ALTARES S.R.L.
Via S. Andrea 53 – I 38062 ARCO (TN)
Tel. +39 0464 512085
Fax +39 0464 515532
info@altares.it - www.altares.it

Security Target

RFID Identification and Geolocation system for waste collection - Arco40 evo v. 1.0

ALTARES S.R.L.
Via S. Andrea 53 – I 38062 ARCO (TN)
Tel. +39 0464 512085
Fax +39 0464 515532
info@altares.it - www.altares.it

DOCUMENT VERSIONS

Version	Date	Author	Amendments
1.0	06/16/2017	Adriano Coldebella	First issue
1.1	07/17/2017	Adriano Coldebella	Conformance claim has been reviewed
1.2	09/14/2017	Adriano Coldebella	Document version has been reviewed
1.3	10/05/2017	Adriano Coldebella	Conformance claim has been reviewed
1.4	14/12/2017	Adriano Coldebella	Minor document revision and bug fix

Table 1 – Document version

Summary

Index Images

Index tables

0 Document Introduction

0.1 Document structure

The Security Target contains the following additional sections:

- **Security Target Introduction** [Rif. §1]: this section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- **Conformance claim** [Rif. §2]: this section states the Conformance Claims to Common Criteria.
- **Security problem definition** [Rif. §3]: this section details asset, threats that are countered by the TOE and the environment, the organizational policy that the TOE must fulfill and the assumptions.
- **Security objectives** [Rif. §4]: this section details the security objectives of the TOE and of his environment.
- **Extended Components Definition** [Rif. §5]: this section defines the extended component utilized in this ST.
- **Security requirements:** [Rif. §6]: this section presents the security functional requirements (SFR) for the TOE, and details the assurance requirements (SAR).
- **TOE summary specification** [Rif. §7]: this section describes the security functions represented in the TOE that satisfy the security requirements.

0.2 Acronyms

Acronym	Description
CC	Common Criteria
EAL	Evaluation Assurance Level
GPRS	General Packet Radio Service
GPS	Global Positioning System
IT	Information Technology
PP	Protection Profile
RFID	Radio Frequency IDentification
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
WBIS	Waste Bin Identification Systems

Table 2 - Acronyms

0.3 Definitions

Terms	Definition
WASTE BIN	Is the container used by house holders to put their own waste. Include: bags, bins and wheelie bins with **ID-TAG**
ID-TAG	A rfid (radio-frequency identification) chip installed on a **WASTE BIN** for its unique identification.
READER	Device connected with Vehicle computer (by wire or wireless) used for decode and transmit to vehicle software the information stored on a **ID-TAG**
VEHICLE SOFTWARE	Software installed on vehicle computer distributed with each Arco40Evo device
CLEARANCE DATA MANAGEMENT MODULE	Part of vehicle software responsible of composition, secure storage and transmission of **CLEARANCE DATA RECORD**
CLEARANCE DATA RECORD	Data structure represented a **WASTE BIN** clearance
SECURITY MODULE	Is a part of Server side software that receive information (as **CLEARANCE DATA RECORDS**) from Arco40Evo device
APPLICATION SERVER	Is the server that contain the security module application

Table 3 - Definitions

0.4 Reference

[RIF.1] WBISPP104 - Protection Profile Waste Bin Identification Systems WBIS-PP Version 1.04 BSI-PP-0010-2004

[RIF.2] Common Criteria for Information Technology Security Evaluation. Part 1-3, April 2017, Version 3.1 Revision 5.

1 Security Target introduction (ASE_INT)

1.1 Security Target reference

Title: Security Target for "Identification and Geolocation system for waste collection Arco40 evo v.1.0" ver. 1.4

Date: 14/12/2017

Author: Adriano Coldebella

1.2 TOE reference

Product name: **Arco40 evo v. 1.0**

Developer: Altares s.r.l.

1.3 TOE overview

1.3.1 Usage and major security features of a TOE

The TOE allows to identify waste bins (or other urban furniture) 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, washed, etc.... Note that this type of systems 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.

The TOE allows certifying that the flow of data from the RFID tag to the Vehicle Software and to the Application server is secure during its whole process.

In a general way, the described process is applicable to every urban furniture and action performed.

A 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 **WASTE BIN** is 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 (or business company or organisation) 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. The vehicle software supplements these data by adding:

- Date and time of **ID-TAG** reading (obtained from vehicle computer clock synchronized with GPS receiver);
- GPS position of the vehicle during **ID-TAG** reading;
- Vehicle ID unique identifier;
- Clearance identification number (a counter of valid readings done for the vehicle ID);

and then forms a CLEARANCE DATA RECORD from all these data.

The records are transmitted by the **CLEARANCE DATA MANAGEMENT MODULE** to the **SECURITY MODULE** in the application Server. The **CLEARANCE DATA MANAGEMENT MODULE** 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 possible malfunctions during transfer are detected and the failed records are retransmitted until the transmission succeeds.

The clearance records 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 record etc.) aside from the billing functionality to supplement the security functionality of the TOE.

1.3.2 TOE type

The **RFID Identification and Geolocation system for waste collection - Arco40 evo v. 1.0** is a "Waste Bin Identification System (WBIS)" as defined in the WBIS-PP. WBIS are systems which allow the identification of clearance **WASTE-BIN** with **ID-TAG**, in order to determine how often a specific **WASTE BIN** has been cleared.

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.

1.3.3 Required not-TOE hardware/software/firmware

The TOE is a product that follows the common criteria WBIS-PP. The TOE consists as an **ID-TAG**, the **CLEARANCE DATA MODULE** in vehicle software, and **SECURITY MODULE** in APPLICATION SERVER. All other components are not part of the TOE but of the TOE environment.

The following table describes whole non-TOE system components. See figure 2 for further details.

Name	type	Version	Description
READER	Hw	various	Device that reads and decode an ID-TAG
SOLARIS	Hw	1.0	Arco40Evo main board based on Arm A5 processor
SOLARIS kernel	Sw	1.0	Altares operating system kernel based on linux 4.4.x
SOLARIS bsp	Sw	1.0	Solaris board support package. It Integrates all device drivers for Solaris board, mosquitto broker for data communication and bootloader.
EVOWD	SW	1.0	EVO watch dog application
EVOUI	SW	1.0	EVO user interface manager
Evo.json	Config	1.0	Configuration file for the EVOFSM
EVOFSM	SW	1.0	EVO Finite State Machine. Is the main application program in vehicle computer

Table 4 – Required not-TOE components

1.4 TOE description

Waste bin identification systems (WBIS) consist of the following components:

- **ID-TAG** containing the identification data of the **WASTE-BIN**
- Vehicle with **READER**, vehicle computer with GPS/GPRS and optional sensors. The vehicle software is installed on the vehicle computer and the **CLEARANCE DATA MANAGEMENT MODULE** is a part of it.
- **APPLICATION SERVER** in the Data center. The security module is installed on the application server.

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

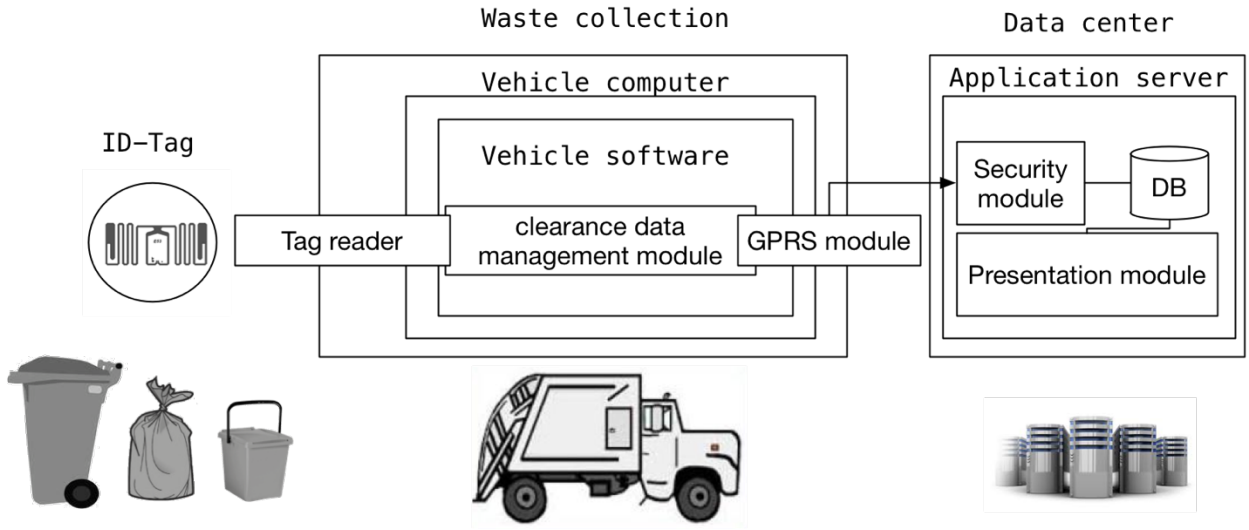

Figure 1 - Waste Bin Identification System

A 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. Also, in phase the reading the tag, the system provides the possibility of assigning "anomalies", for example: wrong conferment, broken bin, etc

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 by the **READER** 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. The vehicle software supplements these data by adding:

- Date and time of **ID-TAG** reading (obtained from vehicle computer clock synchronized with GPS receiver);
- GPS position of the vehicle during **ID-TAG** reading;
- Vehicle ID unique identifier;
- Clearance identification number (a counter of valid readings done for the vehicle ID);

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

Each **CLEARANCE DATA RECORD** is transmitted by the **CLEARANCE DATA MANAGEMENT MODULE** to the application Server and received by **SECURITY MODULE**. The **CLEARANCE DATA MANAGEMENT MODULE** 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 record to the Application server only those data records which were created in a clearance vehicle are accepted as valid data. In addition, possible malfunctions during transfer are detected.

The clearance data records can be stored on a server computer by the application server software. Optionally the data records can be analyzed further in order to defeat additional possible attacks (invalid, copied identification data, etc.). The clearance records contained in the application server can export 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 records 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 authorized personnel has access to the vehicle software and the security module due to suitable physical and organizational measures. This protection is implemented by the vehicle with its components and in the Data center with the server computer.

1.4.1 Limits of the TOE

The TOE consists of an **ID-TAG**, the **CLEARANCE DATA MANAGEMENT MODULE** included in 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 server 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. Additional interfaces, especially to the accounting centers, are not part of the evaluation. The DB and the Presentation module in application software are also not part of the TOE.

1.4.2 Physical scope

Figure 2 shows the physical scope of the TOE.

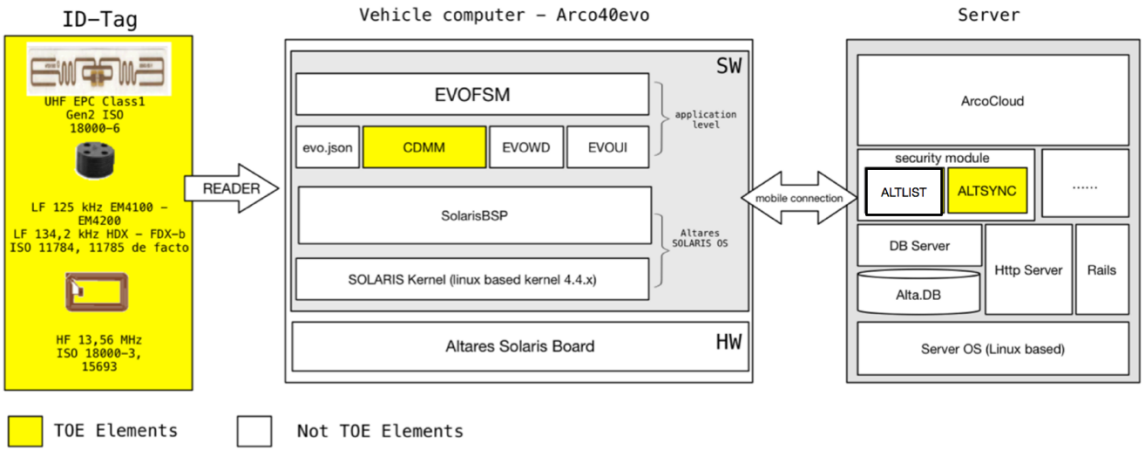

Figure 2 – TOE's physical scope

The physical RFID tag can be one of the following:

- UHF EPC Class 1 Gen2 ISO 18000-6;
- HF 13,56 MHz ISO 18000-3, 15693;
- LF 125 kHz (EM4100, EM4200) or LF 124,2 kHz (HDX, FDX b) ISO 11784, 11785;

Each kind of RFID tag requires a specific **READER**. The vehicle computer is based on Altares Solaris Board designed and produced by Altares srl who provides also the operating system based on linux kernel 4.4.x and the BSP (board support package). The BSP level, named SolarisBSP, integrates the device drivers and the software ALTSND used for guarantee a secure communication layer between vehicle computer and remote

server. The CDMM application in the application level implements the **CLEARANCE DATA MANAGEMENT MODULE**.

At the server side, the security module is realized by two daemons (a daemon is a type of program on Unix-like operating systems that runs unobtrusively in the background, rather than under the direct control of a user, waiting to be activated by the occurance of a specific event or condition):

- ALTLIST that implements the security level in communication (QoS 1);
- ALTSYNC that provide the synchronization between data received and the application central database

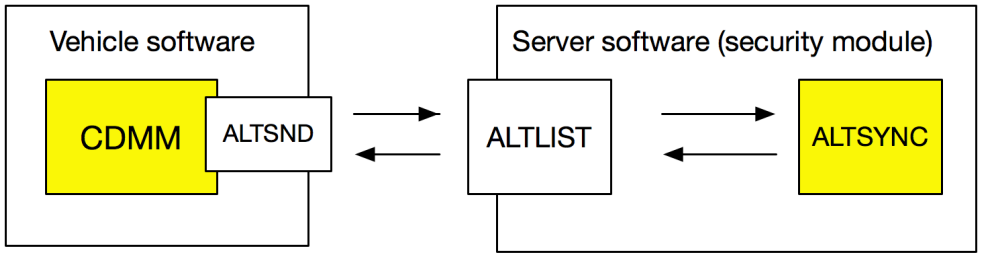

Figure 3 – Message structure

1.4.3 Logical scope

This ST is strictly conformant with [WBISPP104] as shows at figure 1 and therefore its logical scope is fully applicable. (TOE scope marked yellow).

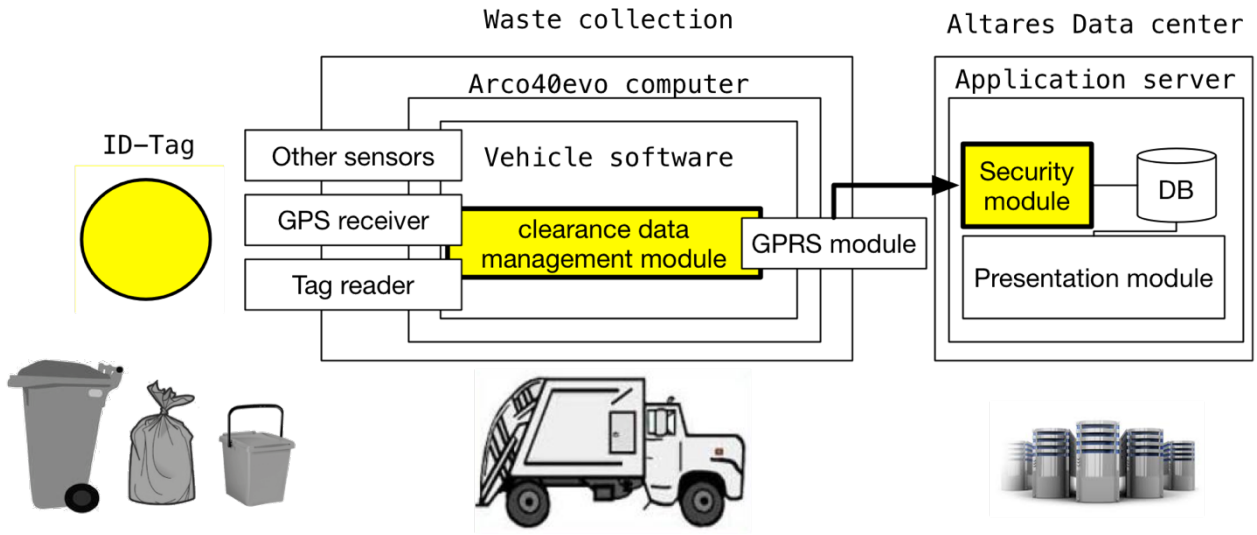

Figure 4 – TOE's logical scope

The previous logical scope is instantiated for the actual TOE as shown in the figure 2 (TOE scope marked yellow):

The main security features available are the following:

- Recognition of invalid identification data: The TOE will recognize manipulation of identification data (AT1) stored in **ID-TAG** or during transfer between **ID-TAG** and the **READER** in vehicle.

- Recognition of invalid clearance data records: The TOE will recognize any attempt to transfer arbitrary (i.e. invalid) clearance data records (AT+) to the security module. The TOE will recognize manipulations of clearance record (AT) during processing and storage within the vehicle and manipulations of the clearance data records (AT+) by random jam during transfer from the vehicle software to the security module.
- Fault tolerance: The vehicle software as a part of the TOE will ensure that the data of the clearance data records (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 records (AT+) from the vehicle software to the security module is possible in a case that clearance data records (AT+) are lost in the primary memory of the vehicle software.
- Automatic retransmission: The TOE will identify if data has not been adequately received by the security module and it will recover repeating data transmission.

2 CONFORMANCE CLAIM (ASE_CCL)

2.1 CC conformance claim

ST and TOE are conformant to version 3.1 (Revision 5) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- Common Criteria for Information Technology Security Evaluation. Version 3.1 Rev.5 Part 1 april 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 5 april 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 5 april 2017

2.2 PP claim

This Security Target is strictly conformant with the Protection Profile Waste Bin Identification Systems WBIS-PP Version 1.04 BSI-PP-0010-2004.

2.3 Package claim

The claimed assurance package is EAL1, augmented with ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2. These augmentation are necessary for the conformance to PP, that is certified against version 2.1 of CC.

2.4 Conformance rationale

The following rationales are provided:

The TOE Type in the ST is the same as the TOE type in the referenced PP, that is, a waste bin identification system.

Although [WBISPP104] was certified against Common Criteria 2.1, this ST claims conformance with Common Criteria version 3.1 R5, which provides the same or greater guarantees.

The Security Problem Definition in the ST is strictly conformant with the Security Problem Definition in the PP, because:

- the threats in the ST are identical to the threats in the PP
- the assumptions in the ST are identical to the assumptions in the PP
- the OSPs in the ST are identical to the OSPs in the PP.

The Security Objectives for the TOE in the ST are identical to the Security Objectives in the PP.

The Security Objectives for the operational environment in the ST are identical to the Security Objectives in the PP.

The Security Requirements are the same stated in the PP.

Moreover, as the assurance level of PP contains different requirements from those provided from the current version of Common Criteria, we have chosen an EAL1 assurance level augmented with ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2, which allows verification that the security problem is really addressed by the TOE and its operational environment.

3 Security Problem Definition (ASE_SPD)

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 any assumptions that are made regarding the TOE environment, the assets requiring protection, the identified threat agents and the threats they pose to the assets, and organizational 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.

3.1 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 Date and time of the clearance.
- AT3 GPS position.
- AT4 Vehicle ID
- AT5 Clearance ID (counter) for the vehicle
- AT6 Additional information

The record of clearance AT will be created within the vehicle computer. 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. AT2 is retrieved from the internal clock of the vehicle computer synchronized with GPS global time. AT3 is retrieved from the GPS subsystem and AT4 are retrieved from internal configuration file (evo.json). AT5 is a clearance index stored in the secure/non volatile memory of the Solaris board and updated at each new clearance. AT6 is retrieved from sensors subsystem and contains additional information about clearance.

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.

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.

3.2 Threats

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 records (AT+) from the vehicle software to the security module by means of e.g. electromagnetic radiation, which corrupts the data of clearance data records (AT+) only in a purely random way.

3.3 Organizational 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 records (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 records (AT+) from the vehicle software to the security module is possible in a case that clearance data records (AT+) are lost in the primary memory of the vehicle software.

3.4 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 server 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.

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.

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

The TOE shall recognise any attempt to transfer arbitrary (i.e. invalid) clearance data records (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 records (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 records (AT+) from the vehicle software to the security module is possible in a case that clearance data records (AT+) are lost in the primary memory of the vehicle software.

4.2 Security Objectives for the operational 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-TAG**s 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.

4.3 Security objectives rationale

4.3.1 Security objectives coverage

The following table provides a mapping of security objectives to the environment defined by the threats, policies and assumptions, illustrating that each security objective covers at least one threat and that each threat is countered by at least one objective, assumption or policy.

	TOE			Environment				
	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						
P.Safe			X					
A.Check							X	
A.Id				X				
A.Trusted					X			
A.Access						X		
A.Backup								X

Table 5 - Security Objectives Mapping

4.3.2 Security objectives sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat.

4.3.2.1 Threats and Security Objectives 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.

4.3.2.2 Policies and Security Objectives Sufficiency

P.Safe **(Fault tolerance)**

establishes the availability of the relevant data for the transfer of the clearance data records (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.

4.3.2.3 Assumptions and Security Objectives 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 every clearance data record sent by a vehicle is correctly received in the right sequence and ask to vehicle software in case of a gap. This is exactly repeated by the objective OE.Check, so this objective 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.

5 Extended component definition

The extended components used are those that are defined in the [WBISPP104] Protection Profile claimed in this Security Target. These components are used methodologically as they are defined in the PP.

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 integrity 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 Security Requirements

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

Assignment: The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows **[assignment]**.

Refinement : The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for additions, and strike-through, for deletions.

6.1 Extended Component Definition

The extended components used are those that are defined in the [WBISPP104] Protection Profile claimed in this Security Target. These components are used methodologically as they are defined in the PP.

FDP_ITT.5 Internal transfer integrity protection

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_ITT.5.1

The TSF shall enforce the [**integrity SFP**] to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.

6.2 Security Functional Requirements

6.2.1 Data authentication (FDP_DAU)

6.2.1.1 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 records AT+**]

FDP_DAU.1.2

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

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

6.2.2 Internal TOE transfer (FDP_ITT)

6.2.2.1 Internal transfer integrity protection (FDP_ITT.5) (Common Criteria Part 2 extended)

FDP_ITT.5.1

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

NOTE: The following Security Function Policy (SFP) Data Integrity Policy is defined for the requirement "Internal transfer integrity protection (FDP_ITT.5)": The User Data (AT1 and AT+) shall be protected in order to maintain its integrity.

6.2.3 Stored data integrity (FDP_SDI)

6.2.3.1 Stored data integrity monitoring (FDP_SDI.1)

FDP_SDI.1.1

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

6.2.4 Fault tolerance (FRU_FLT)

6.2.4.1 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**] when the following failures occur: [**Loss of user data in the primary memory of the vehicle software**].

6.2.5 Dependancy Analysis

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.

Functional Requirements	CC Required Dependencies	Satisfied Dependences
FDP_DAU.1	no request	fulfilled
FDP_ITT.5	no request	fulfilled
FDP_SDI.1	no request	fulfilled
FRU_FLT.1	FPT_FLS.1	See note 1

Table 6 – Dependencies of the functional requirements

NOTA 1 - **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.

6.3 Security Assurance Requirements

The security assurance requirements are those corresponding to EAL1 components as described in Common Criteria 3.1R5 Part 3, augmented with ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2.

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Stated security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 7 - Security Assurance Requirements (SAR)

ADV_FSP.1 Basic functional specification		
Dependencies:	None	
Developer action elements:	ADV_FSP.1.1D ADV_FSP.1.2D	The developer shall provide a functional specification. The developer shall provide a tracing from the functional specification to the SFRs.
AGD_OPE.1 Operational user guidance		
Dependencies:	ADV_FSP.1	Basic functional specification
Developer action elements:	AGD_OPE.1.1D	The developer shall provide operational user guidance.
AGD_PRE.1 Preparative procedures		
Dependencies:	None	
Developer action elements:	AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
ALC_CMC.1 Labeling of the TOE		
Dependencies:	ALC_CMS.1	TOE CM coverage
Developer action elements:	ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMS.1 TOE CM coverage		
Dependencies:	None	
Developer action elements:	ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
ASE_INT.1 ST introduction		
Dependencies:	None	

Developer action elements:	ASE_INT.1.1D	The developer shall provide an ST introduction.
ASE_CCL.1 Conformance claims		
Dependencies:	ASE_INT.1 ASE_ECD.1 ASE_REQ.1	ST introduction Extended components definition Stated security requirements
Developer action elements	ASE_CCL.1.1D ASE_CCL.1.2D	The developer shall provide a conformance claim. The developer shall provide a conformance claim rationale.
ASE_OBJ.2 Security objectives		
Dependencies:	ASE_SPD.1	Security problem definition
Developer action elements	ASE_OBJ.2.1D ASE_OBJ.2.2D	The developer shall provide a statement of security objectives. The developer shall provide a security objectives rationale.
ASE_ECD.1 Extended components definition		
Dependencies:	None	
Developer action elements	ASE_ECD.1.1D ASE_ECD.1.2D	The developer shall provide a statement of security requirements. The developer shall provide an extended components definition.
ASE_REQ.2 Derived security requirements		
Dependencies:	ASE_ECD.1 ASE_OBJ.2	Extended components definition Security objectives
Developer action elements:	ASE_REQ.2.1D ASE_REQ.2.2D	The developer shall provide a statement of security requirements. The developer shall provide a security requirements rationale.
ASE_SPD.1 Security Problem Definition		
Dependencies:	None	
Developer action elements:	ASE_SPD.1.1D	The developer shall provide a security problem definition.
ASE_TSS.1 TOE summary specification		
Dependencies:	ASE_INT.1 ASE_REQ.1 ADV_FSP.1	ST introduction Stated security requirements Basic functional specification
Developer action elements:	ASE_TSS.1.1D	The developer shall provide a TOE summary specification.
ATE_IND.1 Independent testing – conformance		
Dependencies:	ADV_FSP.1 AGD_OPE.1 AGD_PRE.1	Basic functional specification Operational user guidance Preparative procedures
Developer action elements:	ATE_IND.1.1D	The developer shall provide the TOE for testing.
AVA_VAN.1 Vulnerability survey		
Dependencies:	ADV_FSP.1 AGD_OPE.1 AGD_PRE.1	Basic functional specification Operational user guidance Preparative procedures
Developer action elements:	AVA_VAN.1.1D	The developer shall provide the TOE for testing.

6.3.1 Security Assurance Requirements Rationale

The assurance level for this security target 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. The ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2 augmentation allows verification that the security problem is really addressed by the TOE and its operational environment.

6.4 Security requirements rationale

6.4.1 Security Requirement Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

	OT.INV#1	OT.INV#2	OT.Safe
FDP_DAU.1		**X**	
FDP_ITT.5	**X**	**X**	
FDP_SDI.1	**X**	**X**	
FRU_FLT.1			X

Table 8 - Security Functional Requirement to TOE Security Objective Mapping

6.4.2 Security Requirements Sufficiency

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.

7 TOE Summary Specification

This section describes how the TOE meets each SFR providing, for each SFR from the statement of security requirements, a description of how the SFR is met, providing potential consumers of the TOE with a high-level view of how each SFR is satisfied.

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.

The objective is performed with SFR **FDP_ITT.5** e **FDP_SDI.1**

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.

The objective is performed with SFR **FDP_ITT.5**, **FDP_SDI.1** e **FDP_ DAU.1**

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.

The objective is performed with **SFR FRU_FLT.1**.

FDP_DAU.1 **Basic data authentication**

This SFR requires the TOE to provide a capability to generate evidence that can be used as a guarantee of the validity of the records. This is satisfied with the implementation of a secure mechanism over each stored record. This secure mechanism is generated by the TOE in the e vehicle software. Another secure mechanism is used for communication sent to the security module along with the rest of the record. This data is finally saved in the database.

FDP_ITT.5 **Internal transfer integrity protection**

This SFR requires the TOE to protect the integrity of AT1 and AT during transmission between physically separated parts of the TOE.

The implementation of this requirement has two different parts:

Protection of the integrity of AT1 during transmission from the ID Tag to the vehicle software: This is achieved providing a checksum inside AT1 itself, which is verified by the vehicle software.

Protection of the integrity of AT during transmission from the vehicle software to the security module: As stated in the previous SFR, a checksum is also generated by the vehicle software over the contents of AT and is transmitted for verification to the security module in the office software.

FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.1 requires the TSF to monitor the data stored for random manipulation. This requirement also has two different parts:

Monitoring of AT1 integrity within identification unit: as stated in the summary specification of FDP_ITT.5 this is achieved with the verification of the checksum in AT1 performed by the vehicle software.

Monitoring of AT integrity during storage within the vehicle: when a record is created it is automatically saved to the secondary storage along with its checksum. When the record is recovered for transmission to the security module, this checksum is also recovered and verified before sending to the security module.

FRU_FLT.1 Degraded fault tolerance

This requirement requires the TOE to ensure that each data block is transferred to the security module even in case of loss of user data from the primary memory. This is achieved saving each data block in secondary memory (flash/sd) after reading it.