Erste Evaluierung

Gefäßidentifikationssystem BiTech (WBIS)

Sicherheitsvorgaben (ST)

BSI-DSZ-CC-0282

Version 2.15
27.06.06

Evaluierungsgrundlage:

Common Criteria, Vers. 2.1

Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik

Vertrauenswürdigkeitsstufe: EAL 1

Hersteller/Antragsteller:

deister electronic GmbH

Hermann-Bahlsen-Str. 11-13, 30890 Barsinghausen

INHALTSVERZEICHNIS

Tabellenverzeichnis

Abbildungsverzeichnis

1 Dokument-Organisation

Diese Sicherheitsvorgaben sind Vorgaben für den Evaluationsgegenstand (EVG) „Gefäßidentifikationssystem BiTech“, im Evaluierungsverfahren nach Common Criteria (Version 2.1) für die Vertrauenswürdigkeitsstufe EAL1.

Aus Gründen der Übersicht sind aus dem Schutzprofil „Protection Profile Waste Bin Identification Systems WBIS-PP, Version 1.04“ [3] entnommene Teile durch schwarze Schrift gekennzeichnet, für die Sicherheitsvorgaben neu entstandene Passagen wurden in grauer Schrift gehalten.

Das Dokument ist wie folgt unterteilt:

Abschnitt 2 enthält einführendes Material für die Sicherheitsvorgaben.

Abschnitt 3 beschreibt den typischen Einsatzbereich und die Definition des EVG.

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.

Abschnitt 8 PP-Postulate bestätigt eine Übereinstimmung mit dem zugrunde liegenden Schutzprofil.

Abschnitt 9 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 anschließende 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. Der nächste Abschnitt von 9 enthält einige Argumente für die Adress-Abhängigkeitsanalyse und die interne Folgerichtigkeit und gegenseitige Unterstützung der Anforderungen. Dem folgen die Erklärung zu der EVG-Übersichtsspezifikation und Angaben zur Vertrauenswürdigkeit mit anschließender Erklärung zu den PP-Postulaten.

In Abschnitt 10 wird ein Verzeichnis mit Literaturangaben bereitgestellt. Listen mit Abkürzungen, Mnemocodes und ein Glossar dienen zur Definition von wiederholt gebrauchten Kurzbezeichnungen.

2 ST-Einführung

Dieses Kapitel enthält eine Beschreibung des EVG sowie den Anwendungsbereich und die Grenzen.

Die ST-Einführung ist in folgende Abschnitte unterteilt:

2.1 ST-Identifikation

Sicherheitsvorgaben (ST) zum EVG Gefäßidentifikationssystem BiTech (WBIS)
Zertifizierungs-Nr.: BSI-DSZ-CC-0282
Version 2.15 vom 27.06.2006
Autoren: Stefan Eichler,
Britta Busche

2.2 ST-Übersicht

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.

Gefäßidentifikationssystem BiTech:

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

Bei der BSU handelt es sich um eine von deister electronic entwickelte Mikroprozessor gesteuerte Hardware. Die BSU verfügt über weitere Schnittstellen zu anderen Komponenten des Abfallsammelfahrzeuges, wie einem Wiegesystem, die jedoch nicht Teil des EVG sind. Die Firmware auf dieser BSU bildet aus den Identifikationsdaten (AT1) zusammen mit dem Zeitstempel (AT2) und optionalen Daten einen Leerungsdatensatz (AT).

Leerungsdatensätze AT werden zu Leerungsdatenblöcken AT+ zusammengefasst. Ein Leerungsdatenblock besteht aus einem Header und bis zu 10 Leerungsdatensätzen. Zur Authentisierung der Leerungsdatenblöcke wird im Header jedes neu angelegten Leerungsdatenblockes (AT+) die Kennung der im Fahrzeug befindlichen BSU gespeichert. Die Generierung und Verwendung dieser Kennung wird im Rahmen der Funktionalen Spezifikation (FSP) näher beschrieben.

Nach Bildung eines neuen Leerungsdatensatzes (AT) wird sofort die Anzahl der nun gültigen ATs im Header erhöht und der Leerungsdatensatz in den Leerungsdatenblock AT+ eingefügt. Zur Sicherung der Datenintegrität wird ein neu ermittelter CRC-Wert dem Leerungsdatenblock angehängt.
Sind in einem Leerungsdatenblock AT+ 10 Leerungsdatensätze (AT) vorhanden, so ist dieser Datenblock abgeschlossen und es wird ein neuer Leerungsdatenblock generiert.

Die Leerungsdatenblöcke werden im Fahrzeugrechner in unterschiedlichen Speichern abgelegt (Primär- und Sekundärspeicher). Die optionalen Daten sind von der Applikation, also von den über Schnittstellen mit der BSU 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 über Primär- oder Sekundärspeicher bis in eine Bürosoftware übertragen. Die ins Büro übermittelten Leerungsdatensätze (AT) und Leerungsdatenblöcke (AT+) werden hier wiederum mit Hilfe des Sicherheitsmoduls auf Datenintegrität und Gültigkeit (Authentisierung) überprüft.

Bei BiTech kann der Datentransfer in die Bürosoftware mit unterschiedlichen Datenträgern bzw. Datentransfermethoden erfolgen. So z. B. ein dienstleistungsnaher (wie täglicher) Datentransfer zum jeweiligen privatwirtschaftlichen oder kommunalen Entsorgungsunternehmen. 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 BiTech 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 BiTech der EVG bis in die entsorgungspflichtige Körperschaft! Dies geschieht durch den Datentransfer mit einem in der BSU vorhandenen und entnehmbaren Langzeitdatenspeicher. Dieser Langzeitdatenspeicher kann direkt in der entsorgungspflichtigen Körperschaft ausgelesen werden und darüber hinaus – je nach Wunsch – auch dort archiviert werden.

Es kommen Transponder zum Einsatz, die sowohl nur lesbar (Read Only und OTP) als auch les- und beschreibbar (Read/Write) sind. Die Speicherung auf dem Abfallsammelfahrzeug erfolgt auf

mindestens zwei Speichermedien, deren Dateninhalte in der Rechentechnik im Büro ausgelesen werden können. Bei den Speichermedien kann es sich um gleiche oder verschiedene Medien handeln, z.B. PCMCIA-Card, Speichermodul, ...

Der EVG kommt im Beispiel des Gefäßidentifikationssystems überall dort zum Einsatz, wo die Datenintegrität und Gültigkeit bei der Übertragung von Daten zwischen den Komponenten sichergestellt werden muss. Das heißt:

- Alle Identifikationsdaten des Abfallbehälters (AT1) werden auf Integrität geprüft.
- Die bestehenden Leerungsdatensätze (AT) werden zu Leerungsdatenblöcken (AT+) zusammengefasst, wobei diese durch einen CRC mit nicht öffentlichem Polynom und Startwert gesichert werden.
- Die Gültigkeit der Leerungsdatenblöcke (AT+) wird durch die eindeutige Kennung und Identifizierung des Fahrzeugrechners (BSU) sichergestellt.
- Die Leerungsdatenblöcke werden jeweils auf einem Primär- und Sekundärspeicher gespeichert.
- Bei der Übergabe an die Bürosoftware wird mit Hilfe des Sicherheitsmoduls die Datenintegrität der Leerungsdatenblöcke (AT+) und Leerungsdatensätze (AT) überprüft.

BiTech kann neben der Identifikation von Abfallgefäßen auch bei anderen Behältern angewendet werden.

Lieferumfang des Gefäßidentifikationssystem BiTech:

Name	Versionsnummer	Lieferumfang	Bestandteil des EVG
Transponder (ID-Tag)	Siehe Anlage Identifikation der Transponder (ACM) [5]		x
Firmware in der BSU	Version 2.57[1] Version 1.5 Version 27/06/06	- BSU mit Firmware BSU_CAN_8V2_57.HE_ (nicht Bestandteil des EVG) Beinhaltet: DE_BSI_M16_LIB.A - Gefäßidentifikationssystem Installations- und Benutzer-handbuch [6]	x
Bürosoftware mit Sicherheitsmodul	Version 1.5, Version 2.0.1 (s. Fußnote 1) Version 27/06/06	- DE_BSI_PC_DLL. Dateien: DE_BSI_PC_DLL.DLL und DE_BSI_PC_DLL.H - Bürosoftware BiDIP - BiDIP2 Installations- und Benutzerhandbuch [7]	x
	Version 20/09/05	- Handheld BHT, BHT lite, BHI, BHI Pro Manual [8]	

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

[1] **zum Zeitpunkt der Zertifizierung**

2.3 Postulat der Übereinstimmung mit den CC

Die Evaluierung des EVG erfolgt auf Basis der Common Criteria (CC)
- Teil 1, Version 2.1, August 1999
- Teil 2, Version 2.1, August 1999
- Teil 3, Version 2.1, August 1999:

Übereinstimmung des EVG mit den CC:
Teil 2 der CC 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.
Der EVG ist konform zu Teil 3 der CC.
Der EVG ist konform zum Schutzprofil „Protection Profile Waste Bin Identification Systems WBIS-PP, Version 1.04“ (siehe Kapitel 8).

Die angestrebte Vertrauenswürdigkeitsstufe ist EAL 1.

3 EVG-Beschreibung

Die EVG-Beschreibung ist in folgende Abschnitte unterteilt:

3.1 Beschreibung des Gesamtsystems

Das Abfallbehälter-Identifikations-System (WBIS) 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.
- Bürorechner im Büro. Das Sicherheitsmodul und die Bürosoftware sind installiert auf dem Bürorechner.

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

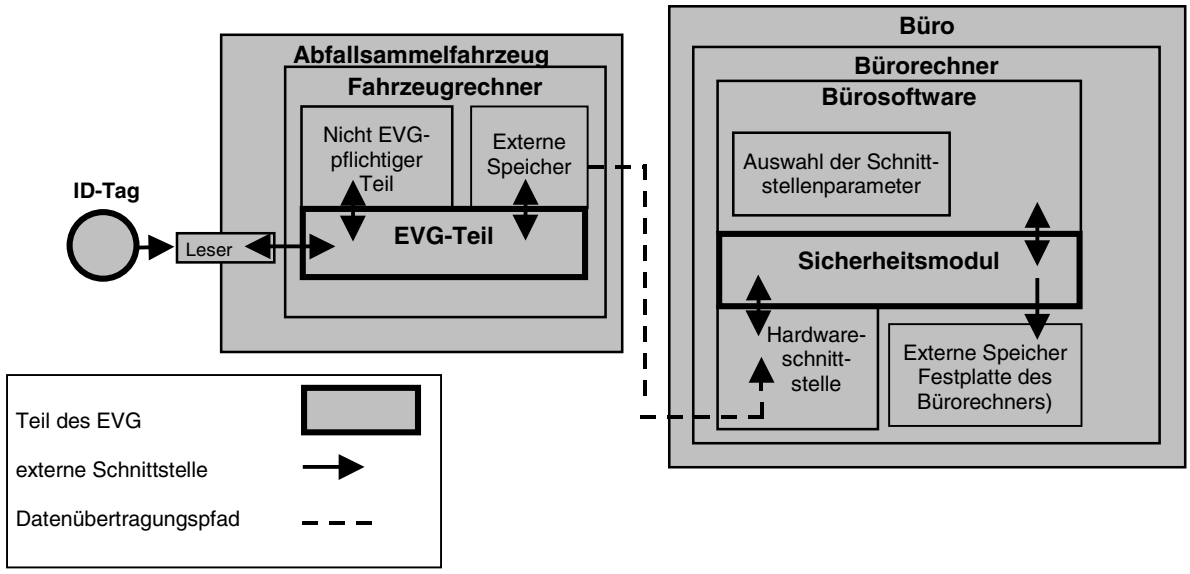

Abbildung 1: Abfallbehälter-Identifikations-System

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 und anschließend an die Fahrzeugsoftware weitergeleitet. Die dabei möglichen Übertragungsfehler und eventuelle Manipulationen werden von der Fahrzeugsoftware erkannt. 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. Zur Authentifizierung des Leerungsdatenblockes wird sofort bei dessen Erstellung die Kennung der im Fahrzeug befindlichen BSU eingefügt.

Die Leerungsdatenblöcke werden 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 autorisierten Fahrzeug erstellten Leerungsdatenblöcke als gültig erkannt werden. Zusätzlich werden die bei einer Übertragung möglichen Fehler erkannt.

Die Leerungsdatenblöcke 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, oder die Leerungsdatenblöcke selbst 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 Leerungsdatenblöcke 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.

3.2 Definition des EVG

Der EVG setzt sich aus folgenden Komponenten zusammen:

Transponder (ID-Tag):	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 sowohl nur lesbar (Read Only und OTP) als auch les- und beschreibbar (Read/Write), wobei die unique ID unveränderbar ist. Der beschreibbare Teil des Transponders ist nicht Teil des EVG. Weitere Angaben zu den Transpondern erfolgen im Rahmen der Funktionalen Spezifikation (FSP).
EVG-Teil der Fahrzeugsoftware:	Bei dem EVG der Fahrzeugsoftware handelt es sich namentlich um DE_BSI_M16_LIB, Version 1.5, Dateien: DE_BSI_M16_LIB.A und DE_BSI_M16_LIB.H, Handbuch: Gefäßidentifikationssystem Installations- und Benutzerhandbuch. Anmerkung: Diese Library wird zusammen mit der BSU Firmware DE_BSU auf einem von der Firma deister electronic entwickelten Fahrzeugrechner (BSU) betrieben, basierend auf einem Mikroprozessor der MC16 Familie von Mitsubishi.

Sicherheitsmodul: Bei dem Sicherheitsmodul handelt sich um den EVG-Teil der Bürosoftware
DE_BSI_PC_DLL, Version 1.5,
Dateien: DE_BSI_PC_DLL.DLL und DE_BSI_PC_DLL.H,
Handbuch: BiDIP2 Installations- und Benutzerhandbuch.
Anmerkung: Dieses Modul muss in die Bürosoftware eingebunden werden, die nicht Bestandteil des EVG ist.
Die Software mit integriertem EVG läuft auf einem IBM kompatiblen PC mit Betriebssystem ab MS-Windows 95 und Nachfolger.

Sofern eine Änderung des EVG in der Firmware und der Bürosoftware notwendig ist, muss diese Änderung in beide Teile einfließen. Dies wird durch die Änderung der Versionsnummer beider Teile angezeigt.

Der EVG hat folgende Aufgaben:

- Überprüfen der eingelesenen Identifikationsdaten (AT1) mit angehängtem CRC auf Integrität (CRC-Prüfung auf Gültigkeit).
- Generieren des Leerungsdatensatzes AT durch Einfügen der Idenitfikationsdaten AT1 und des Zeitstempels AT2.
- Generieren von Leerungsdatenblöcken AT+ für jeweils maximal zehn einzufügende Leerungsdatensätze (AT).
- Einfügen der BSU-Kennung als Gültigkeitsmerkmal in den Header jedes Leerungsdatenblocks AT+.
- Sofortiges Einfügen des Leerungsdatensatzes AT in den Leerungsdatenblock AT+ und sofortiges Sichern mittels CRC.
- Speichern der Leerungsdatenblöcke AT+ auf externen Speichern (Primär- und Sekundär-speicher).
- Auslesen der Leerungsdatenblöcke AT+ von den externen Speichern in das Sicherheitsmodul des Bürorechners über eine von der Bürosoftware ausgewählte Hardwareschnittstelle. Dazu übergibt die Bürosoftware die Auswahl der Schnittstelle an das Sicherheitsmodul. Der Aufruf der Schnittstelle erfolgt durch das Sicherheitsmodul).
- Im Sicherheitsmodul prüfen der BSU-Kennung auf Gültigkeit der Leerungsdatenblöcken AT+.
- Ebenfalls prüfen des CRC-Wertes auf Integrität der Leerungsdatenblöcken AT+.
- Kennzeichnung der Leerungsdatenblöcken AT+ bezüglich Gültigkeit und Integrität durch das Sicherheitsmodul.

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. 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 EVGs durchlaufen, bevor sie in die externen Speicher 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 Sicherheitsmoduls 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 die Leser vom EVG angesprochen werden und Identifikationsdaten vom Leser zum EVG geschickt werden.
- Eine bidirektionale Schnittstelle zwischen dem EVG-Teil der Fahrzeugsoftware und dem nicht EVG-pflichtigen Teil 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 aus den externen Speichern gelesen werden.
- Eine bidirektionale Schnittstelle zwischen Bürosoftware und Sicherheitsmodul. Sie ist bidirektional, da Parameter wie Hardwareschnittstelle an das Sicherheitsmodul und Fehlermeldungen an die Bürosoftware übergeben 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.

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.

4 EVG-Sicherheitsumgebung

Die EVG-Sicherheitsumgebung ist in folgende Abschnitte unterteilt:

4.1 Annahmen
4.2 Bedrohungen
4.3 Organisatorische Sicherheitspolitiken

Der folgende Abschnitt dient der Definition von Art und Umfang der Sicherheitsbedürfnisse, die der EVG adressiert. Daher enthält dieser Abschnitt 4.1 alle Annahmen an die Umgebung des EVG, 4.2 die zu schützenden Werte, die bekannten Angreifer und die Bedrohungen, die sie für die Werte darstellen sowie 4.3 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 den Datenfeldern:

AT1 Identifikationsdaten des Abfallbehälters

AT2 Zeitstempel (Datum und Uhrzeit) des Leerungsvorgangs.

AT+ Der Leerungsdatenblock AT+ wird jeweils nach Erhalt eines neuen Leerungsdatensatzes AT direkt auf der Fahrzeugsoftware gebildet. Bei der Übertragung der Leerungsdatensätze AT von der Fahrzeugsoftware zum Sicherheitsmodul im Büro sind die Leerungsdatensätze somit bereits zu einem Leerungsdatenblock AT+ zusammengefasst. Der Leerungsdatenblock AT+ ist ein schutzwürdiges Objekt in einem WBIS bei der Kommunikation zwischen der Fahrzeugsoftware und dem Sicherheitsmodul.

Es gibt zwei Arten von Leerungsdatensätzen:
a) abrechnungsrelevante Datensätze,
b) nicht abrechnungsrelevante Datensätze.

Ein abrechnungsrelevanter Datensatz muss zwingend gültige Identifikaitonsdaten AT1 und den Zeitstempel AT2 enthalten. Ein nicht abrechnungsrelevanter Datensatz enthält falsche oder keine Identifikationsdaten[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.

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.**

4.1 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 vertauenswürdig. Alle Personen, die das System installieren, initialisieren[3] 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 Leerungsdatenblöcke (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 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.

A.Installation *Korrekte Inbetriebnahme*

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

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.

[3] **Unter Initilisierung versteht man die Übergabe von Parametrisierungdaten, wie BSU-Kennung, Adressen der Leser, Schüttungsparameter, ...**

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[4]:

- 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 Handys, deren Strahlung einer Sendequelle im gleichen Frequenzbereich des Lesers entspricht,
- weiteren Transponder im Lesefeld, die die Übertragung stören können

(siehe auch Fußnote 4 auf Seite 15).

T.Create *Ungültige Leerungsdatenblöcken*

Ein Angreifer (S.Attack) erzeugt beliebige Leerungsdatenblöcke (AT+) und überträgt diese an das Sicherheitsmodul. Diese Manipulation kann z.B. durch eine elektromagnetische Entladung an einem elektromagnetischen Speicher, wie der PCMCIA-Card oder dem Speichermodul verursacht werden (siehe auch Fußnote 4 auf Seite 15).

T.Jam#2 *Verfälschte Leerungsdatensätze*

Ein Angreifer (S.Attack) verfälscht Leerungsdatensätze (AT) während der Bearbeitung und der Speicherung innerhalb des Fahrzeuges oder stört die Übertragung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul z.B. durch elektromagnetische Strahlung, um die Daten der Leerungsdatenblöcke (AT+) ausschließlich rein zufällig zu verfälschen. Diese elektromagnetische Strahlung resultiert zum Beispiel von elektrischen Geräten, wie Handys, deren Strahlung einer Sendequelle im gleichen Frequenzbereich des Lesers entspricht (siehe auch Fußnote 4 auf Seite 15).

4.3 Organisatorische Sicherheitspolitiken

Die folgende Regel wird für den 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 möglich ist.

[4] **Die Liste der Beispiele garantiert keine Vollständigkeit.**

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.

Die Sicherheitsziele sind in folgende Abschnitte unterteilt:

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 soll 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 soll jeden Versuch einer Übermittlung willkürlicher (z.B. ungültiger) Leerungsdatenblöcke (AT+) an das Sicherheitsmodul erkennen. Der EVG soll 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 soll sicherstellen, dass die Daten der Leerungsdatenblöcke (AT+) durch eine redundante Sicherung in einem sekundären Speicher gesichert werden, auf eine Weise, dass der Transfer der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul möglich ist, sofern Leerungsdatenblöcke (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 sollten 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 *Zugriffsschutz*

Die Umgebung soll durch angemessene Mittel sicherstellen (Verschluss, Passwort zur Zugriffskontrolle 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, soll durch ausreichende Maßnahmen ausgeschlossen werden.

OE.Check *Vollständigkeitsprüfung*

Es soll 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 soll durch eine erneute Datenübermittlung wiederhergestellt werden. Die Intervalle müssen der Kapazität des entsprechenden Speichers vom Fahrzeugrechner angepasst sein.

OE.Backup *Datensicherung*

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

[5] **Dieses Umgebungssicherheitsziel 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.

Die IT-Sicherheitsanforderungen sind in folgende Abschnitte unterteilt:

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.

6.1.2 EVG-interner Transfer (FDP_ITT)

6.1.2.1 Interne 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) **Datenintegritätspolitik** ist für die Anforderung “Interne Transferintegrität (FDP_ITT.5)” formuliert:

Die Benutzerdaten (AT1 und AT+) sollen geschützt werden, um ihre Integrität zu wahren.

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 innerhalb des TSC gespeicherten Benutzerdaten auf *zufällige Manipulation* bei allen Objekten auf Basis folgender Attribute: *Identifikationsdaten AT1 innerhalb der Identifikationseinheit und Aufzeichnungen von Leerungsdatensätzen AT während des Speicherns innerhalb des Fahrzeuges* überwachen.

6.1.4 Fehlertoleranz (FRU_FLT)

6.1.4.1 Verminderte Fehlertoleranz (FRU_FLT.1)

FRU_FLT.1.1 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*.

6.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Die folgende Tabelle enthält die Vertrauenswürdigkeitsklassen mit den Vertrauenswürdigkeitskomponenten für die Evaluierungsstufe EAL 1. Sie entstammen den Common Criteria (CC), Teil 3 [2].

Tabelle 1: Anforderungen der Vertrauenswürdigkeitsstufe EAL 1

Klassen	Vertrauenswürdigkeitskomponenten
ACM	ACM_CAP.1
ADO	ADO_IGS.1
ADV	ADV_FSP.1, ADV_RCR.1
AGD	AGD_ADM.1, AGD_USR.1
ALC	-
ATE	ATE_IND.1
AVA	-

6.3 Sicherheitsanforderungen an die IT-Umgebung

Es bestehen keine Sicherheitsanforderungen an die IT-Umgebung des EVG.

6.4 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 und werksseitig durch einen CRC geschützt. 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 soll jede Art von Beeinflussung der internen Kommunikationswege in den Bürorechnern verhindern.

R.Check *Überprüfung der Vollständigkeit*

Der Benutzer soll in regelmäßigen Abständen die vollständige Übertragung der Leerungsdatenblöcke (AT+) zwischen Fahrzeug und Büro prüfen. Der Benutzer soll 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, Leerungsdatenblöcken (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 Identifikationssystemes auf dem Fahrzeug müssen die BSU-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**

7 EVG-Übersichtsspezifikation

Die EVG-Übersichtsspezifikation ist in folgende Abschnitte unterteilt:

7.1 EVG-Sicherheitsfunktionen
7.2 Maßnahmen zur Vertrauenswürdigkeit

7.1 EVG-Sicherheitsfunktionen

Die EVG-Übersichtsspezifikationen beschreiben die Sicherheitsmechanismen, die die Sicherheitsanforderungen aus Abschnitt 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) an den "nicht EVG-pflichtigen Teil der Fahrzeugsoftware" übergibt. Bei diesem Ergebnis handelt es sich um eine Information, ob der aus dem Transponder eingelesene CRC-Wert mit dem aktuellen durch den EVG berechneten CRC-Wert übereinstimmt.
TSF_BSU-KEN	Funktion, die in einen neu angelegten Leerungsdatenblock (AT+) die Kennung des angeschlossenen Fahrzeugrechners (BSU) schreibt. In jeden neu angelegten Leerungsdatenblock AT+ wird die Kennung der BSU ausgelesen und sofort eingefügt. Bei einem Wechsel der Kennung wird ein ggf. offener Leerungsdatenblock sofort abgeschlossen und ein neuer AT+ mit der nun aktuellen Kennung angelegt.
TSF_AT+CRC	Funktion, die über einen gültigen Leerungsdatenblock (AT+), bestehend aus Leerungsdatensätzen (AT) den CRC-Wert berechnet und diesen CRC-Wert dem Leerungsdatenblock anhängt.
TSF_SAFE	Funktion, die die Leerungsdatenblöcke AT+ im primären und sekundären Speicher ablegt und wieder ausliest.
TSF_BSU-CHK	Funktion, die die Gültigkeit der vom Fahrzeugrechner an das Sicherheitsmodul übergebenen Leerungsdatenblöcke (AT+) überprüft.
TSF_AT+CHK	Funktion, die aufgrund der vom Fahrzeugrechner an das Sicherheitsmodul übergebenen Leerungsdatenblöcken (AT+) mit beigefügtem CRC-Wert den CRC-Wert berechnet und das Ergebnis (gültig/ungültig) anzeigt. 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 EAL 1 werden in der folgenden Tabelle dargestellt.

Tabelle 2: Maßnahmen zur Vertrauenswürdigkeit

Vertrauenswürdigkeits-komponente	Maßnahmen
ACM_CAP.1	Die Firmware- und Software-Komponente des EVG ist mit einem eindeutigen Verweisnamen und einer Versionsnummer gekennzeichnet, siehe Abschnitt 2.1. Die Angaben befinden sich auch im Benutzerhandbuch für den EVG.
ADO_IGS.1	Die erforderlichen Prozeduren für die Installation, den Anlauf und den Betrieb des EVG sind im Benutzerhandbuch für den EVG dokumentiert.
ADV_FSP.1	Im Dokument "Funktionale Spezifikation" werden die sichtbaren TSF-Schnittstellen und das Verhalten der TSF beschrieben.
ADV_RCR.1	Im „Nachweis der Übereinstimmung" von EVG-Übersichtsspezifikation und Funktionaler Spezifikation werden die entsprechenden Übereinstimmungen nachgewiesen.
AGD_ADM.1	Entfällt: Aufgrund der Vorgaben des EVG ist ein Systemverwalterhandbuch nicht notwendig. Dies wird im Benutzerhandbuch begründet.
AGD_USR.1	Im Benutzerhandbuch des EVG sind alle für den sicheren Betrieb notwendigen Informationen dokumentiert.
ATE_IND.1	Der Entwickler stellt den EVG einschließlich spezieller Testgeräte bereit. Die Prüfstelle prüft den EVG bei technischer Unterstützung des Entwicklers.

Die einzelnen Vertrauenswürdigkeitsmaßnahmen werden wie folgt erfüllt:

ACM_CAP.1 Versionsnummern 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.
Diese Forderung wird erfüllt, dadurch dass die Firmware- und Software-Komponenten des EVG mit einem eindeutigen Verweisnamen und einer Versionsnummer gekennzeichnet werden, die sich auch im Handbuch wiederfinden. Sofern eine Änderung des EVG in der Firmware und der Bürosoftware notwendig ist, muss diese Änderung in beide Teile einfließen. Dies wird durch die Änderung der Versionsnummer beider Teile angezeigt.

ADO_IGS.1 Installations-, Generierungs- und Anlaufprozeduren fordert für die sichere Installation und Generierung sowie den sicheren Anlauf des TOE (EVG), dass die erforderlichen Prozeduren dokumentiert werden. Die Dokumentation muss die für die sichere Installation und Generierung sowie den sicheren Anlauf des TOE (EVG) erforderlichen Schritte beschreiben.
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.

ADV_FSP.1 Informelle funktionale Spezifikation fordert eine informelle Beschreibung der für den Benutzer sichtbaren externen TSF-Schnittstelle und des TSF-Verhaltens auf hoher Ebene in Form einer funktionalen Spezifikation. Sie muss den Zweck und die Methode des Gebrauchs aller externen TSF-Schnittstellen beschreiben, einschließlich Details der Wirkungen, Ausnahmen und Fehlermeldungen, wie jeweils angemessen. Die funktionale Spezifikation muss zeigen, dass alle EVG-Sicherheitsanforderungen angesprochen sind.
Diese Forderung wird erfüllt, dadurch dass die sichtbaren TSF-Schnittstellen und das Verhalten der TSF in dem separaten Dokument "Funktionale Spezifikation" beschrieben werden.

ADV_RCR.1 Informeller Nachweis der Übereinstimmung fordert eine Analyse der Übereinstimmung aller benachbarten Paare der bereitgestellten TSF-Darstellungen (EVG-Übersichtsspezifikation,

funktionale Spezifikation, …). Die Analyse muss für jedes Paar benachbarter TSF-Darstellungen nachweisen, dass die gesamte relevante Sicherheitsfunktionalität der abstrakteren TSF-Darstellung in der weniger abstrakten TSF-Darstellung korrekt und vollständig verfeinert wurde.
Diese Forderung wird erfüllt, dadurch dass im separaten Dokument „Nachweis der Übereinstimmung" die entsprechenden Übereinstimmungen von EVG-Übersichtsspezifikation und Funktionaler Spezifikation nachgewiesen werden.

AGD_ADM.1 Systemverwalterhandbuch fordert ein Systemverwalterhandbuch, das sich an das zuständige Personal für die Systemverwaltung richtet.
Entfällt: Aufgrund der Vorgaben des EVG ist ein Systemverwalterhandbuch nicht notwendig. Dies wird im Benutzerhandbuch begründet.

AGD_USR.1 Benutzerhandbuch fordert ein Handbuch, das sich an Benutzer des TOE (EVG) richtet, die nicht für die Systemverwaltung zuständig sind. Das Benutzerhandbuch muss den Gebrauch der vom TOE (EVG) bereitgestellten Sicherheitsfunktionen sowie die Funktionen und Schnittstellen, die für den Benutzer zugänglich sind, beschreiben. Es muss alle Verantwortlichkeiten des Benutzers klar darstellen, die mit den in der Darlegung der EVG-Sicherheitsumgebung enthaltenen Annahmen zum Benutzerverhalten zusammenhängen, sowie Warnungen, die in einer sicheren Verarbeitungsumgebung kontrolliert werden sollen. Auch müssen alle Sicherheitsanforderungen an die IT-Umgebung beschreiben, die für den Benutzer relevant sind.
Diese Forderung wird erfüllt, dadurch dass im Benutzerhandbuch des EVG alle für den sicheren Betrieb notwendigen Informationen dokumentiert sind.

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.

Die Maßnahmen in der Tabelle 2 sind ausreichend, weil sie den Anforderungen an die Vertrauenswürdigkeit aus den CC [2] für EAL 1 entsprechen.

8 PP-Postulate

Der EVG entspricht dem Schutzprofil „Protection Profile Waste Bin Identification Systems WBIS-PP, Version 1.04“.

Zusätzlich zu den in den PP [3] beschriebenen IT-Sicherheitsanforderungen sind folgende Annahmen, Ziele und Anforderungen in diesen ST hinzugekommen:

Annahmen	A.Installation: Korrekte Inbetriebnahme	siehe Kapitel 4.1
Umgebungssicherheitsziele	OE.Installation: Korrekte Inbetriebnahme	siehe Kapitel 5.2
Sicherheitsanforderungen an die Nicht-IT-Umgebung	R.Installation: Korrekte Inbetriebnahme	siehe Kapitel 6.4

9 Erklärungen

Die Erklärungen sind in folgende Abschnitte unterteilt:

9.1 Einleitung

Die Tabellen in den Unter-Abschnitten 9.2.1 Abdeckung der Sicherheitsziele und 9.3.1 Abdeckung der Sicherheitsanforderungen bilden die Sicherheitsziele und Sicherheitsanforderungen an den EGV ab.

9.2 Erklärung zu den Sicherheitszielen

9.2.1 Abdeckung der Sicherheitsziele

Tabelle 3: Darstellung 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						

9.2.2 Hinlänglichkeit der Sicherheitsziele

9.2.2.1 Hinlänglichkeit der Politiken und Sicherheitsziele

P.Safe (Fehlertoleranz) setzt die Verfügbarkeit von den wichtigen Daten für die Übertragung der Leerungsdatenblöcke (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.

9.2.2.2 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.

9.2.2.3 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 BSU-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.

9.3 Erklärung zu den Sicherheitsanforderungen

9.3.1 Abdeckung der Sicherheitsanforderungen

Tabelle 4: Gegenüberstellung: Funktionale Sicherheitsanforderungen ←→ Sicherheitsziele

Funktionale Sicherheitsanforderungen an den EVG / EVG 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 5: Gegenüberstellung: Sicherheitsanforderungen ←→ Umgebungssicherheitsziele

Sicherheitsanforderungen an die Umgebung / EVG Sicherheitsziele	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

9.3.2 Hinlänglichkeit der Sicherheitsanforderungen

9.3.2.1 Hinlänglichkeit der EVG Sicherheitsanforderungen und gegenseitige Unterstützung

OT.Inv#1 (Erkennen ungültiger Identifikationsdaten) zielt auf das Erkennen von manipulierten Identifikationsdaten (AT1) aus empfangenen Leerungsdatensätzen (AT) innerhalb der Identifikationseinheit und während des Transfers zwischen der Identifikationseinheit und der Fahrzeugsoftware, die separate Teile des EVG darstellen. 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.

9.3.2.2 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.

9.4 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.

9.5 Erklärung zu den Abhängigkeiten

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

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.

Tabelle 6: Abhängigkeiten der funktionalen Anforderungen

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

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.

9.6 Erklärung zu 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.

9.6.1 Zusammenwirken der IT-Sicherheitsfunktionen

Tabelle 7: Gegenüberstellung: Funktionale Sicherheitsanforderungen ←→ Sicherheitsfunktionen

Funktionale Sicherheitsanforderungen an den EVG / Sicherheitsfunktionen	TSF_IDCHK	TSF_BSU-KEN	TSF_AT+CRC	TSF_SAFE	TSF_BSU-CHK	TSF_AT+CHK
FDP_DAU.1		x			x	
FDP_ITT.5			x			
FDP_SDI.1	x					x
FRU_FLT.1				x		

FDP_DAU.1 wird durch die Funktion TSF_BSU-KEN erfüllt, weil durch das sofortige Auslesen der Kennung aus dem Fahrzeugrechner (BSU) und das sofortige Einfügen in einen neu angelegten Leerungsdatenblock AT+ die notwendige Voraussetzung geschaffen wird, dass der Benutzer die Fähigkeit zur Verifizierung des Gültigkeitsnachweises erhält. Bei einem Wechsel der Kennung wird ein ggf. offener Leerungsdatenblock sofort abgeschlossen und ein neuer AT+ mit der nun aktuellen Kennung angelegt. **FDP_DAU.1** wird durch die Funktion TSF_BSU-CHK erfüllt, weil durch die Prüfung der Kennung für den Fahrzeugrechner (BSU) der Benutzer die Fähigkeit zur Verifizierung des Gültigkeitsnachweises erhält.

FDP_ITT.5 wird durch die Funktion TSF_AT+CRC erfüllt, weil durch die Erzeugung des CRC-Wertes als Integritätsmerkmal für einen Leerungsdatenblock AT+ der Schutz der Benutzerdaten (AT+) vor Modifikation durch Benutzer durchgesetzt wird, wenn diese zwischen materiell getrennten Teilen des EVG übertragen werden. Dadurch, dass nur ID-Tags mit CRC zum Einsatz kommen, 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+ 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 Leerungsdatenblöcke im Primär- und Sekundärspeicher die notwendige Voraussetzung geschaffen wird, dass bei einem Verlust von Benutzerdaten im Primärspeicher der Fahrzeugsoftware durch den Transfer von Leerungsdatenblöcken von der Fahrzeugsoftware zum Sicherheitsmodul mit Hilfe der im sekundären Speicher gespeicherten Daten der Betrieb sichergestellt wird.

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

- neu gebildete Leerungsdatenblöcke AT+ durch die Funktion TSF_BSU-KEN (Auslesen der BSU 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 Zeitstempel AT2, sowie weiteren optionalen Daten in einem Leerungsdatensatz AT zusammengefasst werden,
- anschließend die Leerungsdatensätze AT sofort in die Leerungsdatenblöcke AT+ abgelegt und sofort mittels der Funktion TSF_AT+CRC durch einen CRC-Wert gesichert werden,
- diese Leerungsdatenblöcke 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 Leerungsdatenblöcke AT+ geprüft wird, wodurch die Datenintegrität der Leerungsdatensätze AT festgestellt wird,
- durch die Funktion TSF_BSU-CHK im Sicherheitsmodul der Bürosoftware die Gültigkeit der Leerungsdatenblöcke AT+ festgestellt wird.

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

9.6.2 EVG-Funktionsstärke

Da der EVG vor allem gegen unabsichtliche oder zufällige Veränderungen und Verluste von Daten, z.B. durch technische Effekte oder Defekte, wirkt, genügt für seine Prüfung zunächst die Vertrauenswürdigkeitsstufe EAL1. Diese enthält keine Familien der Klasse AVA, insbesondere keine Komponenten der Familie AVA_SOF „Stärke der Sicherheitsfunktionen“. Postulate zur EVG-Funktionsstärke sind somit nicht erforderlich.

9.7 Vertrauenswürdigkeitsmaßnahmen und Vertrauens-würdigkeitsstufe

Die Vertrauenswürdigkeitsstufe für den EVG ist EAL1. 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 der Tabelle 2 in Abschnitt 7.2 ist nachgewiesen, dass die Vertrauenswürdigkeitsmaßnahmen die Vertrauenswürdigkeitsanforderungen erfüllen.

Für einen EVG, der zum Schutz von Identifikationsdaten, Leerungsdatensätzen und Leerungsdatenblöcken 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 der CC ausreichend und angemessen.

9.8 Erklärung zu den PP-Postulaten

Die Annahmen dieser ST sind vollständig dem PP entnommen. Zusätzlich ist die Annahme A.Installation: Korrekte Inbetriebnahme hinzugekommen. Die IT-Sicherheitsanforderungen dieser ST sind vollständig dem PP entnommen. Zusätzlich ist die IT-Sicherheitsanforderungen R.Installation: Korrekte Inbetriebnahme hinzugekommen. Die Sicherheitsziele dieser ST sind vollständig dem PP entnommen. Zusätzlich ist das Sicherheitsziele OE.Installation: Korrekte Inbetriebnahme hinzugekommen.

10 Anhang

10.1 Literaturangaben

[1] Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.1, August 1999 — Teil *2*: Funktionale Sicherheitsanforderungen.

[2] Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.1, August 1999 — Teil 3: Anforderungen an die Vertrauenswürdigkeit.

[3] Schutzprofil (PP) Protection Profile Waste Bin Identification Systems WBIS-PP, Version 1.04 nach Common Criteria, Vers. 2.1

[4] Funktionale Spezifikation (FSP) Gefäßidentifikationssystem BiTech (WBIS), Version 2.16 nach Common Criteria, Vers. 2.1

[5] Identifikation der Transponder, Zu Konfigurationsmanagement (ACM), Version 1.01

[6] Gefäßidentifikationssystem BiTech Installations- und Benutzerhandbuch der Firma deister electronic GmbH

[7] BiDIP2 Installations- und Benutzerhandbuch der Firma deister electronic GmbH

[8] Handheld BHT, BHT lite, BHI, BHI Pro Manual der Firma deister electronic GmbH

10.2 Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSU	BiTech Bus Controller, deister electronic
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	On Time Programmable
PP	Protection Profile (Schutzprofil)
RB	BiTech Readermodul für Bodyantenne, deister electronic
RZ-DUO	BiTech Readermodul für zwei AZ Zahnantennen, deister electronic
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)

10.3 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

10.4 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	Zeitstempel (Datum und Uhrzeit) des Leerungsvorgangs.
AT+	Der Leerungsdatenblock AT+ wird jeweils nach Erhalt eines neuen Leerungsdatensatzes AT direkt auf der Fahrzeugsoftware gebildet. Bei der Übertragung der

Leerungsdatensätze AT von der Fahrzeugsoftware zum Sicherheitsmodul im Büro sind die Leerungsdatensätze somit bereits zu einem Leerungsdatenblock AT+ zusammengefasst. 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 beschrieben und gelesen werden.