3 Mnemocodes der EVG-Übersichtsspezifikation

AT+	Leerungsdatenblock
CHK	Check des CRC-Wertes bzw. der Kennung
CRC	Create des CRC-Wertes
ID	Tag-ID
KEN	Kennung
SAFE	Speichern der Daten

8.4 Glossar

AT Ein Leerungsdatensatz AT zu einer Leerung ist ein schutzwürdiges Objekt in einem WBIS. Ein Leerungsdatensatz AT besteht aus den Datenfeldern AT1 und AT2

AT1 Identifikationsdaten des Abfallbehälters

AT2 Zuordnungsdaten: GFE-Kennung, Zeitstempel (Datum und Uhrzeit) des Leerungsvorgangs.

AT+ Der Leerungsdatenblock AT+ wird bei der Kommunikation zwischen Fahrzeugsoftware und dem Sicherheitsmodul gebildet. Der Leerungsdatenblock AT+ ist ein schutzwürdiges Objekt in einem WBIS bei der Kommunikation zwischen der Fahrzeugsoftware und dem Sicherheitsmodul.

CRC Ein Zahlenwert, der über einen definierten Bereich von Daten unter Verwendung einer zyklischen Rechenvorschrift erstellt wird. Dieser Wert dient zur Kontrolle der Integrität der Daten.

Header Kopfzeilen einer Datenstruktur, die Informationen über die nachfolgende Datenstruktur geben.

Transponder Einheit, welche ihre gespeicherten Informationen übermittelt, wenn sie durch einen Transceiver aktiviert ist.

Lesetransponder können ausschließlich gelesen werden. OTP (One Time Programmable) Transponder können einmal beschrieben werden und verhalten sich wie Lesetransponder. Read/Write Transponder können mehrfach oder mindestens einmal beschrieben und gelesen werden.