IMELO

IMELO-Ident

Sicherheitsvorgabe für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.1

Security Target for the Waste Bin Identification System “IMELO-Secure” Version 1.1

Version:	9
Stand:	14. September 2022
Verfasser:	Markus Wagner, Hartmut Möllmann, Ulrich Schurkus, Matthias Spielmann, Pascal Steinhoff
Cert-Nr.:	BSI-DSZ-CC-1013-V2

IMELO-Ident

Sicherheitsvorgabe für das Behälter Identifikationssystem

Inhalt:

Abbildungen:

Tabellen:

IMELO-Ident
Sicherheitsvorgabe für das Behälter Identifikationssystem

1 ST Einführung

1.1 ST Identifizierung

ST Titel:	IMELO-Ident Sicherheitsvorgabe für das Behälter Identifikationssystem „IMELO-Secure“ Version 1.1
ST Version:	9
ST Datum:	14. September 2022
ST Autoren:	Markus Wagner, Hartmut Möllmann, Ulrich Schurkus, Matthias Spielmann, Pascal Steinhoff
Zertifizierungs- ID:	BSI-DSZ-CC-1013-V2

Tabelle 1: ST Identifizierung

1.2 EVG Identifikation

Gesamt EVG:

EVG-Name: IMELO-Secure
EVG-Version: 1.1

Einzelkomponenten des EVG:

Software:	IMELO-Secure.dll V1.1	Sicherheitsfunktionen für Mobilsysteme und Office unter Win32 und Win64
ID-Tag:	IMELO-Tag LF	[134,2 kHz nach DIN 30745]
	IMELO-Tag UHF	[868 MHz nach DIN 30745]
	Die genauen Typen der Transponder sind im Anhang gelistet - *Liste der ID-Tags*	

1.3 EVG Übersicht

Der Evaluierungsgegenstand (EVG) besteht aus folgenden Teilkomponenten des Behälteridentifikationssystems IMELO-IDENT:

- ID-Tag mit den Identifizierungsdaten des Abfallbehälters
- Sicherheitsmodul der Fahrzeugsoftware
- Sicherheitsmodul der Bürosoftware
- Folgende Handbücher:

Handbuch	Adressat	Referenz
IMELO-Ident Ergänzendes Benutzerhandbuch zur Handhabung der Sicherheitsfunktionen nach Common Criteria	Disponent, Fahrzeugbesatzung, Kundenadministrator, IMELO Techniker	[AGD_OPERG]
IMELO-Ident Bürosoftware IMELO Dispo2 und IMELO	Kundenadministrator,	[AGD_PREPGO]

IMELO-Ident

Sicherheitsvorgabe für das Behälter Identifikationssystem

Handbuch	Adressat	Referenz
FTP-Importdienst Installationsanleitung	IMELO Techniker	
IMELO-Ident Fahrzeugsoftware Installationsanleitung	IMELO Techniker	[AGD_PREPGV]

Tabelle 2: Übersicht der Handbücher

Die Installation der Fahrzeugsoftware wird ausschließlich durch IMELO Techniker vorgenommen, der Kunde erhält einen fertig konfigurierten Fahrzeugrechner.
Die Bürosoftware wird entweder durch den Systemadministrator des Kunden oder durch IMELO Techniker entsprechend der Installationsanleitung AGD_PREPGO vorgenommen.
Die Adressaten der Handbücher erhalten diese in digitaler Form per Email. Der Disponent ist für die Weitergabe des Benutzerhandbuches an die Fahrzeugbesatzung verantwortlich.

Dabei sind die softwareseitigen EVG-Bestandteile von der restlichen Software in der Form gekapselt, dass die Sicherheitsfunktionalitäten (vgl. Kapitel 6.1) innerhalb einer Systembibliothek (IMELO-Secure.dll) gruppiert wurden. Diese softwareseitigen Bestandteile sind in Abbildung 1 rot markiert und mit „(EVG)“ gekennzeichnet. Wie zu erkennen ist, beinhaltet das gesamte IMELO-IDENT weitere Funktionen und Dienste, die nicht Bestandteil des EVG sind, optional durch den Kunden aber genutzt werden können.

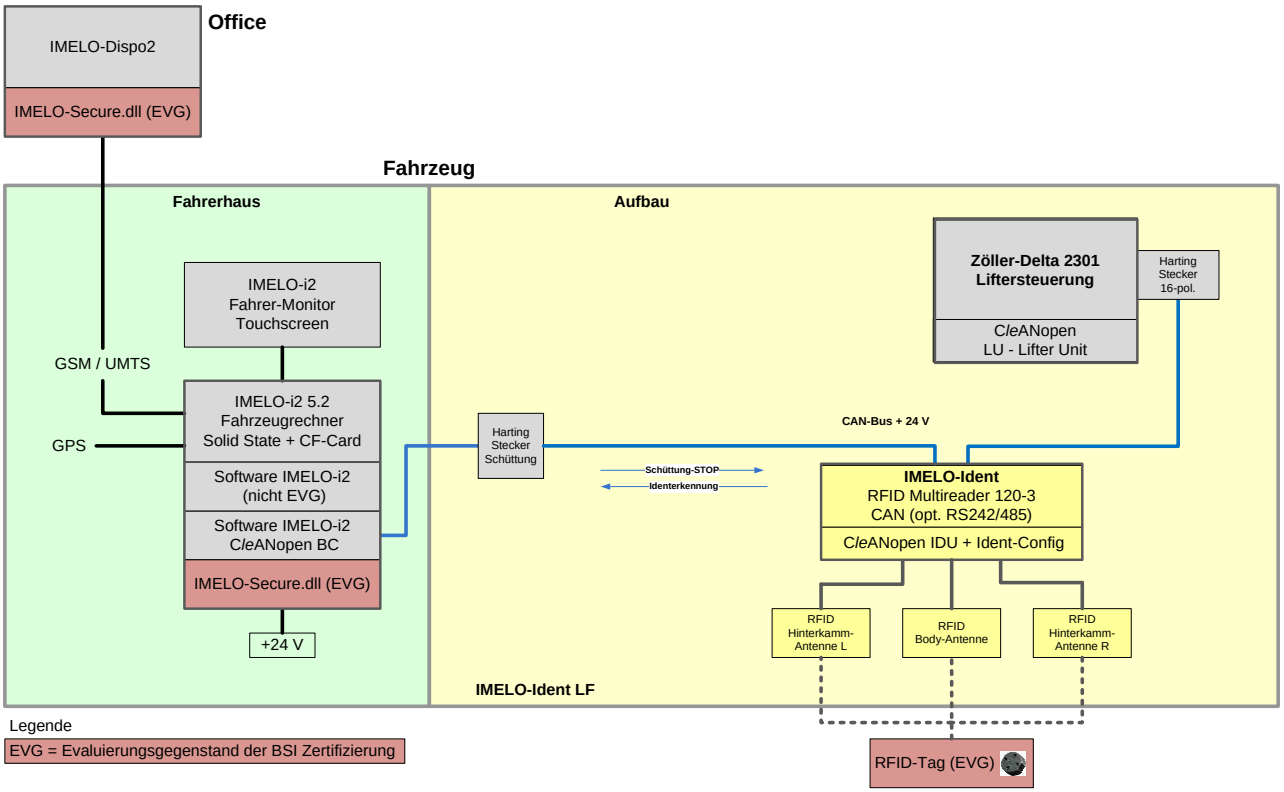


Abbildung 1: Beispiel eines IMELO-Ident Aufbaus (LF)

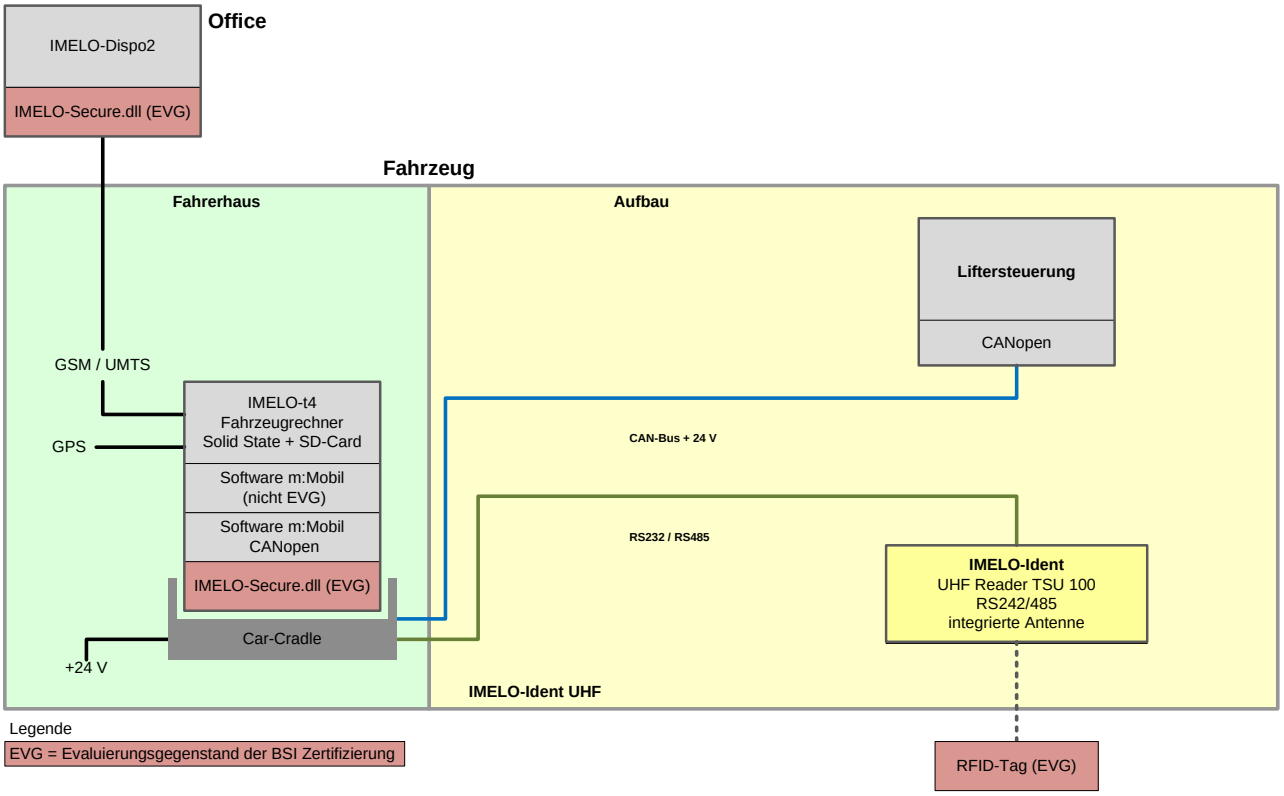


Abbildung 2: Beispiel eines IMELO-Ident –Aufbaus (UHF)

Die Kommunikation zwischen dem ID-Tag am Abfallbehälter und dem Fahrzeug wird durch den EVG in zwei möglichen Ausprägungen realisiert. Dabei kommen zum einen die LF- (134,2 kHz gemäß [DIN 30745]) und zum anderen die UHF (868 MHz gemäß [DIN 30745]) Transpondertechnologien zum Einsatz:

Datenstrombetriebsart	Antenne	Bauform	Anbauposition
HDX	Luftspule	Puck	Chipnest
HDX	Ferritkern	Puck	Chipnest
HDX	Ferritkern	Body	4-Rad Body
HDX	Ferritkern	Body	Seitlich vom Kamm
FDX	Luftspule	Puck	Chipnest
FDX	Ferritkern	Stiftsockel	Kammleiste
FDX	Luftspule	Diamond	Diamond

Tabelle 3: Überblick eingesetzte LF-Transponder

Da es im UHF-Bereich deutlich größere Reichweiten als im LF-Bereich gibt, gibt es keine Abhängigkeiten von Modulation, Antennenform, Bauform und Anbauposition. Die Auswahl der entsprechenden Konfiguration erfolgt auf Basis der Anforderungen des Kunden, hat aber keine Auswirkungen auf die Funktionsweise des EVG.

Die Übertragung der Leerungsdatenblöcke zwischen dem Fahrzeugrechner und dem Bürorechner erfolgt in einem einstellbaren Intervall via GSM/UMTS. Hierdurch wird sichergestellt, dass Leerungsdatenblöcke regelmäßig übertragen und örtlich vom Fahrzeugrechner getrennt aufbewahrt werden. Somit wird ein möglicher Datenverlust neben den in den Sicherheitsfunktionalitäten beschriebenen Prozessen minimiert.

1.3.1 Funktionen und Sicherheitsfunktionen des EVG

Der Evaluierungsgegenstand und seine zugehörigen nicht EVG-Komponenten bietet neben der Identifizierung von Abfallbehältern folgende optional nutzbare Funktionen:

- Tourplanung und Auftragsbearbeitung,
- Tourdaten, Tourführung inkl. Navigation im Fahrzeug,
- Wiegefunktion für Abfallbehälter am Fahrzeug, und
- Abrechnungserstellung im Büro

Dabei werden durch den EVG folgende Sicherheitsfunktionen gemäß der Vorgaben aus dem Schutzprofil umgesetzt:

- Überprüfung der Integrität der übergebenen Identifizierungsdaten des ID-Tag (LF und UHF),
- Integritätssicherung von Leerungsdatensätzen (AT) durch Bildung von CRC32-Checksummen,
- Integritätssicherung von Leerungsdatenblöcken (AT+) durch Bildung von CRC32-Checksummen,
- Generierung einer eindeutigen Mobilgeräteerkennung im Leerungsdatenblock,
- Authentifizierung eines Leerungsdatenblockes,
- Redundante Speicherung von Leerungsdatenblöcken und
- Wiederherstellung von Leerungsdatenblöcken vom primären oder sekundären Speicher
- Generierung einer eindeutigen Mobilgerätekennung im Leerungsdatensatz.
- Authentifizierung der Leerungsdatensätze

1.3.2 EVG Typ

Bei dem Evaluierungsgegenstand (EVG) handelt es sich um Abfallbehälteridentifikationssystem (Waste Bin Identification System) gemäß dem Schutzprofil [WBIS-PP].

1.3.3 Notwendige Nicht-EVG-Bestandteile (Hardware/Software/Firmware)

Der Evaluierungsgegenstand erfordert folgende zusätzlichen Bestandteile, um korrekt arbeiten zu können:

Notwendiger Nicht-EVG-Bestandteil	Anforderungen
Leser am Fahrzeug	Leser für LF (134,2 kHz gemäß [DIN 30745]) Leser für UHF (868 MHz gemäß [DIN 30745])
Fahrzeugrechner Hardware Variante 1 (primär LF, UHF)	Lüfterloser Truck-PC für erweiterten Temperaturbereich unter Windows XP, Windows 7, Windows 10 oder höher mit GPS-, UMTS/LTE-Modul, RS485-, RS232-Schnittstelle, Digital I/O, USB und CAN-Schnittstelle

Notwendiger Nicht-EVG-Bestandteil	Anforderungen
Fahrzeugrechner Hardware Variante 2 (UHF)	Mobiler Fahrzeugrechner unter Windows 7, Windows 10 oder höher mit GPS, UMTS/HSDPA-Modul, Farbkamera, USB-Schnittstelle zu CarCradle mit RS485-, RS232-Schnittstelle, Digital I/O und CAN-Schnittstelle
Fahrzeugrechner Software	Windows Desktop-Applikation IMELO-i2 mit den Modulen die die IMELO-Secure.dll aufrufen - i2Ident V1.2.x (* Software Versionsbildung) - i2Prozess V3.2.x - i2Transfer V3.3.x
Bürorechner – Hardware	PC unter Windows XP SP3, Windows 7, Windows 10 oder höher mit mindestens 4 GB RAM, mindestens 1,66 GHz Dual-Core-CPU, Microsoft SQL Server Express 2008 R2 Express oder höher
Bürorechner - Software	Windows Desktop-Applikation IMELO-Dispo2 mit den Modulen die die IMELO-Secure.dll aufrufen - Ifeu.ImeloDispo2.FtpImportDienst.exe V1.3.x

Tabelle 4: Anforderungen Nicht-EVG Bestandteile

Ferner sind für einige nicht EVG-Funktionalitäten sowie für die Sinnhaftigkeit des Systems auch optionale Komponenten des Gesamtsystems sowie das Fahrzeug selbst erforderlich.

* Software Versionsbildung
Auch die Softwarekomponenten die nicht EVG-Bestandteile sind haben eine dreiteilige Versionskennung V[A].[B].[C] mit folgender Bedeutung:
[A] - Ist die Hauptversion, ändert sich, wenn EVG Bestandteile verändert werden
[B] - Ändert sich, wenn Teile in der Software verändert werden, die Sicherheitsfunktionen aufrufen
[C] - Ändert sich, wenn „Nicht-EVG-Bestandteile“ verändert werden

1.4 EVG Beschreibung

Das Behälteridentifikationssystem „IMELO-Ident“ 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 **inkl. dem Sicherheitsmodul IMELO-Secure.dll V1.1** ist installiert auf dem Fahrzeugrechner.
- Bürorechner im Büro. Die Bürosoftware (**inkl. dem Sicherheitsmodul IMELO-Secure.dll V1.1**) ist auf dem Bürorechner installiert.

Die zu evaluierenden EVG-Bestandteile sind oben in fett **hervorgehoben**
Die folgende Abbildung gibt einen Überblick über das Abfallbehälter-Identifizierungssystem:

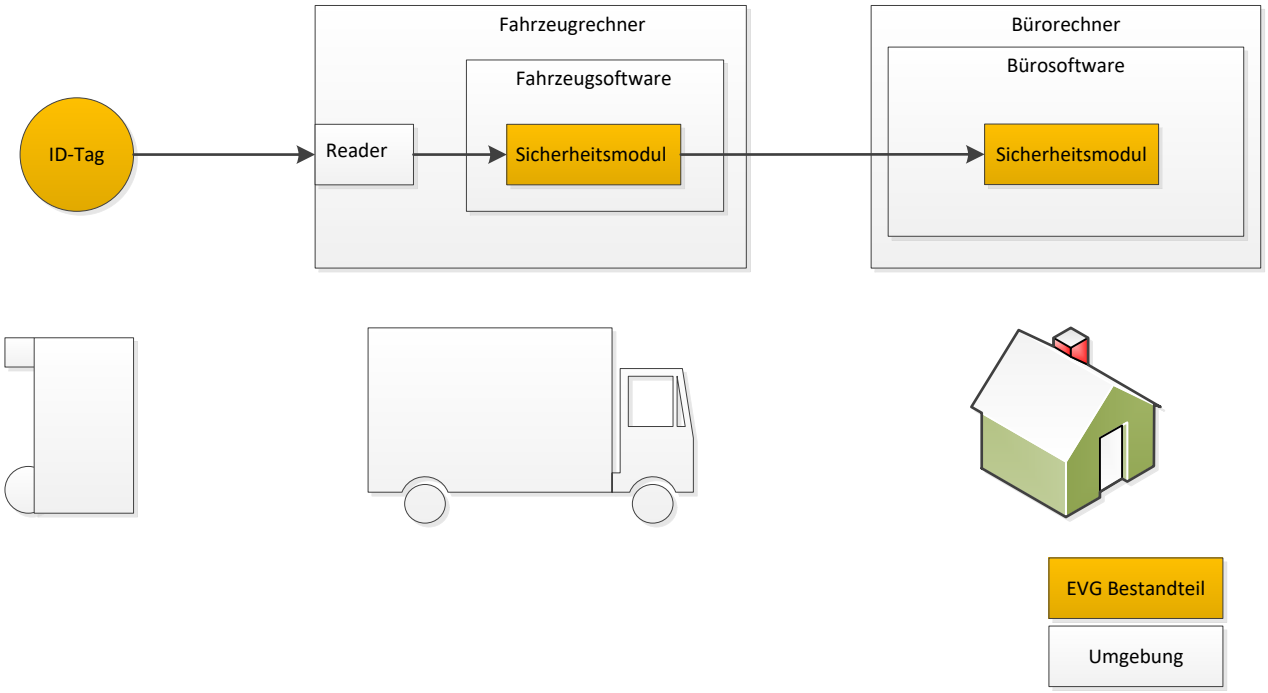


Abbildung 3: Übersicht Abfallbehälter-Identifizierungssystem

Die in der Abbildung 3 orange dargestellten Komponenten bilden den Evaluierungsgegenstand, wobei die relevanten EVG-Bestandteile der Software in einer separaten Bibliothek gekapselt sind.

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

Das System bietet die Möglichkeit, die Abrechnung über die Anzahl der Leerungen eines Abfallbehälters durchzuführen. Die Abfallbehälter werden mit einem Datenträger (ID-Tag) ausgestattet. Das ID-Tag speichert Identifizierungsdaten, die zur Identifizierung des Abfallbehälters herangezogen werden. Diese Daten sind einmalig und nicht vertraulich. Jedem Datensatz ist in der Regel ein Gebührenpflichtiger eindeutig zugeordnet. Die Identifizierungsdaten werden während (bzw. vor/nach) der Leerung eines Abfallbehälters durch den Reader ausgelesen und an die Fahrzeugsoftware weitergeleitet. Dort wird mit Sicherheitsfunktionen (IMELO-Secure.dll) die Integrität der Identifizierungsdaten des ID-Tag geprüft. 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. Anschließend wird der Datensatz inkl. der aktuellen Zeitangabe an das Sicherheitsmodul der Fahrzeugsoftware übergeben, welche den Datensatz um eine eindeutige Mobilgerätekennung ergänzt und darüber einen CRC32 generiert, anfügt und den so entstanden Leerungsdatensatz speichert.

Ein oder mehrere Leerungsdatensätze werden zu einem Leerungsdatenblock zusammengefasst und IMELO-Secure.dll generiert und ergänzt eine eindeutige Mobilgerätekennung und fügt abschließend den CRC32-Check hinzu. Es können auf diese Weise alle Leerungsdatensätze einer Tour zusammen zum Office übertragen werden.

Die IMELO-Secure.dll als Bestandteil der Fahrzeugsoftware sorgt durch geeignete Maßnahmen (z.B. Backup der Daten auf redundanten Speichern und eine zeitnahe Übermittlung an die Büro-

software) dafür, dass die Übermittlung nach vorheriger Wiederherstellung 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 Fahrzeug erstellten Datenblöcke 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 Datenblöcken enthalten sind, oder die Datenblöcke 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.

Das ID-Tag und die Datenübertragungsstrecke zwischen dem ID-Tag und der Fahrzeugsoftware, die im Fahrzeug gespeicherten Daten sowie die Übertragungstrecke zwischen der Fahrzeugsoftware und dem Sicherheitsmodul sind potenziellen Angriffen ausgesetzt. Bei der Betrachtung des Angriffspotenzials muss der potenzielle Wert der zu schützenden Daten in Betracht gezogen werden. Dieser Wert ist als gering zu sehen. Es wird deshalb ein niedriges Angriffspotential (basic attack potential) 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.

1.4.1 Physische und logische Abgrenzung des Evaluierungsgegenstandes

Der Evaluierungsgegenstand ist ein Produkt im Sinne der Common Criteria. Der Evaluierungsgegenstand besteht (wie in Abbildung 3 dargestellt) aus dem ID-Tag, dem Sicherheitsmodul (IMELO-Secure.dll) der Fahrzeugsoftware und dem Sicherheitsmodul (IMELO-Secure.dll) des Bürorechners. Alle anderen Komponenten (siehe auch Abb. 1) sind nicht Bestandteil des Evaluierungsgegenstands und gehören zu dessen Umgebung.
Der Evaluierungsgegenstand ist ein verteiltes System bestehend aus dem ID-Tag, dem Sicherheitsmodul der Fahrzeugsoftware und dem Sicherheitsmodul der Bürosoftware. Schnittstellen sind zwischen dem ID-Tag (EVG) und dem Reader (Nicht-EVG) sowie zwischen dem Sicherheitsmodul der Fahrzeugsoftware (EVG) und der Fahrzeugsoftware (Nicht-EVG) bzw. dem Sicherheitsmodul der Bürosoftware (EVG) und der Bürosoftware (Nicht-EVG) vorhanden. Die Sicherheitsfunktionalitäten (vgl. Kapitel 6.1) werden ausschließlich von EVG-Bestandteilen umgesetzt. Weitere Funktionen außerhalb des Evaluierungsgegenstandes sind nicht Bestandteil der Evaluierung. Die Abrechnungssoftware ist auch kein Bestandteil des Evaluierungsgegenstandes.

2 Postulat der Übereinstimmung

2.1 Postulat der Übereinstimmung mit den CC

Die Sicherheitsvorgaben sowie der EVG sind konform zu:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017 [CC_P1],
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 5, April 2017 [CC_P2],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 5, April 2017 [CC_P3],
- Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017 [CEM].

Der EVG und die Sicherheitsvorgabe erweitert den zweiten Teil der CC [CC_P2] um FDP_ITT.5 und sind konform zum dritten Teil der CC [CC_P3].

2.2 Postulat der Übereinstimmung mit Schutzprofilen

Diese Sicherheitsvorgaben sind konform (strict conformance) zu den folgenden Common Criteria Schutzprofilen:

- Protection Profile Waste Bin Identification Systems WBIS-PP (Version 1.04), BSI-PP-0010-2004 [WBIS-PP].

Die EVG Sicherheitsumgebung, die Sicherheitsanforderungen und die Sicherheitsziele innerhalb dieser Sicherheitsvorgaben wurden aus dem Schutzprofil [WBIS-PP] übernommen. Zusätzlich wurde eine weitere Annahme, sowie ein weiteres zugehöriges Sicherheitsziel für die EVG-Umgebung definiert.

2.3 Postulat der Übereinstimmung zur Vertrauenswürdigkeitsstufe

Die Sicherheitsvorgaben sowie der EVG sollen die im Schutzprofil vorgegebene Vertrauenswürdigkeitsstufe, wie es der dritte Teil der Common Criteria [CC_P3] für Produktzertifizierungen definiert, erreichen. Darüber hinaus wurde die Vertrauenswürdigkeitsstufe um

- ASE_OBJ.2,
- ASE_REQ.2, und
- ASE_SPD.1

erweitert, so dass sich die Vertrauenswürdigkeitsstufe EAL1 augmented ergibt.

2.4 Konformitätsbegründung

Die EVG-Sicherheitsumgebung (ASE_SPD[1]) der vorliegenden Sicherheitsvorgabe enthält alle Elemente der EVG-Sicherheitsumgebung des Schutzprofils [WBIS-PP]. Es wurden keinerlei Be-

[1] ASE_SPD wird definiert um eine strict conformance zum Schutzprofil [WBIS-PP] zu erfüllen.

drohungen oder organisatorische Sicherheitspolitiken hinzugefügt. Es wurde lediglich eine Annahme zur eindeutigen Mobilgeräteerkennung aufgenommen, die jedoch nicht der EVG-Sicherheitsumgebung des Schutzprofils widerspricht. Somit sind die Sicherheitsvorgaben konform (strict conformance) zu dem Schutzprofil. Somit sind auch die EVG-Typen dieses STs und des [WBIS-PP] übereinstimmend.
Die Sicherheitsziele dieser Sicherheitsvorgaben enthalten ebenfalls alle Sicherheitsziele des Schutzprofils [WBIS-PP]. Zusätzlich wurde ein Sicherheitsziel für die Umgebung zur eindeutigen Mobilgerätekennung aufgenommen. Keine im Schutzprofil definierten Sicherheitsziele wurden geändert oder entfernt. Das hinzugefügte Sicherheitsziel für die Umgebung widerspricht nicht den im Schutzprofil definierten Sicherheitszielen. Somit sind die Sicherheitsvorgaben bezüglich der Sicherheitsziele konform (strict conformance) zu dem Schutzprofil.
Die Sicherheitsanforderungen dieser Sicherheitsvorgaben sind ebenfalls identisch zu den Sicherheitsanforderungen des Schutzprofils. Alle Operationen innerhalb der funktionalen Sicherheitsanforderungen sind in der vom Schutzprofil vorgegebenen Art und Weise durchgeführt worden, wodurch die Sicherheitsanforderungen konform zum Schutzprofil [WBIS-PP] sind. Details über die Anforderungen können dem Kapitel 5 entnommen werden.

3 EVG-Sicherheitsumgebung

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

Schutzwürdige Objekte

Schutzwürdiges Objekt	Beschreibung	
AT	Ein Leerungsdatensatz AT zu einer Leerung ist ein schutzwürdiges Objekt in einem WBIS. Ein Leerungsdatensatz AT besteht aus den Datenfeldern: • Transpondernummer (AT1) • Zeitstempel (AT2) • Leerungsstatus (gestoppt oder geleert) (AT3) • Optional Gewicht (AT4) • Optional Geokoordinate (Längengrad, Breitengrad) im Format WGS84 (AT5) • Optional Liftertyp • Optional Barcode des Behälteretikettes Zu schützen sind dabei die unten aufgeführten Datenfelder mit der Kennung **AT**x	
	AT1	Identifikationsdaten des Abfallbehälters
	AT2	Zeitstempel (Datum und Uhrzeit) des Leerungsvorgangs.
	AT3	Leerungsstatus
	AT4	Gewicht (Netto, Brutto, Tara, Status), falls vorhanden
	AT5	Geokoordinate, falls vorhanden
	AT6	Mobilgerätekennung (MobilgeräteID/Computername)
AT+	Vor der Übertragung der Leerungsdatensätze AT von der Fahrzeugsoftware zum Sicherheitsmodul im Büro werden die Leerungsdatensätze zu einem Leerungsdatenblock AT+ zusammengefasst. Der Leerungsdatenblock AT+ ist ein schutzwürdiges Objekt in einem WBIS bei der Kommunikation zwischen der Fahrzeugsoftware und dem Sicherheitsmodul.	

Tabelle 5: Schutzwürdige Objekte

Subjekte

Subjekt	Beschreibung
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.

Tabelle 6: Subjekte

Angreifer

Angreifer	Beschreibung
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

Tabelle 7: Angreifer

3.1 Annahmen

Annahme	Beschreibung
A.Id	*ID-Tag* Das ID-Tag befindet sich fest am Abfallbehälter. Die Identifizierungsdaten (AT1) des Abfallbehälters sind in dem ID-Tag gespeichert. Es werden nur ID-Tags mit einmaligen Identifizierungsdaten installiert. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des Evaluierungsgegenstandes sicherzustellen.
A.Trusted	*Vertrauenswürdiges Personal* Die Besatzung des Fahrzeugs und die Benutzer des Bürorechners (S.Trusted) sind autorisiert und [2]vertrauensvoll. Alle Personen, die das System installieren oder warten sind autorisiert und vertrauenswürdig (S.Trusted). Alle Personen, die für die Sicherheit der Umgebung verantwortlich sind, (S.Trusted) sind autorisiert und vertrauenswürdig.
A.Access	*Zugangsschutz* Die Umgebung stellt durch geeignete Maßnahmen (Verschluss, Zugangskontrolle durch Passwörter usw.) sicher, dass nur die Benutzer bzw. das Servicepersonal (S.Trusted) den direkten Zugang zu allen Komponenten des Evaluierungsgegenstands, außer zum ID-Tag, haben. Die Beeinflussung der internen Verbindungskanäle durch einen potenziellen Angreifer (S.Attack) innerhalb der IT - Struktur des Bürorechners ist aufgrund geeigneter Maßnahmen ausgeschlossen.
A.Check	*Überprüfung der Vollständigkeit* Der Benutzer (S.Trusted) prüft in regelmäßigen Abständen, ob alle Leerungsdatenblöcke (At+) von dem Fahrzeugrechner übertragen worden sind (Vollständigkeit der Übertragungen). Erkannte Datenverluste werden vom Benutzer in einem bestimmten Zeitraum durch erneute Anforderung beim Fahrzeugrechner behoben. Dieser Zeitraum ist konsistent mit der Kapazität des entsprechenden Speichers am Fahrzeugrechner, der zur Speicherung der Leerungsdatenblöcke (AT+) zur Verfügung steht.
A.Backup	*Datensicherung* Der Benutzer (S.Trusted) sichert die vom Evaluierungsgegenstand erzeugten Daten regelmäßig im Archiv. Der Evaluierungsgegenstand schützt nicht vor Datenverlusten im Archiv.
A.UId	*Eindeutige Mobilgerätekennung* Der mit der Installation des Fahrzeugrechners beauftragte Benutzer (S.Trusted) generiert gemäß der im Handbuch spezifizierten Syntax eine eindeutige Mobilgerätekennung. Diese wird durch den Benutzer (S.Trusted) vor Integration in die

[2] Korrektur des PP 6.2.2.3 A.Trusted worin „authorised“ fehlt.

Annahme	Beschreibung
	Fahrzeugsoftware mithilfe der herstellerinternen Datenbank auf Eindeutigkeit und Korrektheit überprüft. Anschließend sorgt der Benutzer (S.Trusted) dafür, dass die eindeutige Mobilgerätekennung zur weiteren Verarbeitung in der Büro-software hinterlegt wird.

Tabelle 8: Annahmen

3.2 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.

Bedrohung	Beschreibung
T.Man	*Manipulierte Identifikationsdaten* Ein Angreifer (S.Attack) manipuliert die Identifizierungsdaten (AT1) im ID-Tag durch Mittel (z.B. mechanische Einwirkung), die die Identifizierungsdaten (AT1) ausschließlich rein zufällig verfälschen.
T.Jam#1	*Gestörte Identifkationsdaten* Ein Angreifer (S.Attack) stört die Übertragung der Identifizierungsdaten (AT1) vom IDTag zum Reader im Fahrzeug durch Mittel (z.B. elektromagnetische Strahlung), die die Identifizierungsdaten (AT1) ausschließlich rein zufällig verfälschen.
T.Create	*Ungültige Leerungsdatensätze* Ein Angreifer (S.Attack) erzeugt beliebige Leerungsdatenblöcke (AT+) und über-trägt diese an das Sicherheitsmodul.
T.Jam#2	*Verfälschte Leerungsdatensätze* Ein Angreifer (S.Attack) verfälscht Leerungsdatensätze (AT) während der Bear-beitung und der Speicherung innerhalb des Fahrzeuges oder stört die Übertra-gung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicher-heitsmodul z.B. durch elektromagnetische Strahlung, um die Daten der Lee-rungsdatenblöcke (AT+) ausschließlich rein zufällig zu verfälschen.

Tabelle 9: Bedrohungen

3.3 Organisatorische Sicherheitspolitik

Die folgende Regel wird für den EVG formuliert:

Politik	Beschreibung
P.Safe	*Fehlertoleranz* Die Fahrzeugsoftware muss sicherstellen, dass die Daten der Leerungsdatenblö-cke (AT+) durch eine redundante Speicherung in einem sekundären Speicher so zu schützen sind, dass die Übertragung der Leerungsdatenblöcke von der Fahr-zeugsoftware zum Sicherheitsmodul nach einem Verlust der Daten in einem pri-mären Speicher möglich ist.

Tabelle 10: Organisatorische Sicherheitspolitik

4 Sicherheitsziele

Dieser Abschnitt identifiziert und definiert die Sicherheitsziele für den EVG und seine Umgebung. Sicherheitsziele spiegeln die festgelegte Absicht wider und begegnen den identifizierten Bedrohungen. Zusätzlich entsprechen sie der identifizierten Sicherheitspolitik und den Annahmen.

4.1 Sicherheitsziele für den EVG

Die Sicherheitsziele für den EVG sind exakt dem Schutzprofil [WBIS-PP] entnommen.

Sicherheitsziel	Beschreibung
OT.Inv#1	*Erkennung von ungültigen Identifizierungsdaten* Der EVG soll manipulierte Identifizierungsdaten (AT1), die im ID-Tag gespeichert sind oder während der Übertragung zwischen dem ID-TAG und dem Leser im Fahrzeug verändert wurden, erkennen.
OT.Inv#2	*Erkennung von ungültigen Leerungsdatensätzen* Der EVG soll jeden Versuch, willkürliche Leerungsdatenblöcke (AT+) an das Sicherheitsmodul zu übertragen, erkennen. Der EVG soll Manipulationen von Leerungsdatensätzen (AT) während der Verarbeitung und Speicherung im Fahrzeug erkennen. Ferner soll der EVG Manipulationen des Leerungsdatensatzes erkennen, die durch zufällige Störungen während der Übertragung vom Sammelfahrzeug an das Sicherheitsmodul entstanden sind.
OT.Safe	*Fehlertoleranz* Die Fahrzeugsoftware als Teil des EVG soll sicherstellen, dass die Daten der Leerungsdatenblöcke durch eine redundante Speicherung in einem sekundären Speicher in einer Art und Weise gesichert werden, dass die Übertragung der Leerungsdatenblöcke (AT+) von der Fahrzeugsoftware zum Sicherheitsmodul für den Fall möglich ist, dass Leerungsdatenblöcke (AT+) im primären Speicher der Fahrzeugsoftware verloren gehen.

Tabelle 11: Sicherheitsziele EVG

4.2 Sicherheitsziele für die Umgebung

Sicherheitsziel	Beschreibung
OE.Id	*ID-Tag* Der ID-Tag befindet sich fest am Abfallbehälter. Die Identifizierungsdaten (AT1) des Abfallbehälters sind in dem ID-Tag gespeichert. Es werden nur ID-Tags mit einmaligen Identifizierungsdaten verwendet. Die korrekte Zuordnung dieser Daten zum Gebührenpflichtigen ist organisatorisch außerhalb des EVG zu realisieren.
OE.Trusted	*Vertrauenswürdiges Personal* Durch organisatorische Maßnahmen wird sichergestellt, dass die Besatzung des Sammelfahrzeuges sowie die Benutzer des Bürorechners (S.Trusted) autorisiert und vertrauenswürdig sind. Alle Personen, die das System installieren oder warten sind autorisiert und vertrauenswürdig. Alle Personen, die für die Sicherheit der Einsatzumgebung (S.Trusted) verantwortlich sind, sind autorisiert und vertrauenswürdig.
OE.Access	*Zugangsschutz* Die Einsatzumgebung stellt durch geeignete Maßnahmen (Verschluss, Zugangs-

Sicherheitsziel	Beschreibung
	kontrolle durch Passwörter etc.) sicher, dass nur Benutzer bzw. das Serviceper-sonal (S.Trusted) über einen direkten Zugriff zu allen Komponenten mit Ausnah-me des ID-Tags verfügen. Die Manipulation der internen Verbindungskanäle durch einen potentiellen Angreifer (S.Attack) innerhalb der IT-Struktur des Büro-rechners muss durch ausreichende Maßnahmen ausgeschlossen werden.
OE.Check	*Überprüfung der Vollständigkeit* Der Benutzer (S.Trusted) überprüft in regelmäßigen Abständen, ob die vom Fahr-zeug an das Sicherheitsmodul übertragenen Daten vollständig sind. Erkannte Datenverluste sind durch den Benutzer durch erneute Anforderung der Daten vom Fahrzeugrechner zu beheben. Der Zeitraum muss konsistent mit der Kapazi-tät des entsprechenden Speichers am Fahrzeug sein.
OE.Backup	*Datensicherung* Es soll sichergestellt sein, dass in regelmäßigen Zeitabständen durch den Benut-zer (S.Trusted) Sicherheitskopien der vom EVG erzeugten Daten erstellt werden.
OE.UId	*Eindeutige Mobilgerätekennung* Es soll sichergestellt werden, dass durch den mit der Installation des Fahrzeug-rechners beauftragten Benutzer (S.Trusted) gemäß der im Handbuch spezifizier-ten Syntax eine eindeutige Mobilgerätekennung erstellt wird. Zusätzlich muss sichergestellt werden, dass der Benutzer (S.Trusted) diese vor Integration in die Fahrzeugsoftware mithilfe der herstellerinternen Datenbank auf Eindeutigkeit und Korrektheit überprüft. Anschließend soll der Benutzer (S.Trusted) dafür sorgen, dass die eindeutige Mobilgerätekennung zur weiteren Verarbeitung in der Büro-software hinterlegt wird.

Tabelle 12: Sicherheitsziele für die Umgebung

4.3 Erklärung der Sicherheitsziele

4.3.1 Abdeckung der Sicherheitsziele

Bedrohung, Annahme, Poli-tik / Sicher-heitsziele	OT.Inv#1	OT.Inv#2	OT.Safe	OE.Id	OE.Trusted	OE.Access	OE.Check	OE.Backup	OE.UId
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.UId									X

Bedrohung, Annahme, Politik / Sicherheitsziele	OT.Inv#1	OT.Inv#2	OT.Safe	OE.Id	OE.Trusted	OE.Access	OE.Check	OE.Backup	OE.UId
P.Safe			X						

Tabelle 13: Abdeckung Sicherheitsziele

4.3.2 Zulänglichkeit der Sicherheitsziele

4.3.2.1 Bedrohungen und Hinlänglichkeit der Sicherheitsziele

T.Man (Manipulierte Identifikationsdaten) definiert Angriffe, bei denen die Identifizierungsdaten (AT1) innerhalb der Identifizierungseinheit ID-Tag manipuliert werden. Dem wird durch das Sicherheitsziel OT.Inv#1 begegnete, indem der EVG manipulierte Identifizierungsdaten während der Übertragung zwischen ID-Tag und Fahrzeug oder beim Speichern im ID-Tag erkennt. Dadurch wird die Bedrohung T.Man direkt abgewehrt.
T.Jam#1 (Gestörte Identifikationsdaten) definiert Angriffe, bei denen der Transfer der Identifizierungsdaten (AT1) zwischen ID-Tag und Leser am Fahrzeug elektromagnetisch gestört wird (z.B. durch elektromagnetische Einflüsse). Dem wird durch das Sicherheitsziel OT.Inv#1 begegnet, indem der EVG gestörte Identifizierungsdaten während der Übertragung zwischen ID-Tag und Fahrzeug erkennt. Dadurch wird die Bedrohung T.Jam#1 direkt abgewehrt.
T.Create (Ungültige Leerungsdatensätze) definiert Angriffe, bei denen Leerungsdatensätze willkürlich erzeugt werden und an das Sicherheitsmodul übertragen werden. Dem wird durch das Sicherheitsziel OT.Inv#2 begegnet, indem der EVG jegliche Versuche von willkürlich übertragenen Leerungsdatensätzen an das Sicherheitsmodul erkennt. Dadurch wird die Bedrohung T.Create direkt abgewehrt.
T.Jam#2 (Verfälschte Leerungsdatensätze) definiert Angriffe, bei denen Leerungsdatensätze (AT) während ihrer Verarbeitung und Speicherung im Sammelfahrzeug zerstört werden oder deren Übertragung zum Sicherheitsmodul gestört wird. Dem wird durch das Sicherheitsziel OT.Inv#2 begegnet, indem der EVG jegliche Störungsversuche während des Transfers der Daten sowie manipulierte gespeicherte Datensätze erkennt. Dadurch wird die Bedrohung T.Jam#2 direkt abgewehrt.

4.3.2.2 Annahmen und Hinlänglichkeit der Sicherheitsziele

A.Id (ID-Tag) definiert, dass das ID-Tag am Abfallbehälter befestigt ist und es die eindeutigen identifizierungsdaten (AT1) des Behälters beinhaltet. Die Zuordnung zwischen der Identifizierungseinheit und dem Gebührenpflichtigen ist durch organisatorische Maßnahmen hergestellt. Da das Sicherheitsziel OE.Id exakt das gleiche bestätigt, ist es hinreichend für die Annahme A.Id.
A.Trusted (Vertrauenswürdiges Personal) stellt sicher, dass alle Subjekte (bis auf der Angreifer) autorisiert[3] und vertrauenswürdig sind. Das Sicherheitsziel OE.Trusted bestätigt exakt das gleiche und ist somit hinreichend für die Annahme A.Trusted.
A.Access (Zugangsschutz) definiert, dass der Zugang zum EVG mit Ausnahme der Identifizierungseinheit, ausschließlich für autorisiertes und vertrauenswürdiges Personal möglich ist. Darüber hinaus schließt es die Fähigkeit eines Angreifers aus, den internen Verbindungskanal innerhalb der IT-Struktur des Bürorechners zu beeinflussen. Das Ziel OE.Access bestätigt exakt dieses und ist somit hinreichend für die Annahme A.Access.
A.Check (Überprüfung der Vollständigkeit) stellt sicher, dass der Benutzer regelmäßig überprüft, ob die vom Sammelfahrzeug zum Büro übertragenen Daten vollständig sind. Ein dabei er-

[3] Der Wortlaut wurde hier zur Behebung einer Inkonsistenz des Schutzprofils angepasst.

kannter Verlust kann durch eine erneute Übertragung der Daten behoben werden. Die Überprüfungsintervalle sind dabei konsistent mit der Kapazität des zugehörigen Speichers auf dem Bordrechner des Sammelfahrzeuges zu wählen. Da das Ziel OE.Check dies exakt bestätigt, ist es hinlänglich für die Annahme A.Check.
A.Backup (Datensicherung) stellt sicher, dass der Benutzer in regelmäßigen Zeitabständen Sicherheitskopien von den Daten erstellt, die der EVG erzeugt. Das Ziel OE.Backup bestätigt dies exakt und ist somit hinreichend für die Annahme A.Backup.
A.UId (Eindeutige Mobilkerätekennung) stellt sicher, dass der Benutzer bei der Installation der Software eine eindeutige Mobilgerätekennung erzeugt, diese überprüft, in die Fahrzeugsoftware integriert und für die spätere Datenverarbeitung in der Bürosoftware hinterlegt. Das Ziel OE.UId bestätigt dies exakt und ist somit hinreichend für die Annahme A.UId.

4.3.2.3 Politik und Hinlänglichkeit der Sicherheitsziele

P.Safe (Fehlertoleranz) legt fest, dass die Verfügbarkeit der Leerungsdaten bei der Übertragung von der Bordrechner-Software zum Sicherheitsmodul auch im Falle des Verlustes aus dem Primärspeicher durch redundante Datenhaltung mithilfe eines Sekundärspeichers gegen ist. Dies ist das exakt wiederholte Sicherheitsziel OT.Safe, so dass dieses Ziel hinlänglich durch P.Safe abgedeckt ist.

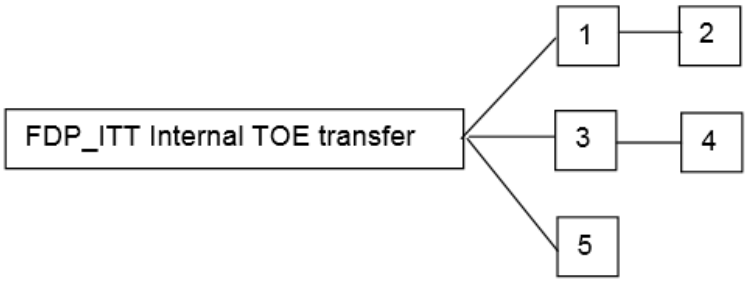
4.4 Erweiterte Komponentendefinition

Die erweiterte Komponentendefinition basiert vollständig auf dem Anhang C des Schutzprofils [WBIS-PP, 9] und dient dazu eine weitere funktionale Sicherheitsanforderung (FDP_ITT.5) aus der Famile FDP_ITT (internal TOE transfer / interne EVG Transfer) zu definieren.
FDP_ITT.5 beschreibt die funktionale Sicherheitsanforderung zum Integritätsschutz der Daten. Dabei wird ein im Vergleich zu FDP_ITT.1 stärker eingegrenzter Ansatz verfolgt, da es nicht notwendigerweise gefordert ist, dass der EVG eine Zugangskontrollrichtlinie und/oder Informationsflussrichtlinie implementiert. Daher wird hier lediglich die Manipulation von Daten adressiert.

Die Famile „internal TOE transfer“ (FDP_ITT) wird wie folgt erweitert (es werden lediglich Änderungen dargestellt).

FDP_ITT Internal TOE transfer

Component levelling



FDP_ITT.5 Der interne Integritätsschutz während des Transfers erfordert es, dass Benutzerdaten gegen Manipulation geschützt werden, während sie zwischen den unterschiedlichen Bestandteilen des EVG übermittelt werden.

FDP_ITT.5 Interner Integritätsschutz während des Transports

Hierarchisch zu: Keinen anderen Komponenten

FDP_ITT.5.1	Die TSF müssen die Einhaltung der [Zuweisung: *Integritätsrichtlinie(n)*] erzwingen, um die Modifizierung von Benutzerdaten zu verhindern, wenn diese zwischen physisch getrennten EVG-Teilen übertragen werden

Abhängigkeiten: Keine Abhängigkeiten

5 IT-Sicherheitsanforderungen

Dieses Kapitel definiert die funktionalen Sicherheitsanforderungen und die Anforderungen an die Vertrauenswürdigkeit des EVG und dessen Umgebung.
Die Komponenten der funktionalen Sicherheitsanforderungen werden in Kapitel 5.1 „Funktionale Sicherheitsanforderungen an den EVG“ beschrieben und sind aus der Common Criteria [CC] abgeleitet worden. Ausgenommen hiervon ist die Komponente FDP_ITT.5, welche im Schutzprofil [WBIS-PP] definiert worden ist. Operationen, die in diesen Sicherheitsvorgaben auf funktionale Sicherheitsanforderungen durchgeführt wurden, sind *kursiv* dargestellt.
Die Übersicht über die Anforderungen an die Vertrauenswürdigkeit des EVG ist weiter oben“ zu finden, und wurde aus den Common Criteria [CC] abgeleitet.
Der Abschnitt 5.3 identifiziert die IT-Sicherheitsanforderungen, die durch die IT Umgebung einzuhalten sind.
Die Anforderungen an die Nicht-IT Umgebung sind in Abschnitt 5.4 beschrieben.

5.1 Funktionale Sicherheitsanforderungen an den EVG[4]

5.1.1 Datenauthentisierung (FDP_DAU)

5.1.1.1 Einfache Datenauthentisierung (FDP_DAU.1)

FDP_DAU.1.1 Die TSF müssen eine Funktion zur Generierung von Nachweisen als Gültigkeitsgarantie von *Leerungsdatensätzen (AT) und Leerungsdatenblöcken (AT+)*[5] bereitstellen.

FDP_DAU.1.2 Die TSF müssen den *Benutzern (S.Trusted)* [6]die Möglichkeit zur Verifizierung des Gültigkeitsnachweises der angezeigten Informationen bereitstellen

5.1.2 EVG interner Transfer (FDP_ITT)

5.1.2.1 Integrität der internen Übertragung (FDP_ITT.5)

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

FDP_ITT.5.1 Die TSF müssen die Einhaltung der *Datenintegritätspolitik* [7]erzwingen, um die Modifizierung von Benutzerdaten zu verhindern, wenn diese zwischen physisch getrennten EVG-Teilen übertragen werden

Die folgende Sicherheitsfunktionspolitik (SFP) **Datenintegritätspolitik** ist für die Anforderung „Einfacher interner Übertragungsschutz (FDP_ITT.5) definiert:
„Die Benutzerdaten (AT1 und AT+) müssen geschützt werden, um ihre Integrität zu gewährleisten.“

[4] Die nachfolgenden funktionalen Sicherheitsanforderungen wurden aus Lesbarkeitsgründen ins Deutsche übersetzt.
[5] Assignment des PP: list of objects or information types
[6] Assignment des PP: list of subjects
[7] Assignment des PP: Integrity SFP(s)

5.1.3 Integrität der gespeicherten Daten (FDP_SDI)[8]

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

FDP_SDI.1.1 Die TSF müssen die innerhalb von Blöcken gespeicherten und von den TSF kontrollierten Benutzerdaten auf *zufällige Manipulation* [9]bei allen Objekten auf Basis folgender Attribute überwachen: *Identifizierungsdaten AT1 in der Identifizierungseinheit ID-Tag und den Leerungsdatensatz AT während der Speicherung im Fahrzeug*[10].

5.1.4 Fehlertoleranz (FRU_FLT.1)

5.1.4.1 Verminderte Fehlertoleranz (FRU_FLT.1)

FRU_FLT.1.1 Die TSF müssen den Betrieb der *Übertragung der Leerungsdatenblöcke (AT+) von der Bordrechner-Software zum Sicherheitsmodul mit Hilfe der im sekundären Speicher gesicherten Daten*[11] sicherstellen, wenn die folgenden Fehler auftreten: *Verlust der Benutzerdaten im primären Speicher des Sammelfahrzeuges*[12].

5.2 Vertrauenswürdigkeitsanforderungen des EVG

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

Tabelle 14: Vertrauenswürdigkeitsanforderungen EAL1+

[8] FDP_SDI wurde in der Form vom PP abgewandelt, dass der aktuelle Wortlaut aus der CC 3.1 Rev. 4 verwendet wurde
[9] Assignment des PP: integrity errors
[10] Assignment des PP: user data attributes
[11] Assignment des PP: list of TOE capabillities
[12] Assignment des PP: list of type of failures

5.2.1 Entwicklung (ADV)

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

5.2.1.1 Funktionale Spezifikation (ADV_FSP)

Durch den Entwickler muss eine funktionale Spezifikation bereitgestellt werden, die die EVG Sicherheitsfunktionen (TSF) und ihre externen Schnittstellen beschreibt. Dabei müssen der Zweck und die Methode aller externen TSF-Schnittstellen einschließlich der Auswirkungen, Parameter und Fehlermeldungen vollständig dargestellt werden.

5.2.2 Handbücher (AGD)

Die Schutzklasse AGD definiert Anforderungen an die Verständlichkeit, Abdeckung und Vollständigkeit der vorbereitenden und benutzerführenden Dokumentation. Als Benutzer werden alle Personen angesehen, die befugt sind den EVG im Einklang mit den funktionalen Sicherheitsanforderungen zu betreiben. Durch diese Dokumentation wird sichergestellt, dass alle Benutzer-Rollen in der Lage sind den EVG sicher zu betreiben.

5.2.2.1 Operatives Benutzerhandbuch (AGD_OPE)

Der Hersteller hat ein Benutzer-Handbuch bereitzustellen, das die Funktionen und Schnittstellen beschreibt, die für die Benutzer des EVG zur Verfügung stehen. Dabei sind auch die vom EVG bereitgestellten Sicherheitsfunktionen, die für den Benutzer zugänglich sind zu beschreiben. Das Benutzer-Handbuch muss alle Verantwortlichkeiten des Benutzers klar definieren, die für den sicheren Betrieb notwendig sind. Dazu zählen auch Maßnahmen, die zur Erfüllung der Annahmen für die Umgebung umzusetzen sind. Zusätzlich muss das Handbuch die Sicherheitsanforderungen an die IT-Umgebung des EVG beschreiben

5.2.2.2 Vorbereitende Prozeduren (AGD_PRE)

Der Entwickler hat eine Installationsanleitung bereitzustellen, die alle Informationen vermittelt, die notwendig sind um sicherzustellen, dass sein Exemplar des EVG akzeptiert, konfiguriert und aktiviert werden kann. Dabei müssen auch Informationen über die Sicherheitsfunktionen enthalten sein und wie die korrekte Funktionsweise dieser Sicherheitsfunktionen im Betrieb zu gewährleisten sind.

5.2.3 Lebenszyklus (ALC)

Die Schutzklasse ALC definiert Anforderungen für die Qualitätssicherung durch die Annahme eines genau definierten Lebenszyklus-Modells für alle Schritte der TOE-Entwicklung. Dazu zählen auch der Umgang mit Fehlern, der Einsatz eines Konfigurationsmanagementsystems, die richtige Verwendung von Werkzeugen, Schutz der Entwicklungs- und Produktionsumgebung sowie die Auslieferung an den Kunden.

5.2.3.1 Konfigurationsmanagement Einsatzmöglichkeiten (ALC_CMC)

Der Entwickler muss die Eigenschaften des eingesetzten Konfigurationsmanagementsystems dokumentieren.

5.2.3.2 Konfigurationsmanagement Abgrenzung (ALC_CMS)

Der Entwickler muss den Geltungsbereich seines Konfigurationsmanagementsystems dokumentieren und beschreiben, welche EVG-Bestandteile einem solchen System unterliegen. Diese Angaben müssen sich auch im Inhalt der mitgelieferten Konfigurations-Dokumentation wiederfinden.

5.2.4 Testen (ATE)

Diese Schutzklasse definiert die Anforderungen an durchzuführende Tests. Dabei werden die Abdeckung der Tests, die korrekte Funktionsweise des EVG sowie eine Überprüfung der Sicherheitsunktionen durchgeführt.

5.2.4.1 Unabhängiges Testen (ATE_IND)

Der Entwickler muss den EVG in der (den) zu zertifizierenden Konfigurationen(en) zum Testen bereitstellen.

5.2.5 Schwachstellenanalyse (AVA_VAN)

Diese Schutzklasse beschreibt mögliche Schwachstellen in der Entwicklung oder dem Betrieb des EVG. Es wird dabei analysiert, ob potentielle Schwachstellen die während der Evaluierung identifiziert wurden durch einen Angreifer mit dem definierten Angriffspotential ausgenutzt werden können.

5.3 Sicherheitsanforderungen für die IT Umgebung

Diese Sicherheitsvorgaben verlangen gem. dem Schutzprofil [WBIS-PP] keine Sicherheitsanforderungen an die IT-Umgebung.

5.4 Sicherheitsanforderungen für die Nicht-IT Umgebung

Sicherheitsanforderung	Beschreibung
R.Id	*ID-Tag* Der Benutzer muss folgendes sicherstellen: • Die Identifikationseinheit muss fest an dem Abfallbehälter befestigt werden, der durch die Identifikationsdaten in dieser Einheit identifiziert wird. • Die Identifikationsdaten in dieser Einheit sind eindeutig. • Die Zuordnung der Identifikationsdaten zu einem Gebührenpflichtigen erfolgen durch organisatorische Maßnahmen, welche sich nicht im Bereich des EVG befinden. Hierzu zählt auch die Generierung der eindeutigen Mobilgerätekennung und deren Integration in die Fahrzeugsoftware, sowie die Hinterlegung in der Bürosoftware
R.Trusted	*Vertrauenswürdiges Personal* Die Personen, die das Sammelfahrzeug und das Sicherheitsmodul bedienen, installieren und warten sollen autorisiert und vertrauenswürdig sein. Alle Personen, die für die Sicherheit der Betriebsumgebung verantwortlich sind, sollen dafür autorisiert und vertrauenswürdig sein.
R.Access	*Zugangsschutz* Die Umgebung muss durch geeignete Maßnahmen sicherstellen, dass nur die Benutzer und das Wartungspersonal direkten Zugang zu den EVG-Komponenten haben (mit Ausnahme des Zugangs zur Identifikationseinheit). Die Umgebung soll jede Art der Beeinflussung der internen Verbindungskanäle des Bürorechners verhindern.
R.Check	*Überprüfung auf Vollständigkeit* Der Benutzer soll in regelmäßigen Zeitabständen die Vollständigkeit der

Sicherheitsanforderung	Beschreibung
	Übertragung der Leerungsdatenblöcke (AT+) vom Sammelfahrzeug in das Büro überprüfen. Der Benutzer soll die Wiederherstellung und Übertragung der Daten anfordern, von denen er annimmt, dass sie noch nicht vom Sammelfahrzeug in das Büro übertragen worden sind. Die Zeitintervalle der Überprüfung sind konsistent zu der verfügbaren Speicherkapazität des sekundären Speichers des Bordrechners zu wählen.
R.Backup	*Datensicherung* Der Benutzer soll die Daten, die vom EVG erzeugt werden, in regelmäßigen Abständen in einem angebrachten Archiv sichern.

Tabelle 15: Sicherheitsanforderungen für die Nicht-IT Umgebung

5.5 Hinlänglichkeit der Sicherheitsanforderungen

5.5.1 Hinlänglichkeit der Sicherheitsanforderungen des EVG

OT.Inv#1 (Erkennung von ungültigen Identifizierungsdaten) behandelt die Erkennung von manipulierten Identifizierungsdaten (AT1) von Leerungsdatensätzen (AT) innerhalb der Identifizierungseinheit und während der Übertragung zwischen der Identifizierungseinheit und der Bordrechner-Software, welche ein separater EVG-Teil ist. Der Schutz der Integrität der Identifizierungsdaten (AT1), welche in der Identifizierungseinheit gespeichert sind, ist durch FDP_SDI.1 gefordert und deckt zufällige Veränderungen dieser Daten ab. Der Schutz der Integrität der Benutzerdaten (AT1) während der Übertragung zwischen den physisch getrennten Teilen des EVG wird durch FDP_ITT.5 gefordert. Die Sicherung der Datenintegrität schützt also direkt vor Veränderungen der Daten während ihrer Übertragung.
OT.Inv#2 (Erkennung von ungültigen Leerungsdatensätzen) behandelt die Erkennung von manipulierten Leerungsdatensätzen (AT+), welche zwischen der Bordrechnersoftware und dem Sicherheitsmodul übertragen werden; d.h. zwischen zwei physikalisch getrennten Teilen des EVG. Der Schutz der Integrität dieser Benutzerdaten (AT+) wird durch FDP_ITT.5 für die Übertragung zwischen den physisch getrennten EVG-Teilen gefordert. Der Schutz der Datenintegrität schützt dabei gleichzeitig gegen Manipulation der Daten.
OT.Inv#2 behandelt ferner auch die Erkennung von ungültigen Leerungsdatensätzen (AT) während ihrer Verarbeitung und Speicherung im Fahrzeug, sowie die Erkennung einer Manipulation der Leerungsdatensätze (AT), welche zum Sicherheitsmodul übertragen werden. Der EVG liefert gemäß FDP_DAU.1 eine Funktion zur Erzeugung eines Beweises, welcher durch den Benutzer zur Gültigkeitsprüfung genutzt werden kann. Der Schutz der Integrität der im Fahrzeug gespeicherten Benutzerdaten (AT), wird durch FDP_SDI.1 gefordert und wehrt direkt zufällige Veränderungen von diesen Daten ab. Die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 unterstützen sich gegenseitig für die Datenauthentisierung und Integrität. Daher decken die Anforderungen FDP_ITT.5, FDP_DAU.1 und FDP_SDI.1 das Sicherheitsziel OT.Inv#2 hinlänglich ab.
OT.Safe (Fehlertoleranz) behandelt die Verfügbarkeit relevanter Daten für die Übertragung der Leerungsdatensätze (AT+) zwischen dem Fahrzeug und dem Sicherheitsmodul im Falle eines Datenverlustes im Bereich des primären Speichers der Fahrzeugsoftware. Die Funktionalität für diese Datenübertragung wird mit Hilfe eines sekundären Speichers im Falle des Verlustes der Daten aus dem primären Speicher, durch den EVG gemäß FRU_FLT.1 realisiert.

EVG funktionale Sicherheitsanforderung / EVG Sicherheitsziele	OT.Inv#1	OT.Inv#2	OT.Save
FDP_DAU.1		X	
FDP_ITT.5	X	X	
FDP_SDI.1	X	X	
FRAU_FLT.1			X

Tabelle 16: Zuordnung funktionale Sicherheitsanforderungen zu Sicherheitszielen

5.5.2 Hinlänglichkeit der Sicherheitsanforderungen der Umgebung des TOE

OE.Id (Identifizierungseinheit) wird bereitgestellt durch R.Id, da R.Id fordert, was das Ziel OE.Id bestätigt.
OE.Trusted (Vertrauenswürdiges Personal) wird bereitgestellt durch R.Trusted, da R.Trusted fordert, was das Ziel OE.Trusted bestätigt.
OE.Access (Zugangsschutz) wird bereitgestellt durch R.Access, da R.Access fordert, was das Ziel OE.Access bestätigt.
OE.Check (Überprüfung der Vollständigkeit) wird bereitgestellt durch R.Check, da R.Check fordert, was das Ziel OE.Check bestätigt.
OE.Backup (Datensicherung) wird bereitgestellt durch durch R.Backup, da R.Backup fordert, was das Ziel OE.Backup bestätigt.

Anforderungen an die Nicht-IT Umgebung / Sicherheitsziele für die Umgebung	OE.ID	OE.Trusted	OE.Access	OE.Check	OE.Backup	OE.UId
R.ID	X					X
R.Trusted		X				
R.Access			X			
R.Check				X		
R.Backup					X	

Tabelle 17: Zuordnung Anforderungen Nicht-IT Umgebung zu Sicherheitszielen Umgebung

5.6 Erfüllung der Abhängigkeiten

Da die Vertrauenskomponenten exakt der Vertrauenswürdigkeitsstufe EAL 1 entnommen wurden, sind alle Abhängigkeiten erfüllt.
Die Abhängigkeiten der funktionalen Sicherheitsanforderungen für den EVG und dessen Umgebung sind nur zum Teil erfüllt. Die folgende Tabelle gibt einen Überblick über die Abhängigkeiten und erläutert, inwiefern diese erfüllt werden:

Anforderung	Abhängigkeit gem. CC Teil 2	Erfüllt
FDP_DAU.1	Keine Abhängigkeiten	Ja
FDP_ITT.5	Keine Abhängigkeiten	Ja
FDP_SDI.1	Keine Abhängigkeiten	Ja
FRU_FLT.1	FPT_FLS.1	Nein, siehe nachfolgenden Text

Tabelle 18: Abhängigkeiten

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

5.7 Begründung zur Auswahl der Vertrauenswürdigkeitsstufe EAL1+

Die Vertrauenswürdigkeitsstufe für diese Sicherheitsvorgabe ist EAL1+. Dieser Level bewirkt einen weitaus höheren Sicherheitsgrad gegenüber einem nicht evaluierten IT-Produkt oder –System, indem es Vertrauen in den korrekten Betrieb vermittelt. Währenddessen werden die Bedrohungen nicht als ernst angesehen, was in direkter Beziehung zu dem eher niedrig anzusiedelnden Wert der vom EVG zu schützenden Daten steht. EAL1+ bietet unabhängige Sicherheit, um unterstützend dafür Sorge zu tragen, dass im Umgang mit Informationen aus den Leerungsdatensätzen verantwortungsvoll umgegangen wird und dass der EVG einen den Kundenanforderungen angemessenen Schutz gegenüber bekannten Bedrohungen bietet. Durch EAL1+ werden die Sicherheitsfunktionen des EVG unabhängig getestet und die bereitgestellten Anleitungen und Dokumentationen ausführlich evaluiert. Dabei ist mit EAL1+ berücksichtigt, dass eine Prüfung auch ohne das Mitwirken des Herstellers des EVG ohne größere Anstrengungen durchgeführt werden kann. Hierdurch wird die notwendige Flexibilität berücksichtigt, unterschiedliche Systeme mit verschiedenen auf dem Markt erhältlichen Komponenten zusammenzustellen und dabei die Kosten für die Evaluation gering zu halten.

6 EVG Übersichtsspezifikation

6.1 EVG Sicherheitsfunktionen

6.1.1 SF_ID_CHECK_LF

Die vom Reader weitergegebene TransponderID wird mithilfe des ebenfalls übermittelten CRC16 Wertes des LF-Transponders durch die Sicherheitsfunktion auf Integrität geprüft.
Dabei bildet die Funktion eine eigene CRC16-Prüfsumme über die empfangene TransponderID und vergleicht diese mit der entsprechenden mitübermittelten CRC16-Prüfsumme, die in den Transponderdaten hinterlegt ist.
Die Funktion dient zur Umsetzung von FDP_SDI.1.1 und FDP_ITT.5.1.

6.1.2 SF_ID_CHECK_UHF

Die vom Reader weitergegebene TransponderID wird mithilfe des ebenfalls übermittelten CRC16 Wertes des UHF-Transponders durch die Sicherheitsfunktion auf Integrität geprüft.
Dabei bildet die Funktion eine eigene CRC16-Prüfsumme über die empfangene TransponderID und vergleicht diese mit der entsprechenden mitübermittelten CRC16-Prüfsumme, die in den Transponderdaten hinterlegt ist.
Die Funktion dient zur Umsetzung von FDP_SDI.1.1 und FDP_ITT.5.1.

6.1.3 SF_CRC_GEN_AT

Die Sicherheitsfunktion besteht aus zwei Teilen:

1. Funktion zur Ermittlung der eindeutigen Mobilgerätekennung des Fahrzeugrechners. Die Funktion dient zur Umsetzung von FDP_DAU.1.1 und FDP_DAU.1.2
2. Funktion, die einen Leerungssatz mit der zuvor ermittelten eindeutigen Mobilgerätekennung generiert und um eine CRC32-Checksumme über die Elemente AT1-6 ergänzt.
   Die Funktion dient zur Umsetzung von FDP_SDI.1.1.

6.1.4 SF_CRC_GEN_ATP

Die Sicherheitsfunktion besteht aus zwei Teilfunktionen:

1. Funktion zur Ermittlung der eindeutigen Mobilgerätekennung des Fahrzeugrechners.
   Die Funktion dient zur Umsetzung von FDP_DAU.1.1 und FDP_DAU.1.2.
2. Funktion, die aus den Leerungsdatensätzen (AT) und der zuvor ermittelten eindeutigen Mobilgerätekennung des Fahrzeugrechners einen Leerungsdatenblock generiert und vor Übertragung eines Leerungsdatenblockes AT+ eine CRC32-Checksumme über alle enthaltenen Checksummen der Leerungsdatensätze (AT) sowie die angefügte Mobilgerätekennung bildet.
   Die Funktion dient zur Umsetzung von FDP_ITT.5.1.

6.1.5 SF_CRC_CHECK_AT

Funktion zur Prüfung eines Leerungsdatensatzes AT auf Integrität, indem die CRC32-Checksumme über die enthaltenen Elemente AT1-6 berechnet und mit der im Leerungsdatensatz AT enthaltenen Checksumme verglichen wird.
Die Funktion dient zur Umsetzung von FDP_SDI.1.1.

6.1.6 SF_CRC_CHECK_ATP

Funktion zur Prüfung eines Leerungsdatenblockes AT+ auf Integrität, indem die CRC32-Checksumme über alle im Leerungsdatenblock enthaltenen Checksummen von Leerungsdatensätzen AT sowie die im Leerungsdatenblock AT+ gespeicherte eindeutige Mobilgerätekennung gebildet wird und mit der im Leerungsdatenblock AT+ gespeicherten Checksumme verglichen wird. Nach erfolgreicher Integritätsprüfung wird immer SF_MID_CHECK zur Authentifizierung des Leerungsdatenblockes AT+ verwendet.
Die Funktion dient zur Umsetzung von FDP_ITT.5.1.

6.1.7 SF_MID_CHECK

Funktion zur Authentifizierung eines Leerungsdatenblockes AT+ durch Vergleich der im Leerungsdatenblock gespeicherten eindeutigen Mobilgerätekennung mit der Liste der zulässigen Mobilgerätekennungen.
Die Funktion dient zur Umsetzung von FDP_DAU.1.1 und FDP_DAU.1.2.

6.1.8 SF_STORE_ATP

Funktion, die die mit Checksummen und eindeutiger Mobilgerätekennung versehenen Leerungsdatenblöcke AT+ redundant auf dem primären und sekundären Speicher ablegt.
Die Funktion dient zur Umsetzung von FRU_FLT.1.1.

6.1.9 SF_RESTORE_ATP

Funktion, die einen oder mehrere mit Checksummen und eindeutigen Mobilgerätekennungen versehenen Leerungsdatenblöcke AT+ vom primären oder sekundären Speicher liest.
Die Funktion dient zur Umsetzung von FRU_FLT.1.1.

6.1.10 SF_MID_CHECK_AT

Funktion zur Authentifizierung eines Leerungsdatensatzes AT durch Vergleich der im Leerungsdatensatz gespeicherten eindeutigen Mobilgerätekennung mit der Liste der zulässigen Mobilgerätekennungen.
Die Funktion dient zur Umsetzung von FDP_DAU.1.1 und FDP_DAU.1.2.

6.2 Hinlänglichkeit der EVG Sicherheitsfunktionen

	EVG-Teil	FDP_DAU.1.1	FDP_DAU.1.2	FDP_ITT.5.1	FDP_SDI.1.1	FRU_FLT.1.1
SF_ID_CHECK_LF	Fahrzeug			X	X	
SF_ID_CHECK_UHF	Fahrzeug			X	X	
SF_CRC_GEN_AT	Fahrzeug	X	X		X	
SF_CRC_GEN_ATP	Fahrzeug	X	X	X		

	EVG-Teil	FDP_DAU.1.1	FDP_DAU.1.2	FDP_ITT.5.1	FDP_SDI.1.1	FRU_FLT.1.1
SF_CRC_CHECK_AT	Office				X	
SF_CRC_CHECK_ATP	Office			X		
SF_MID_CHECK	Office	X	X			
SF_STORE_ATP	Fahrzeug					X
SF_RESTORE_ATP	Office					X
SF_MID_CHECK_AT	Office	X	X			

Tabelle 19: Hinlänglichkeit der EVG Sicherheitsfunktionen

7 Glossar

ADV	Development
AGD	Guidance Documents
ALC	Life-Cycle Support
ASE	Security Target Evaluation
ATE	Tests
AVA	Vulnerability Assessment
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria (referenced as CC)
CCL	Conformance claims
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
CMC	CM capabilities
CMS	CM scope
COV	Coverage of testing
DEL	Delivery
DVS	Development security
EAL	Evaluation Assurance Level
EVG	Evaluierungsgegenstand
FW	Firmware
FLR	Flaw remediation
FSP	Functional specification
GD	Guidance documents
GUI	Graphical User Interface
HW	Hardware
IMP	Implementation
IND	Independent testing
IP	Internet Protocol
IT	Information Technology
LCD	Life-cycle definition
MB	Mega Byte
OBJ	Security objectives
OBJ	Security objectives
OPE	Operational user guidance
OR	Observation Report
OS	Operating System
OSP	Organisational Security Policy
PC	Personal Computer
PP	Protection Profile
PRE	Preparative procedures
RAM	Random Access Memory
REQ	Security requirements
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SPD	Security problem definition
ST	Security Target
SW	Software
TAT	Tools and techniques
TDS	TOE design

IMELO-Ident

Sicherheitsvorgabe für das Behälter Identifikationssystem

TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interfaces
TSFR	TOE SFR
TSP	TOE Security Policy
TSS	TOE summary specification
UID	Unique Identification number
VAN	Vulnerability analysis
VPN	Virtual Private Network
WBIS	Waste Bin Identification System
WU	Work Unit

8 Referenzen

[AGD_OPERG]	IMELO-Ident Ergänzendes Benutzerhandbuch zur Handhabung der Sicherheitsfunktionen nach Common Criteria, Version 6
[AGD_PREPGO]	IMELO-Ident Bürosoftware IMELO Dispo2 und IMELO FTP-Importdienst Installationsanleitung, Version 7
[AGD_PREPGV]	IMELO-Ident Fahrzeugsoftware Installationsanleitung, Version 5
[CC]	Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2012-09-001. Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2012-09-002. Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2012-09-003.
[CC_P1]	Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-20012-09-001.
[CC_P2]	Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2012-09-002.
[CC_P3]	Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2012-09-004.
[DIN 30745]	Elektronische Identifikation von Abfallsammelbehältern durch Transpondertechnologie mit Frequenzen unter 135 kHz und 868 MHz; Ausgabe 2014-06
[WBIS-PP]	Protection Profile Waste Bin Identification Systems WBIS-PP, Version 1.04, BSI-PP-0010-2004

9 Anhang

9.1 Liste der Ident-Tags

IMELO-TAG LF [134,2 kHz nach DIN 30745]

Artikelnummer	Artikeltyp / Bauform	Artikelbeschreibung
2021273	FDX als Luftspule / Puckgehäuse für Chipnestmontage	BDE Konforme Transponder mit einer Frequenz von 134,2 kHz
2021274	HDX als Luftspule / Puckgehäuse für Chipnestmontage	
1150626	HDX als Luftspule / Puckgehäuse für Chipnestmontage	
1150627	FDX als Luftspule / Puckgehäuse für Chipnestmontage	
1150630	FDX als Luftspule / Puckgehäuse für Chipnestmontage	
1150638	HDX als Luftspule / Puckgehäuse für Chipnestmontage	
1150642	HDX als Glasröhrchen / Puckgehäuse für Chipnestmontage	
1150648	HDX als Glasröhrchen (Ferritkern)/ Stiftsockel	
1150652	HDX als Luftspule / Bodytransponder zur Rumpfmontage	
1151050	HDX als Luftspule, Chipnest, flache Bauform	

IMELO-Ident

Sicherheitsvorgabe für das Behälter Identifikationssystem

IMELO-Tag UHF [868 MHz nach DIN 30745]

Artikelnummer	Artikeltyp / Bauform	Artikelbeschreibung
1151007 1151008	Stabtransponder	BDE Konforme Transponder mit einer Frequenz von 868 MHz
1150658	Luftspule / Puckgehäuse für Chipnestmontage	
1151009	Platetransponder	
1150688	Platetransponder	
1150696	Transponder zur direkten Montage auf Metall	
1150700	Labeltransponder, klebbar	
1150702	ISO-Karten-Transponder, Schrauben oder Nieten	