# Protection Profile
# Waste Bin Identification System
# WBIS-PP
# Version 1.03

—— this page was intentionally left blank ——

## Foreword

This ‘Protection Profile — Waste Bin Identification System’ is issued by Bundesamt für Sicherheit in der Informationstechnik, Germany.

The document has been prepared as a Protection Profile (PP) following the rules and formats of ISO 15408, as known as the Common Criteria version 2.1 [1], [2], [3].

Correspondence and comments to this Waste Bin Identification System Protection Profile (WBIS-PP) should be referred to:

CONTACT ADDRESS

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53175 Bonn, Germany
Tel +49 1888 9582-0
Fax +49 1888 9582-400
Email bsi@bsi.bund.de

*Application note for German speaking users (Anwendungshinweis zur Sprache):*

Das vorliegende Schutzprofil (Protection Profile) ist in Englisch verfasst. Eine deutsche Übersetzung der Kapitel 1.1 PP-Identifizierung (PP-Identification), 2 EVG-Beschreibung (TOE Description) und 3 EVG-Sicherheitsumgebung (TOE Security Environment) ist im Kapitel 8 zu finden.

—— this page was intentionally left blank ——

Table Of Contents

# List of Tables

Conventions

The document follows the rules and conventions laid out in Common Criteria 2.1, part 1 [1], Annex B “Specification of Protection Profiles”.

# Document Organisation

Section 1 provides the introductory material for the Protection Profile.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [2] and Part 3 [3], that must be satisfied by the TOE.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 6 provides a set of arguments that address dependency analysis and the internal consistency and mutual supportiveness of the protection profile requirements.

A reference section is provided to identify background material.

An acronym list is provided to define frequently used acronyms.

# 1 Introduction

This section provides document management and overview information that is required to carry out protection profile registry. Therefore, section 1.1 “Identification” gives labelling and descriptive information necessary for registering the Protection Profile (PP). Section 1.2 “Protection Profile Overview” summarises the PP in narrative form. As such, the section gives an overview to the potential user to decide whether the PP is of interest. It is usable as stand-alone abstract in PP catalogues and registers.

## 1.1 Identification

| | |
|---|---|
| Title: | Protection Profile — Waste Bin Identification System |
| Sponsor: | Bundesamt für Sicherheit in der Informationstechnik |
| Editors: | Cezary Glowacz, Dr. Burkhard Grimm<br>T-Systems GEI GmbH Business Unit ITC Security |
| CC Version: | 2.1 Final |
| Assurance Level: | The minimum assurance level for this PP is EAL1. |
| General Status: | Final |
| Version Number: | 1.03 |
| Registration: | None |
| Keywords: | waste bin identification, data capture, record of clearance, town council |

## 1.2 Protection Profile Overview

This Protection Profile is the work of parties involved in manufacturing and operation of systems for waste disposal related industry.

The intent of this Protection Profile is to specify functional and assurance requirements for the waste bin identification systems (WBIS) which is the target of evaluation (TOE). The Protection Profile defines the security requirements of WBIS for the transfer and storage of records of clearance data. The TOE may implement additional functions and security requirements, but these additional functions and security requirements are not subject to this Protection Profile.

Waste bin identification systems (WBIS) in the sense of this document are systems, which allow to identify waste bins by an ID-tag (e.g. an electronic chip which is referred to as transponder) in order to determine how often a specific waste bin has been cleared. Note that this type of system does not identify the waste directly but the waste bin, which contains the waste for disposal.

The purpose of this type of systems is to count, how often the waste bins have been cleared in order to allow an originator-related billing of waste fees. Frequently, such systems are combined with e.g. a weighing or volume measurement system in order to allow billing according to the frequency of clearance and the weight or volume of the waste disposed of. Other procedures can be thought of and can be integrated into this type of system in the future.

Many town councils in Germany have already implemented such systems from different manufacturers. Some manufacturers have received various ITSEC certificates for their products. However, the town councils as end-users need a certainty concerning the comparability of security certificates which can be required in invitations for tenders for such systems. Therefore it has been requested to BSI to ensure the comparability of competing security certificates by means of a Protection Profile. Aside from the initiative of the town councils as users for the creation of a Protection Profile this Protection Profile can also be used

for billing scenarios in the private domain and business areas.

Waste bin identification systems (WBIS) comprise the electronic collection of data, the transfer and recording of clearance data (which serve as activity confirmation of the waste management enterprises) and the creation of notifications for waste fees by the responsible statutory corporations (cities and rural districts) or the issuing of invoices by the waste management enterprises. As a result of the vast amount of accumulated data it is not possible to manually check in detail every clearance which is to be invoiced. Therefore a high level of confidence is required for the technical reliability of such systems, in the respect that exactly those clearances which have actually been performed are related to the correct originator (i.e. the correct waste bin). As a result it is necessary to protect the data relevant for the billing process (identification data and time stamps) against manipulation and loss within the system.

These data are created when a collection vehicle clears a waste bin. As a result a record of clearance is formed based on the ID number of the bin.

After a collection vehicle has finished a clearance tour the collected data are transmitted to the office of the maintenance and storage facility (either of the community or the private waste management enterprise) by means of possibly different media (data media, wire connection, wireless). In the office these data are stored in a central database. From there the data can be transmitted on a regular basis to authorities or regional computer centres for the billing process.

## 1.3 PP Organisation

The main sections of the PP are its TOE description, TOE Security Environment, Security Objectives, Security Requirements, and Rationale.

The TOE description provides general information about the TOE, serves as an aid to understanding its security requirements, and provides context for the PP's evaluation.

The TOE security environment describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes descriptions of a) assumptions regarding the TOE's intended usage and environment of use, b) threats relevant to secure TOE operation, and c) organisational security policies with which the TOE must comply.

The security objectives reflect the stated intent of the PP. They pertain to how the TOE will counter identified threats and it will cover identified organisational security policies and assumptions. Each security objective is categorised as being for the TOE or for the environment.

The section of IT security requirements is subdivided as follows: (a) TOE security functional requirements, (b) TOE security assurance requirements, (c) security requirements for the IT environment, and (d) security requirements for the Non-IT environment.

The application notes contain additional supporting information on the TOE security environment and on the security functional requirements. The information is intended for the author of a Security Target which is based on this Protection Profile.

The rationale presents evidence that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

The rationale is divided into two main parts. First, a security objectives rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE

security environment and are suitable to cover them. Then, a security requirements rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them.

# 2 TOE Description

The waste bin identification system (WBIS) consists of the following components:

- ID-Tag containing the identification data of the waste bin
- Vehicle with ID-Tag reader, vehicle computer and an optional weighing, volume or similar measurement system. The vehicle software is installed on the vehicle computer.
- Office computer in the office. The security module and the office software are installed on the office computer.

The following Figure shows an overview of the waste bin identification system.

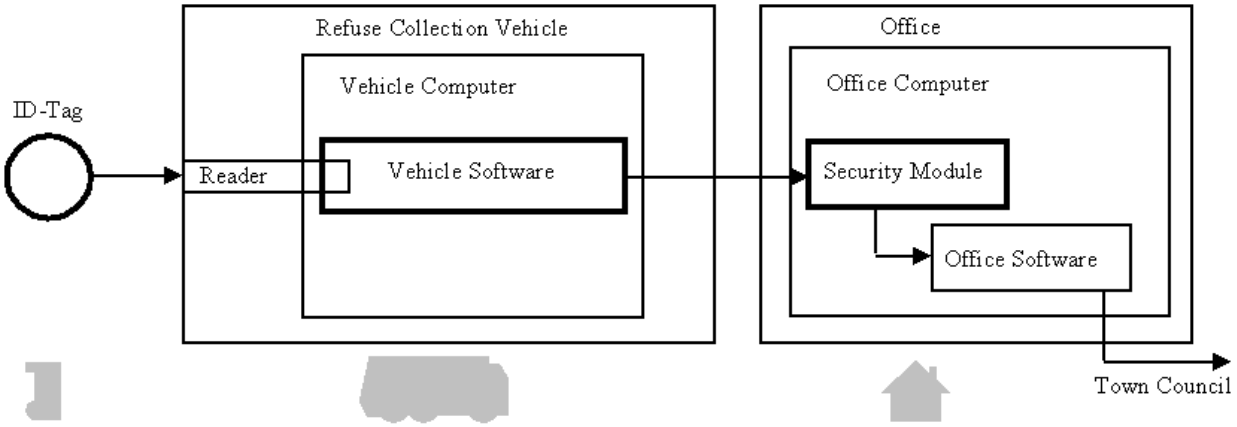



Figure 1: Waste Bin Identification System

The waste bin identification system implements an originator-related billing and assessment of fees for waste management. Aside from the use of these systems by town councils other areas of application in billing scenarios in the private domain and business areas are possible.

The system allows billing scenarios according to the number of clearances of a specific waste bin. The system can optionally comprise e.g. a weighing or volume measurement system for a weight-based billing. Other supplementary modes of operation are possible in the future.

The waste bins are equipped with a data carrier (ID-Tag). The ID-Tag stores identification data, which are used for the identification of the waste bin. These data are unique and not confidential. Usually there is a one to one correspondence between a set of identification data and the person who is subject to charge. The identification data are read during (or before/after) clearance of the waste bin by the reader. Possible malfunctions during transfer and manipulations are detected. The identification data is then transmitted to the vehicle software. Optionally the weight of the waste or the filling height of the waste bin are determined by a dedicated sensors in the vehicle and are transmitted in parallel to the identification data to the vehicle software. The vehicle software supplements these data by adding a date and time information and then forms a record of clearance from all these data.

One or more records of clearance are combined to a clearance data block. In this way all clearance records of a tour can be combined to a clearance data block of the entire tour.

The clearance data blocks are transmitted by the security module to the office software. The vehicle software ensures by means of adequate measures (e.g. backup of data) that the transfer is even possible after a loss of data in the primary memory. The security module

ensures that during transfer of clearance data blocks to the office software only those data blocks which were created in a clearance vehicle are accepted as valid data. In addition, possible malfunctions during transfer are detected.

The clearance data blocks can be stored on the office computer by the office software. Optionally the data blocks can be analysed further in order to defeat additional possible attacks (invalid, copied identification data, etc.). The clearance records contained in the clearance data blocks or the whole clearance data blocks themselves are transmitted to external systems (e.g. of the town council authorities) for the billing process. Such external systems can provide additional functionality (e.g. detection of possible misuse in replayed clearance data blocks etc.) aside from the billing functionality to supplement the security functionality of the TOE.

The ID-Tag and the data transfer between the ID-Tag and the vehicle software, the data stored in the vehicle as well as the transfer between the vehicle software and the security module are subject to potential attacks. When considering the attack potential one must take into account the potential value of the data to be protected. This value can be regarded as low. Therefore low attack potential can be assumed. Only authorised personnel has access to the vehicle software and the security module due to suitable physical and organisational measures. This protection is implemented by the vehicle with its components and the office with the office computer.

## Limits of the TOE

The TOE is a product for the purpose of the Common Criteria. The TOE consists of an ID-Tag, the vehicle software and the security module. All other components (see also Fig. 1) are not part of the TOE but of the TOE environment. The TOE has an external interface to the memories of the vehicle computer, a logical internal interface between the ID-Tag and the vehicle software, a logical internal interface between the vehicle software and the security module, and an external interface between the security module and the office software. The physical channel from the ID-Tag to the vehicle software and from the vehicle software to the security module are not part of the TOE. Only the internal interfaces are considered in this PP. Additional interfaces, especially to the accounting centres of the town councils, are not part of the evaluation. The office software is also not part of the TOE. However, the author of a Security Target can extend the security functionality.

# 3 TOE Security Environment

The purpose of this section is to define the nature and scope of the “security needs” to be addressed by the TOE. Therefore this section will involve (i) any assumptions that are made regarding the TOE environment, (ii) the assets requiring protection, the identified threat agents and the threats they pose to the assets, and (iii) organisational security policies or rules with which the TOE must comply in addressing the security needs.

In the following the assets, subjects and the threat agents will be defined first.

## Assets

**AT** A record of clearance AT corresponding to a clearance of a waste bin is an asset in the WBIS. The record of clearance AT consists of the following data fields:

**AT1** Identification data of the waste bin

**AT2** Time stamp (date and time) of the clearance.

*Application Note 1:*

*The record of clearance AT will be created within components of the TOE installed in the vehicle, for example in the vehicle computer or in the reader. The identification data AT1 is stored in the ID-Tag and it is the asset itself until the creation of the record of clearance AT. The record of clearance AT can as an option consist of further data fields like for example information about the weight of the collected waste.*

**AT+** The records of clearance AT will be combined to clearance data blocks AT+ before transfer from the vehicle software to the security module. The clearance data block AT+ is an asset in WBIS during transfer between vehicle software and security module.

*Application Note 2:*

*A clearance data block (AT+) can combine the records of clearance for an entire clearance tour.*

## Subjects

**S.Trusted** *Trustworthy User*

The crew of the collection vehicle and the users of the office computer. Personnel for installation and maintenance of the system. Furthermore personnel responsible for the security of the environment.

## Threat agents

**S.Attack** *Attacker*

A human or a process acting on his behalf located outside the TOE. The main goal of the S.Attack attacker is to modify or corrupt application sensitive information. The attacker has at most a knowledge of obvious vulnerabilities.

*Application Note 3:*

*The data of the record of clearance (AT) or of clearance data block (AT+) can be corrupted during transfer by purely random effects. Such corruptions are not considered as threats here since no attacker can be identified. The effectiveness of eventually implemented functionality can be verified by functional tests (homologation testing).*

## 3.1 Assumptions

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

The ID-Tag is fastened to the waste bin. The identification data (AT1) of the waste bin are saved in the ID-Tag. There are only ID-Tags with unique identification data in use. The correct correspondence of this data to the chargeable person is to be provided by organisational means which are out of the scope of the TOE.

**A.Trusted** *Trustworthy personnel*

The crew of the collection vehicle and the user of the office computer (S.Trusted) are authorised and trustworthy. All persons who install and maintain the system are authorised and trustworthy (S.Trusted). All persons responsible for the security of the TOE environment (S.Trusted) are authorised and trustworthy.

**A.Access** *Access protection*

The environment ensures by appropriate means (closure, access control by passwords etc.) that only user or service staff (S.Trusted) can directly access the components of the TOE except the ID-Tag. The manipulation of the internal communication channels by potential attacker (S.Attack) within the IT - structure of the office computer is excluded by sufficient measures.

**A.Check** *Check of completeness*

The user (S.trusted) checks at regular intervals if the transported data from the vehicle software to the security module in office is complete. Identified loss of data will be recovered by repeated transport of data. The intervals are consistent with the capacity of the corresponding memory of the vehicle computer.

**A.Backup** *Data backup*

The user (S.Trusted) makes backup copies of the data created by the TOE at regular intervals.

## 3.2 Threats to Security

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. The threats address all assets.

**T.Man** *Manipulated identification data*

An attacker (S.Attack) manipulates the identification data (AT1) within an ID-Tag by means of e.g. mechanical impact, which corrupts the identification data (AT1) only in a purely random way.

**T.Jam#1** *Disturbed identification data*

An attacker (S.Attack) disturbs the transfer of the identification data (AT1) from the ID-Tag to the reader in vehicle by means of e.g. electromagnetic radiation, which corrupts the identification data (AT1) only in a purely random way.

**T.Create** *Invalid records of clearance*

An attacker (S.Attack) creates arbitrary clearance data blocks (AT+) and transmits them to the security module.

**T.Jam#2** *Corrupted record of clearance*

An attacker (S.Attack) corrupts records of clearance (AT) during processing and storage within the vehicle or disturbs the transfer of clearance data blocks (AT+) from the vehicle software to the security module by means of e.g. electromagnetic radiation, which corrupts the data of clearance data block (AT+) only in a purely random way.

*Application note 4:*

*It is not possible to describe the attack methods in more detail since they strongly depend on the implemented technology used for the data channel between the vehicle software and the security module.*

*Application note 5:*

*The author of the Security Target can include additional threats averted by the product.*

## 3.3 Organisational Security Policies

The following rule is stated for the TOE:

**P.Safe** *Fault tolerance*

The vehicle software part of the TOE shall ensure that the data of the clearance data blocks (AT+) is secured by a redundant saving of the data in a secondary memory in such a way that the transfer of the clearance data blocks (AT+) from the vehicle software to the security module is possible in a case that clearance data blocks (AT+) are lost in the primary memory of the vehicle software.

*Application Note 6:*

*The above required functionality refers only to the data stored in the vehicle software. This functionality shall at least be ensured till complete transfer to the security module and hence to the office software. It can be assumed that the protection of the data will be implemented by a backup in a secondary memory of the vehicle computer. The manufacturer can additionally specify a time frame for this data storage in the secondary memory, so during this time frame the data is available for a repeated transfer to the security module. This backup functionality does not protect against the loss of data in the office computer (refer also to A.Backup).*

# 4 Security Objectives

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

## 4.1 Security Objectives for the TOE

The security objectives for the TOE must determine (to the desired extent) the responsibility of the TOE in countering the threats and in supporting the OSPs. Each objective must be traced back to aspects of identified threats to be countered by the TOE and to aspects of OSPs to be met by the TOE. The security objectives may be viewed as providing the reader a link from the identified security needs to the security IT requirements.

**OT.Inv#1** *Recognition of invalid identification data*

The TOE shall recognise manipulation of identification data (AT1) stored in ID-Tag or during transfer between ID-Tag and the reader in vehicle.

*Application Note 7:*

*The security objectives require only the recognition of for example missing data in ID-Tag. The TOE can optionally react by itself to such recognised events. Since this will be not realised in general it is left to the author of the Security Target to define in addition security objectives for the reaction to such events.*

**OT.Inv#2** *Recognition of invalid clearance data blocks*

The TOE shall recognise any attempt to transfer arbitrary (i.e. invalid) clearance data blocks (AT+) to the security module. The TOE shall recognise manipulations of records of clearance (AT) during processing and storage within the vehicle and manipulations of the clearance data blocks (AT+) by random jam during transfer from the vehicle software to the security module.

**OT.Safe** *Fault tolerance*

The vehicle software as a part of the TOE shall ensure that the data of the clearance data blocks (AT+) is secured by a redundant saving of the data in a secondary memory in such a way that the transfer of the clearance data blocks (AT+) from the vehicle software to the security module is possible in a case that clearance data blocks (AT+) are lost in the primary memory of the vehicle software.

## 4.2 Security Objectives for the Environment

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

The ID-Tag is fastened to the waste bin. The identification data (AT1) of the waste bin are saved in the ID-Tag. There shall be only ID-Tags with unique identification data in use. The correct correspondence of this data to the chargeable person is to be provided by organisational means which are out of the scope of the TOE.

**OE.Trusted** *Trustworthy personnel*

It shall be ensured by organisational means that the crew of the collection vehicle and the user of the office computer (S.Trusted) are authorised and trustworthy. All persons which install and maintain the system shall be authorised and trustworthy (S.Trusted). All persons responsible for the security of the TOE environment (S.Trusted) shall be authorised and trustworthy.

**OE.Access** *Access protection*

The environment shall ensure by appropriate means (closure, access control by passwords etc.) that only user or service staff (S.Trusted) can directly access the components of the TOE except the ID-Tag. The manipulation of the internal communication channels by potential attackers (S.Attack) within the IT - structure of the office computer shall be excluded by sufficient measures.

**OE.Check** *Check of completeness*

It shall be ensured that the user (S.Trusted) checks at regular intervals if the transported data from the vehicle software to the security module in office is complete. The identified loss of data shall be recovered by repeated transport of data. The intervals shall be consistent with the capacity of the corresponding memory of the vehicle computer.

**OE.Backup** *Data backup*

It shall be ensured that the user (S.Trusted) makes backup copies of the data created by the TOE at regular intervals.

# 5 IT Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE and the environment.

Security functional requirements components are given in section 5.1 “TOE security functional requirements” are drawn from Common Criteria part 2 [2], except for the component FDP_ITT.5, which is defined in this Protection Profile. Operations for assignment, selection and refinement have been made. Operations not performed in this PP are identified in order to enable instantiation of the PP to a Security Target (ST).

The TOE security assurance requirements statement given in section 5.2 “TOE security assurance requirements” is drawn from the security assurance components from Common Criteria part 3 [3].

Section 5.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 5.4.

## 5.1 TOE Security Functional Requirements

### 5.1.1 Data authentication (FDP_DAU)

#### 5.1.1.1 Basic data authentication (FDP_DAU.1)

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *records of clearance AT and clearance data blocks AT+*[1].

FDP_DAU.1.2 The TSF shall provide *user (S.Trusted)*[2] with the ability to verify evidence of the validity of the indicated information.

*Application Note 8:*

It is considered that the above requirements can be fulfilled at the targeted assurance level of the evaluation without usage of secrets.

### 5.1.2 Internal TOE transfer (FDP_ITT)

#### 5.1.2.1 Internal transfer integrity (FDP_ITT.5) (Common Criteria Part 2 extended)

FDP_ITT.5.1 The TSF shall enforce the *Data Integrity Policy*[3] to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.

[1] assignment: *list of objects or information types*

[2] assignment: *list of subjects*

[3] assignment: *Integrity SFP(s)*

The following Security Function Policy (SFP) **Data Integrity Policy** is defined for the requirement “Basic internal transfer protection (FDP_ITT.5)”:

The User Data (AT1 and AT+) shall be protected in order to maintain its integrity.

### 5.1.3 Stored data integrity (FDP_SDI)

#### 5.1.3.1 Stored data integrity monitoring (FDP_SDI.1)

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for *random manipulation*[4] on all objects, based on the following attributes: *identification data AT1 within identification unit and records of clearance AT during storage within the vehicle*[5].

### 5.1.4 Fault tolerance (FRU_FLT)

#### 5.1.4.1 Degraded fault tolerance (FRU_FLT.1)

FRU_FLT.1.1 The TSF shall ensure the operation of *the transfer of clearance data blocks (AT+) from the vehicle software to the security module with the aid of the data stored in secondary memory*[6] when the following failures occur: *Loss of user data in the primary memory of the vehicle software*[7].

## 5.2 TOE Security Assurance Requirements

**Table 5.1 Assurance Requirements: EAL1**

| Assurance Class | Assurance Components |
|---|---|
| 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 | - |

### 5.2.1 Configuration management (ACM)

#### 5.2.1.1 Configuration items (ACM_CAP.1)

ACM_CAP.1.1D The developer shall provide a reference for the TOE.

ACM_CAP.1.1C The reference for the TOE shall be unique to each version of the

[4] assignment: *integrity errors*

[5] assignment: *user data attributes*

[6] assignment: *list of TOE capabilities*

[7] assignment: *list of type of failures*

TOE.

ACM_CAP.1.2C The TOE shall be labelled with its reference.

## 5.2.2 Delivery and operation (ADO)

### 5.2.2.1 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

## 5.2.3 Development (ADV)

### 5.2.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

### 5.2.3.2 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

## 5.2.4 Guidance Documents (AGD)

### 5.2.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

#### 5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

### 5.2.5 Tests (ATE)

#### 5.2.5.1 Independent testing conformance (ATE_IND.1)

ATE_IND.1.1D The developer shall provide the TOE for testing.

ATE_IND.1.1C The TOE shall be suitable for testing.

## 5.3 Security Requirements for the IT Environment

There are no security requirements imposed on the IT environment in this protection profile.

## 5.4 Security Requirements for the Non-IT Environment

**R.Id** *Identification unit*

The user must ensure the following: The identification unit should be fastened to the waste bin, which is to be identified by the identification data stored in the unit. The identification data stored in installed identification units is unique. The correspondence of the identification data to the chargeable person shall be performed by organisational means, which is not in the scope of the TOE.

**R.Trusted** *Trustworthy personnel*

The persons operating, installing and servicing the vehicle and the security module shall be authorised and trustworthy. All persons responsible for the security of the environment are authorised and trustworthy.

**R.Access** *Access protection*

The environment shall ensure by appropriate means that only the user and the service personnel have direct access to the components of the TOE (except for the identification unit). The environment shall prevent any means of influencing the internal data channels within the office computers.

**R.Check** *Check of completeness*

The user shall check in regular intervals the completeness of the transfer of the data of the clearance data blocks (AT+) from the vehicle to the office. The user shall request the transfer of the data which he determined not to have been transferred yet from the vehicle to the office in order to recover from this. The time intervals of the check and request user actions must be consistent with the available storage capacity provided by the vehicle computer for the purpose of the storage of clearance data blocks (AT+).

**R.Backup** *Data backup*

The user shall back up the data created by the TOE in regular intervals into appropriate archives.

# 6 Rationale

## 6.1 Introduction

The tables in sub-sections 6.2.1 “Security Objectives Coverage” and 6.3.1 “Security Requirement Coverage” provide the mapping of the security objectives and security requirements for the TOE.

## 6.2 Security Objectives Rationale

### 6.2.1 Security Objectives Coverage

**Table 6.1 Security Objectives Mapping**

| Threats - Assumptions - Policies / Security objectives | OT.Inv#1 | OT.Inv#2 | OT.Safe | OE.Id | OE.Trusted | OE.Access | OE.Check | OE.Backup |
|---|---|---|---|---|---|---|---|---|
| T.Man | x | | | | | | | |
| T.Jam#1 | x | | | | | | | |
| T.Create | | x | | | | | | |
| T.Jam#2 | | x | | | | | | |
| A.Id | | | | x | | | | |
| A.Trusted | | | | | x | | | |
| A.Access | | | | | | x | | |
| A.Check | | | | | | | x | |
| A.Backup | | | | | | | | x |
| P.Safe | | | x | | | | | |

### 6.2.2 Security Objectives Sufficiency

#### 6.2.2.1 Policies and Security Objective Sufficiency

**P.Safe (Fault tolerance)** establishes the availability of the relevant data for the transfer of the clearance data blocks (AT+) from the vehicle software to the security module also in case of the loss of these data in a primary memory of the vehicle software by keeping the data in a secondary memory. This is exactly repeated by the objective OT.Safe, so this objective is sufficient for P.Safe.

#### 6.2.2.2 Threats and Security Objective Sufficiency

**T.Man (Manipulated identification data)** deals with attacks in which identification data (AT1) is manipulated within the identification unit. According to OT.Inv#1 the identification data (AT1) which is corrupted (as seen after being read by the reader) will be recognised by the TOE which counters directly the threat T.Man.

**T.Jam#1 (Disturbed identification data)** deals with attacks in which disturbed identification data (AT1) (by random disturbance) is presented to the reader. According to OT.Inv#1 the identification data which is corrupted (as seen after the read by the reader) will be recognised

by the TOE which counters directly the threat T.Jam#1.

**T.Create (Invalid records of clearance)** deals with attacks in which arbitrary records of clearance are created and then transported to the security module. According to OT.Inv#2 any attempt to transport arbitrary (i.e. invalid) records of clearance blocks to the security module will be recognised which counters directly the threat T.Create.

**T.Jam#2 (Corrupted records of clearance)** addresses attacks in which records of clearance (AT) during processing and storage within the vehicle are corrupted or the transfer of the clearance data blocks to the security module is disturbed. According to OT.Inv#2 corruptions of the records of clearance during processing and storage within the vehicle and the clearance data blocks which are corrupted during transfer to security module will be recognised by the TOE which counters directly the threat T.Jam#2.

#### 6.2.2.3 Assumptions and Security Objective Sufficiency

**A.Id (Identification unit)** ensures that the identification unit is fastened to the waste bin which it identifies and the data of installed identification units is unique. The correspondence between the identification data and the chargeable customer is established by organisational means. Since the objective OE.Id states exactly the same, it is sufficient for A.Id.

**A.Trusted (Trustworthy personnel)** ensures that all subjects (except the attacker) are trustworthy. The objective OE.Trusted states exactly the same, so it is sufficient for A.Trusted.

**A.Access (Access protection)** ensures that the access to the TOE, except for the identification unit, is limited to trustworthy personnel only. It excludes also the ability of the attacker to influence the internal communication channels within the IT-structure of the office computer. The objective OE.Access states exactly the same, so it is sufficient for A.Access.

**A.Check (Check of completeness)** ensures that the user checks at regular intervals if the transported data from the vehicle to the office is complete. Identified loss of data will be recovered by repeated transport of data. The intervals are consistent with the capacity of the corresponding memory of the vehicle computer. The objective OE.Check states exactly the same, so it is sufficient for A.Check.

**A.Backup (Data backup)** ensures that the user makes backup copies of the data created by the TOE at regular intervals as the TOE does not provide a corresponding functionality. The objective OE.Backup states exactly the same, so it is sufficient for A.Backup.

# 6.3 Security Requirements Rationale

## 6.3.1 Security Requirement Coverage

**Table 6.2 Security Functional Requirement to TOE Security Objective Mapping**

| TOE Security Functional Requirement / TOE Security objectives | 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 |

**Table 6.3 Environment security requirement to Environment Security Objective Mapping**

| Environment Security Requirement / TOE Security objectives | OE.ID | OE.Trusted | OE.Access | OE.Check | OE.Backup |
|---|---|---|---|---|---|
| R.Id | x | | | | |
| R.Trusted | | x | | | |
| R.Access | | | x | | |
| R.Check | | | | x | |
| R.Backup | | | | | x |

## 6.3.2 Security Requirements Sufficiency

### 6.3.2.1 TOE Security Requirements Sufficiency and Mutual Support

**OT.Inv#1 (Recognition of disturbed identification data)** addresses the recognition of manipulation of identification data (AT1) of records of clearance (AT) within the identification unit and while being transferred between the identification unit and the vehicle software, which are separated parts of the TOE. The protection of the integrity of the identification data (AT1) which is stored in the identification unit is required by FDP_SDI.1 and counters directly random manipulations of this data. The protection of the User Data AT1 to ensure its integrity is required by FDP_ITT.5 for the transfer between physically-separated parts of the TOE. Ensuring the data integrity protects directly against manipulations of the data during the transfer.

**OT.Inv#2 (Recognition of invalid data blocks)** addresses the recognition of manipulation of data clearance blocks (AT+), which are transferred between the vehicle software and the

security module, which are physically separated parts of the TOE. The protection of the User Data AT+ to ensure its integrity is required by FDP_ITT.5 for the transfer between physically-separated parts of the TOE. Ensuring the data integrity protects directly against manipulations of the data. OT.Inv#2 addresses also the recognition of invalid records of clearance AT during processing and storage in the vehicle and manipulations of clearance data blocks AT+ transferred to the security module. The TOE provides according to FDP_DAU.1 a capability to create an evidence which can be used by the user to verify the validity of the data. The protection of the integrity of the user data (AT) which is stored in the vehicle is required by FDP_SDI.1 and counters directly random manipulations of this data. The requirements FDP_ITT.5, FDP_DAU.1 and FDP_SDI.1 are mutually supportive for the data authenticity and integrity. Therefore the requirements FDP_ITT.5, FDP_DAU.1 and FDP_SDI.1 cover sufficiently the security objective OT.Inv#2.

**OT.Safe (Fault tolerance)** addresses the availability of the relevant data for transfer of the clearance data blocks (AT+) from the vehicle software to the security module even in the case of data loss within the primary memory of the vehicle software. The operation of this data transfer with the aid of a secondary memory after the loss of the data in primary memory is realised by the TOE according to FRU_FLT.1.

#### 6.3.2.2 TOE Environment Security Requirements Sufficiency

**OE.Id (Identification unit)** is provided by R.Id, as R.Id requires what the objective OE.Id states.

**OE.Trusted (Trustworthy personnel)** is provided by R.Trusted, as R.Trusted requires what the objective OE.Trusted states.

**OE.Access (Access protection)** is provided by R.Access, as R.Access requires what the objective OE.Access states.

**OE.Check (Check of completeness)** is provided by R.Check, as R.Check requires what the objective OE.Id states.

**OE.Backup (Data Backup)** is provided by R.Backup, as R.Backup requires what the objective OE.Backup states.

## 6.4 Explicitly stated Security Requirements

It was chosen to define FDP_ITT.5 explicitly, because Part 2 of the Common Criteria do not contain a generic security functional requirement for integity protection of user data when it is transmitted between physically-separated parts of the TOE. Furthermore FDP_ITT.5 has a more narrowed approach than FDP_ITT.1, because it does not necessarily require that the TOE implements access control SFP and/or information flow control SFP, and it addresses only manipulations of data.

## 6.5 Dependency Rationale

The security assurance components are taken exactly as specified by EAL1. All dependencies are therefore completely fulfilled.

The functional requirements dependencies for the TOE and for the environment are not completely fulfilled. The following table gives an overview of the dependencies and shows how they are fulfilled.

**Table 6.4 Functional Requirements Dependencies**

| Requirement | Dependencies | Fulfilled |
|---|---|---|
| FDP_DAU.1 | no dependencies | implicitly |
| FDP_ITT.5 | no dependencies | implicitly |
| FDP_SDI.1 | no dependencies | implicitly |
| FRU_FLT.1 | FPT_FLS.1 | see discussion below |

FRU_FLT.1 requires the TOE to ensure the operation of the data transfer from the vehicle software to the security module even if the data is lost within the vehicle software. This requirement is driven to fulfil the organisational security policy, which relates more to the availability of the data then to the correct functionality of the software and does not relate to a secure state of the TOE in terms of the threats the TOE is countering. As the dependency component FPT_FLS.1 relates merely to such secure state of the TOE (i.e. the software) it is not applicable for the TOE.

## 6.6 Rationale for Assurance Level EAL1

The assurance level for this protection profile is EAL1. This EAL provides a meaningful increase in assurance over an unevaluated IT product or system by providing confidence in correct operation, while the threats to security are not viewed as serious, which relates directly to the rather low value of the TOE's assets. EAL1 provides independent assurance to support the contention that due care has been exercised with respect to the protection of information contained in records of clearance and that the TOE provides useful protection against identified threats as required by the customer. EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay. This enables the required flexibility in composing the system of modules taken from the current market, while keeping the associated costs for the evaluation at reasonable low level.

# References

[1] International Organization for Standardization, ISO/IEC 15408-1:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, 1999.

[2] International Organization for Standardization, *ISO/IEC 15408-2:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999.

[3] International Organization for Standardization, *ISO/IEC 15408-3:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999.

# 7 Appendix A - Acronyms

**BSI** Bundesamt für Sicherheit in der Informationstechnik

**CC** Common Criteria

**EAL** Evaluation Assurance Level

**EVG** Evaluierungsgegenstand (German translation of **TOE**)

**IT** Information Technology

**OSP** Organisational Security Policies

**PP** Protection Profile

**SF** Security Function

**SFP** Security Function Policy

**TOE** Target of Evaluation

**TSC** TSF Scope of Control

**TSF** TOE Security Functions

**WBIS** Waste Bin Identification System

# 8 Appendix B - German translations

## 8.1 PP-Identifzierung

| | |
|---|---|
| Titel: | Schutzprofil — Abfallbehälter-Identifikations-Systeme |
| Sponsor: | Bundesamt für Sicherheit in der Informationstechnik |
| Editors: | Cezary Glowacz, Dr. Burkhard Grimm<br>T-Systems GEI GmbH Business Unit ITC Security |
| CC Version: | 2.1 Final |
| Vertrauenswürdigkeitsstufe: | Die Mindestvertrauenswürdigkeitsstufe für dieses Schutzprofil ist EAL1. |
| Allgemeiner Status: | Entgültiger Version |
| Versionsnummer: | 1.0 |
| Registrierung: | Keine |
| Schlüsselbegriffe: | Abfallbehälter-Identifikation, Datenerfassung, Aufzeichnung der Leerung, Kommune |

## 8.2 Schutzprofilübersicht

Dieses Schutzprofil ist das Ergebnis der Zusammenarbeit von Vertretern aus Herstellung und Betrieb von Systemen für die Abfallwirtschaft.

Ziel dieses Schutzprofils ist es funktionale Anforderungen und Vertrauenswürdigkeits-anforderungen für Abfallbehälter-Identifikationssysteme (WBIS) zu spezifizieren, die den Evaluationsgegenstand (EVG) darstellen. Das Schutzprofil definiert die Sicherheitsanforderungen von WBIS für die Übertragung und Speicherung der aufgezeichneten Leerungsdaten. Der EVG kann zusätzliche Funktionen und Sicherheitsanforderungen umsetzen. Diese zusätzlichen Funktionen und Sicherheitsanforderungen sind nicht Gegenstand dieses Schutzprofils.

Abfall-Behälter-Identifikations-Systeme (WBIS) im Sinne dieses Dokuments sind Systeme, durch die Abfallbehälter mit einem ID-Tag (z.B. mit elektronischen 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 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 und nach Gewicht oder Menge abrechnen zu können. Es sind in Zukunft auch andere Verfahren denkbar und mit dem System einsetzbar.

In Deutschland sind in vielen Kommunen bereits derartige Systeme von unterschiedlichen Herstellern installiert. Einige Hersteller verfügen über unterschiedliche Sicherheitszertifikate nach ITSEC. Der kommunale Endanwender benötigt eine Sicherheit bezüglich der Vergleichbarkeit der Sicherheitszertifikate, die bei Ausschreibungen zu fordern sind. Von daher wurde die Forderung an das BSI getragen hier in Form eines Schutzprofils für eine Vergleichbarkeit konkurrierender Sicherheitszertifikate zu sorgen. Abgesehen von der Initiative seitens kommunaler Anwender für die Erstellung eines Schutzprofils kann das Schutzprofil auch im Bereich der Gebührenveranlagung im privaten und gewerblichen Bereich benutzt werden.

Abfall-Behälter-Identifikations-Systeme (WBIS) basieren auf der elektronischen Erfassung, Übertragung und Speicherung von Leerungsdaten (als Leistungsnachweise von den Entsorgungsunternehmen) 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 nur genau die tatsächlich durchgeführten Leerungen abgerechnet und dem richtigen Verursacher (hier Abfallbehälter) zugeordnet werden. In diesem System sind daher die für die Abrechnung relevanten Daten (Identifikationsdaten, Zeitstempel) vor Manipulation und Verlust zu schützen.

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

Nach Abschluss einer Leerungstour des Fahrzeuges werden alle gesammelten Daten in das Büro des Betriebshofes (kommunal oder privat) mit unterschiedlichen Medien (Datenträger, Kabel, drahtlos) übertragen, um dort in einem zentralen Datenbestand gespeichert zu werden. Von hieraus können diese Daten regelmäßig an Behörden oder kommunale Rechenzentren zur Abrechnung mit dem Bürger weitergeleitet werden.

## 8.3 EVG-Beschreibung

Das Abfallbehälter-Identifizierungsystem (WBIS) besteht aus folgenden Komponenten:

- ID-Tag mit den Identifizierungsdaten des Abfallbehälters
- Fahrzeug mit dem (ID-Tag-) Reader, Fahrzeugrechner und einem optionalem 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-Identifizierungsystem[8].

Das Abfallbehälter-Identifizierungsystem 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. Das ID-Tag speichert Identifizierungsdaten, die zur Identifizierung des Abfallbehälters herangezogen werden. Diese Daten sind einmalig und nicht vertraulich. Jedem Datensatz ist in der Regel ein Gebührenpflichtiger eindeutig zugeordnet. Die Identifizierungsdaten werden während (bzw. vor/nach) der Leerung eines Abfallbehälters durch den Reader ausgelesen. Die dabei möglichen Übertragungsfehler und eventuelle Manipulationen werden erkannt. Die

[8] Siehe Abbildung 1 im Abschnitt 2.

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

Ein oder mehrere Leerungsdatensätze werden zu einem Leerungsdatenblock zusammengefasst. Es können auf diese Weise alle Leerungsdatensätze einer Tour zu einem „Touren-Datenblock“ zusammengefasst werden.

Die Leerungsdatenblöcke werden über das Sicherheitsmodul 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 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 Funktionalität (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 Angriffpotential angenommen. Der Zugang zu der Fahrzeugsoftware und zum Sicherheitsmodul ist durch geeignete physikalische und organisatorische Maßnahmen nur autorisiertem Personal möglich. Dieser Schutz wird durch das Fahrzeug mit seinen Komponenten und durch das Büro mit dem Bürorechner realisiert.

## Abgrenzung des Evaluierungsgegenstandes

Der Evaluierungsgegenstand ist ein Produkt im Sinne der Common Criteria. Der Evaluierungs-gegenstand besteht aus dem ID-Tag, der Fahrzeugsoftware und dem Sicherheitsmodul. Alle anderen Komponenten (siehe auch Fig. 1) sind nicht Bestandteil des Evaluierungsgegenstands und gehören zu dessen Umgebung. Der Evaluierungsgegenstand hat eine externe Schnittstelle zu den Speichereinheiten auf dem Fahrzeugrechner, eine logische interne Schnittstelle zwischen dem ID-Tag und der Fahrzeugsoftware, eine logische interne Schnittstelle zwischen der Fahrzeugsoftware und dem Sicherheitsmodul, und eine externe Schnittstelle zwischen dem Sicherheitsmodul und der Bürosoftware. Die physischen Kanäle ID-Tag - Fahrzeugsoftware und Fahrzeugsoftware - Sicherheitsmodul sind nicht Bestandteil des Evaluierungsgegenstands. Nur die internen Schnittstellen werden in diesem Schutzprofil betrachtet. Weitere Schnittstellen, insbesondere die zu den kommunalen Abrechnungsstellen, sind nicht Bestandteil der Evaluierung. Die Bürosoftware ist auch kein Bestandteil des Evaluierungsgegenstandes. Der Autor der Sicherheitsvorgaben kann jedoch den Umfang der Sicherheitsfunktionalität erweitern.

## 8.4 EVG-Sicherheitsumgebung

Der folgende Abschnitt dient der Definition von Art und Umfang der Sicherheitsbedürfnisse, die der EVG adressiert. Daher enthält dieser Abschnitt (i) alle Annahmen an die Umgebung des EVG, (ii) die zu schützenden Werte, die bekannten Angreifer und die Bedrohungen, die sie für die Werte darstellen sowie (iii) 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.

*Application Note 1:*

*Der Leerungsdatensatz AT wird innerhalb der im Fahrzeug installierten Komponenten des TOE, wie z.B. im Fahrzeugrechner oder im Reader, gebildet. Die Identifikationsdaten AT1 sind im ID-Tag gespeichert und bilden für sich ein schutzwürdiges Objekt bis zum Zeitpunkt der Bildung des Datensatzes AT. Der Leerungsdatensatz AT kann optional weitere Datenfelder, wie z.B. Angaben zum Gewicht der Abfälle, enthalten.*

**AT+** Bei der Übertragung der Leerungsdatensätze AT vom 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.

*Anwendungshinweis 2:*

*Ein Leerungsdatenblock (AT+) kann die gesamten Leerungsdatensätze einer Tour zusammenfassen.*

### 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.

*Anwendungshinweis 3:*

*Die Daten des Leerungsdatensatzes (AT) bzw. des Leerunsgdatenblocks (AT+) können auf dem Übertragungsweg verfälscht werden durch rein zufällige Einflüsse. Solche Verfälschungen werden hier nicht als Bedrohungen angesehen, da hier kein Angreifer identifizierbar ist. Die Wirksamkeit ggfs. implementierter Funktionalität kann im Rahmen der funktionalen Tests (Typprüfung) nachgewiesen werden.*

### 8.4.1 Annahmen

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

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

**A.Trusted** *Vertrauenswürdiges Personal*

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

### 8.4.2 Bedrohungen

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

**T.Man** *Manipulierte Identifikationsdaten*

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

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

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

**T.Create** *Ungültige Leerungsdatensätze*

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

**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.

*Anwendungshinweis 4:*

*Es ist nicht weiter möglich, die Angriffmethoden genauer zu beschreiben, da diese stark von der verwendeten Technik, die zur Implementierung des Datenkanals zwischen der Fahrzeugsoftware und dem Sicherheitsmodul verwendet wird, abhängig sind.*

*Anwendungshinweis 5:*

*Der Autor der Sicherheitsvorgaben kann zusätzliche Bedrohungen aufnehmen, die das Produkt abwehrt.*

### 8.4.3 Organisatorische Sicherheitspolitik

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 zu schützen sind, dass die Übertragung der Leerungsdatenblöcke von der Fahrzeugsoftware zum Sicherheitsmodul nach einem Verlust der Daten in einem primären Speicher möglich ist.

*Anwendungshinweis 6:*

*Die oben geforderte Funktionalität bezieht sich ausschließlich auf die Daten in der Fahrzeugsoftware. Diese Funktionalität muss mindestens bis zur vollständigen Übertragung in das Sicherheitsmodul (und damit in die Bürosoftware) gewährleistet werden. Es ist zu erwarten, dass der Schutz der Daten durch eine Backup-Funktionalität (Datenhaltung in einem sekundären Speicher) in der Fahrzeugsoftware realisiert wird. In diesem Fall kann der Hersteller zusätzlich einen Zeitraum spezifizieren, in dem die Daten gesichert werden, und damit auch für eine wiederholte Übertragung zum Sicherheitsmodul verfügbar sind. Wie unter A.Backup dargelegt, schützt diese Backup-Funktionalität nicht vor Datenverlust im Archiv des Bürorechners.*

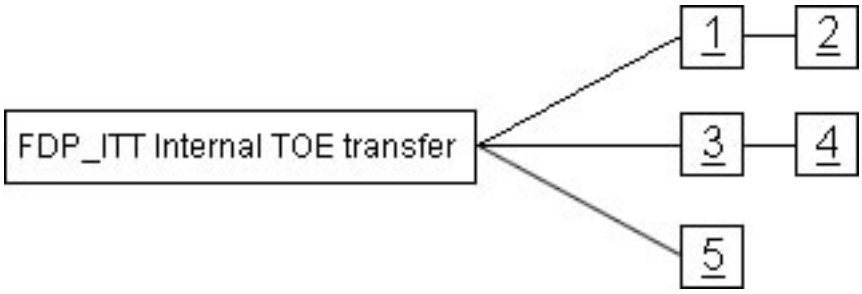
# 9 Appendix C - Definition of the Component FDP_ITT.5

To define the security functional requirements of the TOE an additional component (FDP_ITT.5) of the Family FDP_ITT (Internal TOE transfer) is defined here. This component describes the functional requirements for the integrity protection of data. It has a more narrowed approach than FDP_ITT.1, because it does not necessarily require that the TOE implements access control SFP and/or information flow control SFP, and it addresses only manipulations of data.

The family “Internal TOE transfer” (FDP_ITT)” is extended as follows (only changes are given here).

**FDP_ITT Internal TOE tranfer**

Component levelling




FDP_ITT.5 Internal transfer integrity protection requires user data to be protected against manipulations when transmitted between parts of the TOE.

**FDP_ITT.5** Internal transfer integrity protection

Hierarchical to: No other components.

FDP_ITT.5.1 The TSF shall enforce the [assignment: *integrity SFP(s)*] to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.

Dependencies: No dependencies