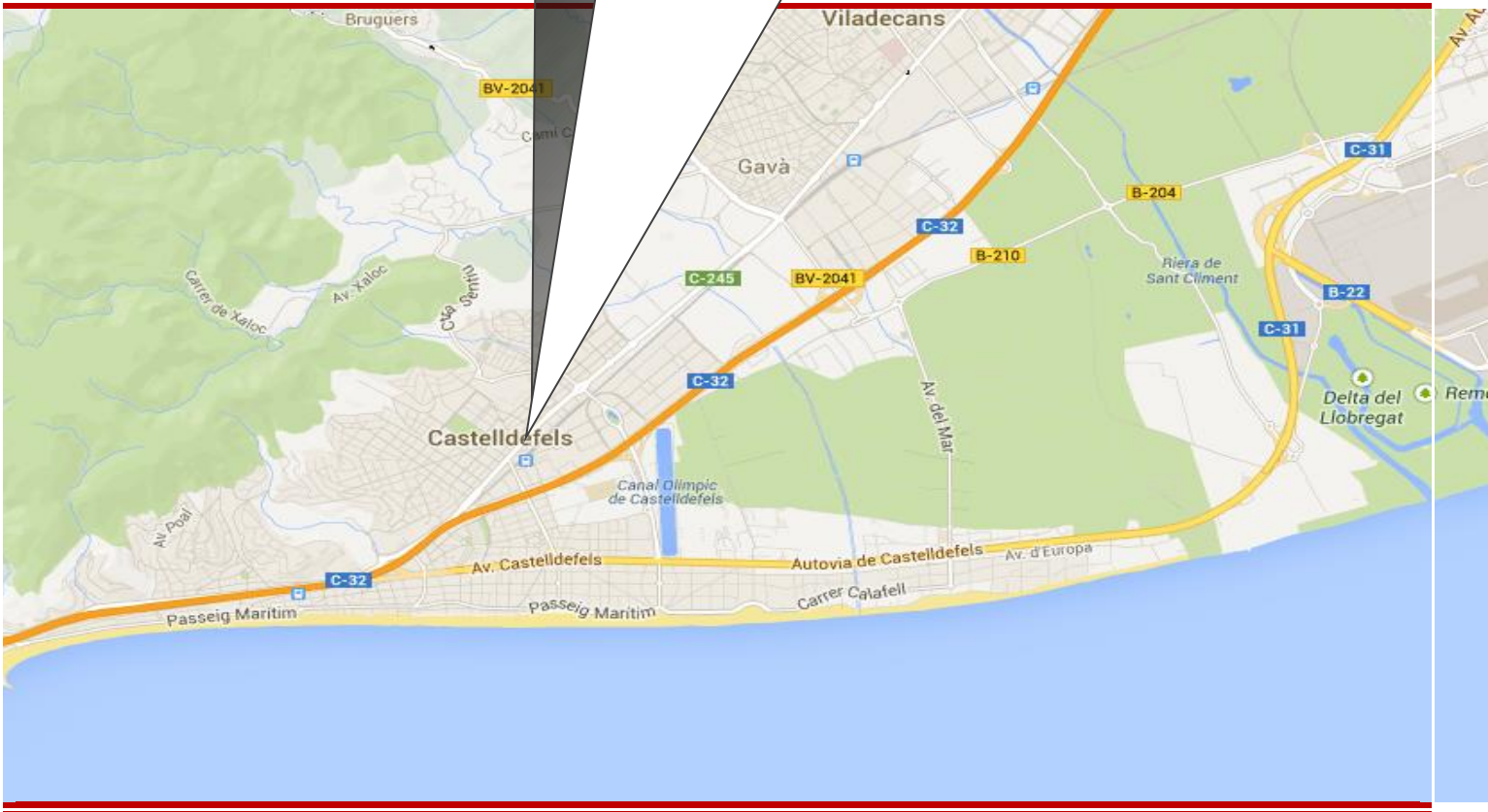
Security Target v1.0

Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors

boreal IT



Contents

1. Introduction

1.1. ST Reference

Title	Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors Security Target
Version	v1.0
Author	Javier Tallón (http://www.jtsec.es)
Publication date (dd/mm/yyyy)	06/02/2014

1.2. TOE Reference

TOE Name	Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors
TOE Version	v1.0
TOE Developer	Boreal Information Technology

1.3. TOE Overview

In this solution, every urban furniture, including waste bins, can have a passive RFID tag that uniquely identifies them. Vehicles include a radio-frequency sensor able to read the RFID tag identification, and it also includes a magnetic proximity sensor to detect the truck arms movement.

Both elements, the RFID tag and the radio-frequency sensor, get together in the vehicle during the process of collecting, the reader reads the tag that contains the waste bin, and the proximity sensor is excited by truck arms that handle up and down the waste bin during collection, washing and any similar action to be performed on the urban furniture.

In the truck cab, a controller named igMobile is installed. igMobile is a device that incorporates a GPRS modem, GPS and other digital and analog inputs and outputs.

The information collected during that operation is send through the Internet GPRS connection to a server in the office/cloud, where data is further exploited, saved and analyzed.

TOE Usage

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 Office 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 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. The vehicle software supplements these data by adding a date and time information and then forms a record of clearance from all these data.

The records 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 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 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 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 the office with the office computer.

TOE Type

The TOE is a waste bin identification system.

Non-TOE hardware and Software

The TOE is a product for the purpose of the Common Criteria. The TOE consists of an ID-Tag, the vehicle software (**igMobile.jar/igMobile.jad**) and the security module (**listen.php**). All other components (see logical scope) are not part of the TOE but of the TOE environment. The TOE has an external interface to the memories of the vehicle computer (igMobile), 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 ST. Additional interfaces, especially to the accounting centres of the town councils, are not part of the evaluation. The office software (igRouter except its security module and InfoGEO) are also not part of the TOE.

The proximity and other hardware sensors are not part of the TOE, but the data collected through those interfaces after being processed by the Vehicle Software are subject to the same requirements as the RFID Tag data.

The TOE needs the following additional hardware / software to work:

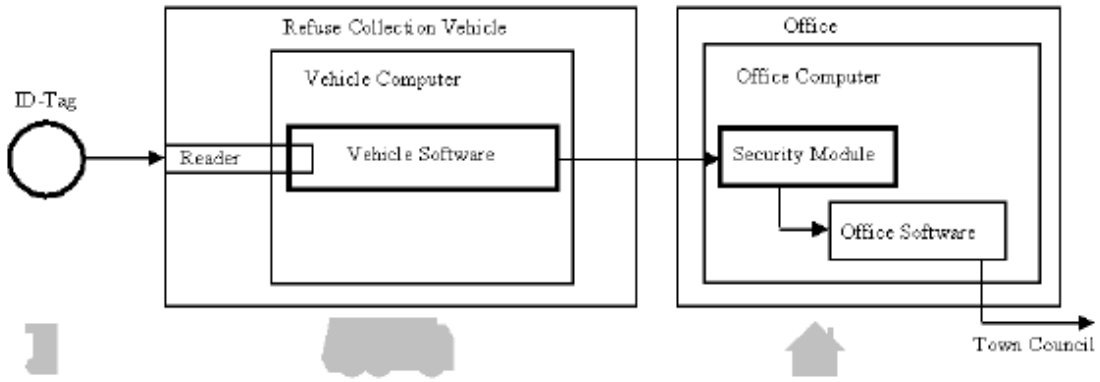
Name	Type	Description
RFID Reader	Hardware	RFID readers read the data stored in the tag when it is at less than 30 cm and send this data to igMobile.
Vehicle Computer	Hardware	The microcontroller solution that runs the vehicle software TOE (igmobile.jar + igmobile.jad)
Connection box	Hardware	Sealed connection boxes allow interconnection of devices installed in the vehicle
Proximity sensor	Hardware	Sensor detecting the truck arms movement in relation to the metallic structure of the bin.
GPS	Hardware	The vehicle computer includes a GPS sensor to known its current position.
Office Computer	Hardware	A general purpose computer running the Security Module TOE (listen.php) and its software environment.
DBASE	Database	The database storing the data collected by the TOE.

InfoGEO & igRouter	Software	Software used to exploit the data collected.
Office Software	Software	The Operating System and additional software needed to execute the TOE and its software environment.

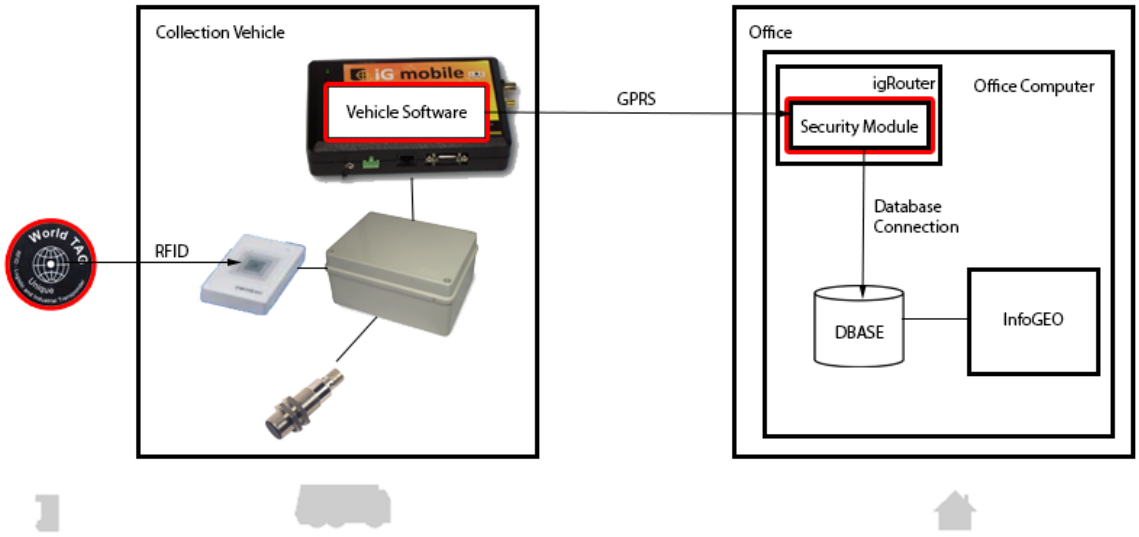
1.4. TOE Description

Logical Scope

This ST is strictly conformant with [WBISPP104] and therefore its logical scope is fully applicable. (TOE scope marked bold).



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



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 blocks: The TOE will recognize any attempt to transfer arbitrary (i.e. invalid) clearance data blocks (AT+) to the security module. The TOE will recognize 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.

- Fault tolerance: The vehicle software as a part of the TOE will 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.

- Automatic retransmission: The TOE will identify if data has not been adequately received by the security module and it will recover repeating data transmission.

Physical Scope

Distributed Name	Type	Description
igmobile.jar	Software	The **vehicle software** that runs in the microcontroller
igmobile.jad	Config	Configuration file for the vehicle software.
listen.php	Software	The software **security module** that runs in the Office and is part of igRouter
World Tag UNIQUE H4002	Hardware	The RFID **ID-Tag**
Preparative Guidance v1.0	Document	The manual used to install the TOE and prepare the operational environment.
Operational Guidance v1.0	Document	The manual used to operate the TOE.
Functional Specification v1.0	Document	The functional specification describing TOE interfaces.

Boreal IT delivers and installs the TOE described in this physical scope. It is packaged in a box containing the RFID tags, the igMobile hardware with the evaluated software installed and storage media with the security module software and the documentation.

2. Conformance Claims

This Security Target and the TOE it describes are fully compliant with Common Criteria 3.1R4.

This Security Target claims conformance with the following Common Criteria parts:

- [CC] Part 2 extended.
- [CC] Part 3 conformant.

The methodology to be used for the evaluation is described in the "Evaluation methodology" of the Common Criteria Standard. September 2012, Version 3.1. Revision 4.

This Security Target is strictly conformant with the Protection Profile Waste Bin Identification Systems WBIS-PP Version 1.04 BSI-PP-0010-2004. The following rationale is 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 R4, 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 with the following exception:
        - Part of the assumption A.Check has been omitted and therefore part of the security objective for the operational environment OE.Check. The part of the PP security objective OE.Check addressing the omitted part of the A.Check assumption is now re-assigned the new security objective for the TOE OT.Check.
    - The OSPs in the ST are a superset of the OSPs in the PP.
        - The OSP P.Check has been added.

3. Security Problem Definition

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.

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 (if available).
AT2 Time stamp (date and time) of the clearance.
AT3 GPS position (if available).

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. The record of clearance can contain an empty AT1 if the proximity sensor detects that a bin has been cleared but the RFID tag has not been adequately read.

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.
Note: In the current TOE each record of clearance AT is transmitted individually, and therefore AT+ is equivalent to AT, however both terms are used for readability and compatibility with the PP.

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.

The data of the record of clearance (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 organizational 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 authorized and trustworthy. All persons who install and maintain the system are authorized and trustworthy (S.Trusted). All persons responsible for the security of the TOE environment (S.Trusted) are authorized 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.

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.

3.3. Organizational Security Policies

The following OSPs are stated for the TOE:

P.Check Check of completeness

The TOE shall identify if data has not been adequately received by the security module and it shall be recovered by repeated transport of data.

P.Save 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.

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 organizational 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 recognize 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 blocks

The TOE shall recognize any attempt to transfer arbitrary (i.e. invalid) clearance data blocks (AT+) to the security module. The TOE shall recognize 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.Save 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.

OT.Check Automatic retransmission

The TOE shall identify if data has not been adequately received by the security module and it shall be recovered by repeated transport of data.

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 organizational means which are out of the scope of the TOE.

OE.Trusted Trustworthy personnel

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

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. 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.

	OT.Inv#1	OT.Inv#2	OT.Save	OT.Check	OE.Id	OE.Trusted	OE.Acess	OE.Check	OE.Backup
T.Man	X								
T.Jam#1	X								
T.Create		X							
T.Jam#2		X							
P.Save			X						
P.Check				X					
A.Id					X				
A.Trusted						X			
A.Access							X		
A.Check								X	
A.Backup									X

4.3.2. 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.

Policies and Security Objective Sufficiency

P.Save (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.Save, so this objective is sufficient for P.Save.

P.Check (Check of completeness) establishes the detection of not adequately transmitted data blocks and the retransmission of them from the vehicle software to the security module if they have not been received correctly. This is exactly repeated by the objective OT.Check, so this objective is sufficient for P.Check.

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 recognized 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 recognized 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 recognized 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 recognized by the TOE which counters directly the threat T.Jam#2.

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 organizational 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. 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.

5. 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, except for the component FDP_ITT.5, which is defined in the [WBISPP104] Protection Profile. Operations for assignment, selection and refinement have been made.

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.

5.1. Extended Components 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.

5.2. Security Functional Requirements

The TOE is part 2 extended. Extended requirements are identified as "Common Criteria Part 2 extended".

5.2.1. Data authentication (FDP_DAU)

5.2.1.1. 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 **[assignment:** *clearance AT and clearance data blocks AT+1*].

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

5.2.2. Internal TOE transfer (FDP_ITT)

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

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

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.

5.2.3. Stored data integrity (FDP_SDI)

5.2.3.1. Stored data integrity monitoring (FDP_SDI.1)

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

5.2.4. Fault Tolerance (FRU_FLT)

5.2.4.1. Degraded fault tolerance (FRU_FLT.1/FLASH)

FRU_FLT.1.1/FLASH The TSF shall ensure the operation of **[assignment:** *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: **[assignment:** *Loss of user data in the primary memory of the vehicle software*].

5.2.4.2. Degraded fault tolerance (FRU_FLT.1/GPRS)

FRU_FLT.1.1/GPRS The TSF shall ensure the operation of **[assignment:** *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: **[assignment:** *Loss of connection with the security module*].

5.3. Security Functional Requirements Rationale

5.3.1. 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.Save	OT.Check
FDP_DAU.1		X		
FDP_ITT.5	X	X		
FDP_SDI.1	X	X		
FRU_FLT.1/FLASH			X	
FRU_FLT.1/GPRS				X

5.3.2. Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable.

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.Save (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 realized by the TOE according to **FRU_FLT.1/FLASH**.

OT.Check (Fault tolerance) addresses the retransmission 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 error during transmission from the vehicle software to the security module. The operation of this data transfer is realized by the TOE according to **FRU_FLT.1/GPRS**.

5.3.3. Dependency Rationale

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.

Requirement	Dependencies	Fulfilled
FDP_DAU.1	None	Implicitly
FDP_ITT.5	None	Implicitly
FDP_SDI.1	None	Implicitly
FRU_FLT.1/FLASH	FPT_FLS.1	See discussion below
FRU_FLT.1/GPRS	FPT_FLS.1	See discussion below

FRU_FLT.1/FLASH 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 while **FRU_FLT.1/GPRS** requires the TOE to ensure the operation of the data transfer from the vehicle software to the security module even if the connection is lost. Those requirements are driven to fulfill organizational security policies (P.Safe and P.Check), which relate more to the availability of the data than 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.

5.4. Security Assurance Requirements

The security assurance requirements are those corresponding to EAL1 components as described in Common Criteria 3.1R4 Part 3, augmented with ASE_SPD.1. No operations are applied.

Assurance Class	Assurance Components
ASE: Security Target Evaluation	ASE_CCL.1: Conformance claims ASE_ECD.1: Extended components definition ASE_INT.1: ST introduction ASE_OBJ.1: Security objectives for the operational environment ASE_REQ.1: Stated security requirements ASE_SPD.1: Security problem definition ASE_TSS.1: TOE summary specification
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
ATE: Tests	ATE_IND.1: Independent testing - conformance
AVA: Vulnerability Assesment	AVA_VAN.1: Vulnerability survey

5.5. Security Assurance Requirements Rationale

The assurance level for this security target EAL1+ASE_SPD.1. 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 augmentation allows verification that the security problem is really addressed by the TOE and its operational environment.

6. 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.

6.1. 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 checksum mechanism over each stored record. This checksum is generated by the TOE in the igMobile vehicle software. Another checksum is calculated and sent to the security module along with the rest of the record. This data is finally saved in the database.

6.2. 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.

6.3. 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.

6.4. FRU_FLT.1/FLASH 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.

6.5. FRU_FLT.1/GPRS 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 data connection. This is achieved by retransmission of the package until success. When a package has been successfully transferred it is marked as removed from the flash memory.

7. References

Code	Description
[WBISPP104]	Protection Profile Waste Bin Identification Systems WBIS-PP Version 1.04 BSI-PP-0010-2004
[CC]	Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2012. Version 3.1 Revision 4.

8. Acronyms

Acronym	Description
PP	Protection Profile
ST	Security Target
EAL	Evaluation Assurance Level
CC	Common Criteria
GPRS	General Packet Radio Service
RFID	Radio Frequency IDentification
GPS	Global Positioning System
WBIS	Waste Bin Identification System
HTTP	Hypertext Transfer Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol