Common Criteria
for Information Technology
Security Evaluation

SOMA-WISE WASTE RFID SYSTEM
Security target

Version 5.0 - Lite

01/07/2013

Table of Contents

1 Introduction

1.1 References

[CC31P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, CCMB-2009-07-001, v3.1 Release 4, September 2012.

[CC31P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2009-07-002, v3.1 Release 4, September 2012.

[CC31P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2009-07-003, v3.1 Release 4, September 2012.

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

[OPE40V03] System Manual SOMA® Wise Waste® V4.0 RFID-V03, February 2013.

[TOEP2] Manual Ww Rfid Toe Parts-V2, February 2013.

1.2 ST reference

1 **Title:** SOMA - WISE WASTE® RFID SYSTEM Security target

2 **Version:** 5.0 - Lite

3 **Author:** SOMA – Sociedade de Montagem de Automóveis S.A.

4 **Publication date:** 01/07/2013

1.3 TOE reference

5 **TOE name:** WISE WASTE® RFID SYSTEM

6 **TOE version:** 3.0.0

7 **Developer:** SOMA

8 **TOE release date:** 15/05/2013

1.4 TOE overview

1.4.1 TOE usage

9 The TOE is the WISE WASTE® RFID SYSTEM, which is a "Waste Bin Identification System" as defined in the WBIS-PP. This is a system that

aims the operational and fleet management of waste collection companies and it is designed to implement billing methods based on how many times one's waste bin is collected.

10 This TOE is classified as a "Waste Bin Identification System (WBIS)" as defined in the WBIS-PP. The full system consists of the following components:

11 - An ID-Tag, containing the identification data of a waste bin.

12 - A vehicle with an ID-Tag reader (consisting in antennas, a multiplexer and reader module), lifter sensors, a button box and a vehicle computer. The vehicle computer consists on a processing unit and a modem. The vehicle software is installed in the vehicle computer, hence, in the module containing the processing unit and the modem. The interface with the driver is done through a tactile display.

13 – The office computer, installed in a remote location. The security module and the server software are in this office computer.

14 Of the above described components, only the following are part of the TOE:

15 – The ID-Tag.

16 – The vehicle software.

17 - The security module.

18 With this system, waste containers equipped with an ID-Tag are identified and their associated clearance data is recorded and time stamped by the vehicle software. This data contains the identification number of the container. The recorded and time stamped information is then sent to the office computer to be used for billing purposes by city councils or waste collection private companies. It should be noted that this system identifies waste containers and not the actual waste.

19 The WISE WASTE® RFID SYSTEM is capable of protecting the billing data for manipulation and loss, providing a reliable structure for data transmission and backup. The collection records are backed up in the vehicle computer, pre-validated by the vehicle software and then sent to the office computer of the city council or disposal company. After strict validation and scrutiny in the security module located in the office computer, the clearance data can then be used to generate billing invoices.

20 Not only clearance data is exchanged between the vehicle software and the office computer. As WISE WASTE® RFID is an operational and fleet management system, all the information regarding the work performed by the collection teams is processed and sent to the office computer.

21 There, through accessing the server software, TOE costumers such as city councils or private waste collection companies may not only manage the work performed by their employees but also charge their own costumers based on the clearance records. They can generate reports, billing invoices and monitor, in real time, the work being performed by the waste collection teams.

22 The access to the vehicle software is granted to authorized personnel only, due to physical and organizational measures. The office computer may only be accessed by anyone who has valid credentials for it.

23 The TOE consists solely on the ID-Tag, the vehicle software and the security module. All other components are part of the TOE environment, not the TOE. Therefore, the TOE environment consists in elements such as the lifter sensors, the button box, the ID-Tag reader (antennas, reader and multiplexer), the tactile display and the physical channels from the ID-Tag to the vehicle software, from the vehicle software to the tactile display and from the vehicle software to the security module. All additional interfaces, as well as the tactile display software and the office software are also not part of this TOE.

24 In terms of security features, the TOE is capable of:

25 – Generate and guarantee the validity of records of clearance data AT and clearance data blocks AT+.

26 – Prevent the modification of user data when it is transmitted between physically separated parts of the TOE.

27 – Monitor stored data for random manipulation.

28 – Implement fault tolerance when loss of user data in the primary memory of the vehicle software occurs.

1.4.2 TOE type

29 The WISE WASTE® RFID SYSTEM is a "Waste Bin Identification System (WBIS)" as defined in the WBIS-PP. WBIS are systems which allow the identification of waste bins with ID-Tags (e.g. an electronic chip which is referred to as transponder) in order to determine how often a specific waste bin has been cleared.

30 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. Therefore, WBIS comprise the electronic collection of data, the transfer and recording of clearance data and the creation of notifications for waste fees. The real time management and storage of the information is done by a web-server and database.

1.4.3 Non TOE Hardware and Software

31 As stated before, the TOE consists exclusively on the ID-Tag, the vehicle software and the security module, the other components are part of the TOE environment. Thus, the following components may be considered as Non-TOE hardware and software:

32 – The five lifter sensors: two of them indicating the presence of 2-wheel containers, one of them indicating the presence of 4-wheel containers and two of them indicating the collection of containers.

33 – The button box, with two illuminated indicators and six illuminated pushbuttons.

34 – The hardware of the three ID-Tag antennas used (being one of them optional).

35 – The hardware and firmware of the ID-Tag multiplexer, used to combine the signals of the three antennas into one single signal.

36 – The hardware and firmware of the ID-Tag reader module.

37 – The hardware and software of the tactile display. The hardware used is a multi-function tactile display, with software developed by SOMA complied using Windows CE 5.0.

38 – All the physical interfaces in-between the components detailed above and the vehicle computer, such as the wiring needed to connect the components.

39 – Any extra features than can be added to the vehicle computer, such a hands-free kit for the vehicle driver with speaker and microphone.

40 – The office computer hardware and the server software, implemented using BMC Remedy Software and Windows Server 2008 R2.

1.5 TOE description

41 The WISE WASTE® RFID SYSTEM, is a "Waste Bin Identification System (WBIS)" and consists of the following components:

42 – An ID-Tag containing the identification of the waste container (the waste is not identified).

43 – An ID-Tag reader (containing up to three antennas, a multiplexer and a reader module), a button box, lifter sensors, a vehicle computer and a tactile display to use as the driver interface, all installed on the vehicle. The vehicle computer consists on a processing unit and a modem. The vehicle computer may also have some add-on features, such as a hands-free kit for the vehicle driver. The vehicle software is the one installed in

the vehicle computer considering no add-on features; therefore, it consists on the processing unit and the modem software.

44 – The office computer, installed in a remote location. The security module and the server software are in this office computer. The server software is responsible for showing the data to the user in an appropriate way.

45 The following picture gives an overview of the WISE WASTE® RFID SYSTEM:

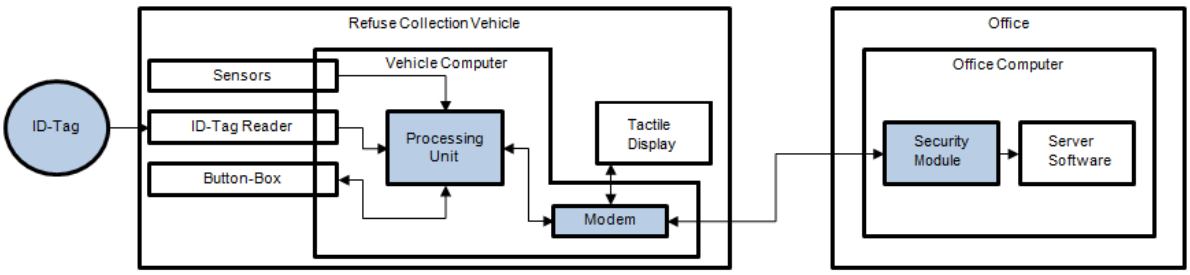


Figure 1 WISE WASTE® RFID Waste Bin Identification System

46 The blue-shaded components in Figure 1 are the parts of the TOE. Hence, the TOE consists in the following modules:

47 - An ID-Tag containing the identification of the waste container (the waste is not identified).

48 - A vehicle computer with a processing unit and a modem. The vehicle software is the one installed in the vehicle computer considering no add-on features, namely, the software of the processing unit and the modem.

49 - A security module installed in a remote location that interfaces the refuse collection vehicle with the office computer.

50 This system allows billing scenarios according to the number of clearances of a specific waste bin, equipped with an ID-Tag, used to identify the container. This data is unique and non-confidential. Usually, there is a one-to-one correspondence between a set of identification data and the person or entity that is subject to charge. The identification data is read by the reader during the emptying of a waste container. If an ID-Tag is correctly identified, a LED indicator situated in the button-box will light up green.

51 The identification data is then forwarded to the vehicle software, parallel with the signals detected from the corresponding lifter sensors and, additionally, with signals from the button-box if that is the case.

52 The processing unit is the one who receives all this information, validates its format, adds a time stamp to it and backups it in non-volatile memory, that can be accessed externally through USB interface

in case of any data loss during further transmissions. Then, the processing unit creates clearance data blocks with a specific format, using the ID records received, and forwards them to the modem, which is also responsible for forwarding some messages directly to the security module and some other messages to the tactile display.

53 The clearance data blocks sent directly to the server are the ones that are going to be used to generate the billing invoices. These data blocks will be analyzed further by the security module, in order to defeat additional possible attacks. The clearance records can then be transmitted to external systems for the billing process by the server software, which is also responsible for showing in real-time the fleet and operational management information.

54 As stated before, some of the messages generated by the processing unit are sent to the modem to be forwarded to the tactile display, which acts as the driver interface. The tactile display is responsible for generating the operational and fleet management information of the system, based on the driver's actions, data registers and also based on the information received from the processing unit through the modem, hence keeping the driver aware of the collection state at every moment. The vehicle driver is completely unaware about the ID-Tag of the container being collected, he only is aware about the state of the collection process, that is, if the container collected was successfully identified or not, hence, if the container collected had an ID-Tag attached to it or not.

55 The information produced by the tactile display is also sent to the modem, to be then forwarded to the office computer. Even though this information is sent to the security module, it is not an asset protected by the TOE and, therefore, no protection mechanism implemented by the TOE is performed for this information.

56 The ID-Tag, the data transmission link between the ID-Tag and the vehicle software and the transmission link between the vehicle 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 seen as low, so low attack potential can be assumed. As stated before, only authorized personnel has access to the vehicle (hence the vehicle computer) and the office computer, due to suitable physical and organizational measures. This protection is implemented by the vehicle with its components and in the office computer.

57 In terms of security features, the TOE is capable of:

58 – Generate and guarantee the validity of records of clearance data AT and clearance data blocks AT+. The vehicle software will be responsible for implementing this security feature.

59 – Prevent the modification of user data when it is transmitted between physically separated parts of the TOE. The vehicle software and the security module will be responsible for implementing this security feature.

60 – Monitor stored data for random manipulation. The vehicle software will be responsible for implementing this security feature.

61 – Implement fault tolerance when loss of user data in the primary memory of the vehicle software occurs. The vehicle software will be responsible for implementing this security feature.

62 The TOE is provided to the final costumer fully installed and configured. The modem and tactile display are installed in the vehicle's cabin, near the driver. The tactile display is installed on top of the vehicle's dashboard (accessible by the driver), but the modem is installed inside the vehicle's dashboard, as well as all electrical connections. The processing unit and ID-Tag reader are provided in an enclosure box, installed on the top left-side of the vehicle, near the backside. The button box, sensors and antennas are installed in the vehicle's lifter, on the backside. As for the security module, it is installed in a remote server and is not provided to the customer. The ID-Tags are installed in each waste bin.

63 Upon delivery of the system, the customer is provided with two printed short manuals per vehicle, one explaining the operators how to work with the tactile display and the other explaining the operators how to work with the button box. These short manuals are summarised parts of the complete system manual and annex, [OPE40V03] and [TOEP2], which are provided to the customer printed in the end of an installation set (that is, when the system installation in a set of vehicles is completed).

2 Conformance claims

2.1 CC Conformance Claim

64 This Security Target is developed according to the Common Criteria for Information Technology Security Evaluation version 3.1 Release 4:

- Part 2 [CC31P2] extended.
- Part 3 [CC31P3] conformant.

2.2 PP Claim, Package Claim

65 This Security Target conforms to Common Criteria Evaluation Assurance Level (EAL) 1 + ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2.

66 This ST claims strict conformance to [WBIS-PP]. As the TOE type written in the ST is exactly the same than the one of the PP, the consistency between both is achieved.

67 [WBIS-PP] was certified for the version 2.1 of Common Criteria. The security target for SOMA-WISE WASTE RFID SYSTEM claims conformance to the version 3.1 R4 of Common Criteria. The usage of this version (3.1 R4) provides the same or greater guarantees than the version 2.1.

68 Therefore, it is acceptable to claim conformance to the protection profile, despite of using a different version of Common Criteria in the security target.

3 Security Problem Definition

3.1 TOE assets

- **AT:** A record of clearance AT corresponding to a clearance of a waste bin is an asset in the TOE. 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 the TOE 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.

3.2 Agents of the threat

- **Attacker** A human or a process acting on his behalf located outside the TOE. The main goal of the attacker is to modify or corrupt application sensitive information. The attacker has at most 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).

3.3 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.

3.4 Threats

69 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** 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** 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** creates arbitrary clearance data blocks (**AT+**) and transmits them to the security module.

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

  An **attacker** 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.

3.5 Organizational Policies

70 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. The above required functionality refers only to the data stored in the vehicle software. This functionality is ensured till complete transfer to the security module and hence to the office 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).

3.6 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 attackers 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.

4 Security Objectives

71 The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition.

72 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

73 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

- **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 remote server. 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 Operational Environment

74 The operational environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE).

- **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 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

75 The following table shows the 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					

4.3.2 Security Objectives Sufficiency

4.3.2.1 Policies and Security Objective Sufficiency

76 **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.

4.3.2.2 Threats and Security Objective Sufficiency

77 **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.

78 **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.

79 **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.

80 **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.

4.3.2.3 Assumptions and Security Objective Sufficiency

81 **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.

82 **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.

83 **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.

84 **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.

85 **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 components definition

5.1 Internal transfer integrity protection (FDP_ITT.5)

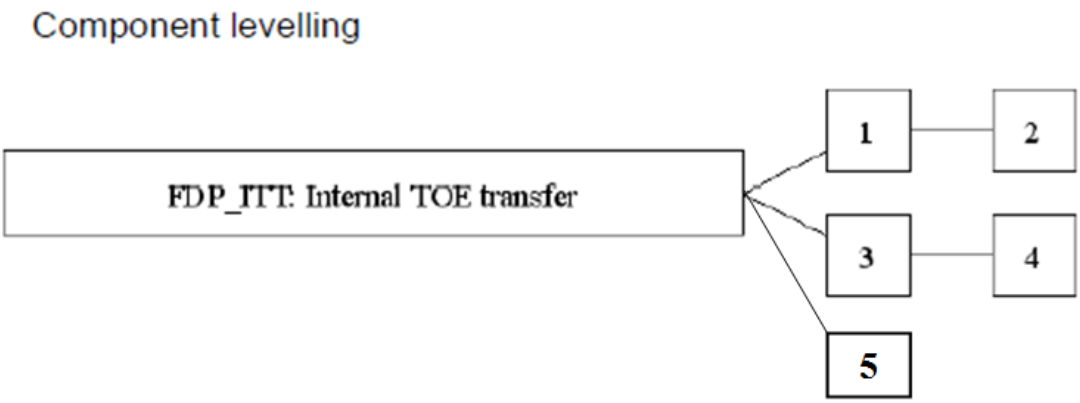
86 To define the security functional requirements of the TOE an additional component (FDP_ITT.5) of the Family FDP_ITT (Internal TOE transfer) is defined here. The family "Internal TOE transfer" (FDP_ITT)" is extended as follows (only changes are given here).

87 FDP_ITT.5 has been defined 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.

88 **Family Behaviour (of FDP_ITT)**

89 In addition of what is included in the [CC31p2] regarding the family behaviour:

FDP_ITT.5 aims the integrity protection of user data when it is transmitted between physically-separated parts of the TOEF. 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.



90 In addition of what is included in the [CC31p2] regarding the components of this family:

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

91 In addition of what is expressed regarding "**management**" and "**audit**" in the [CC31p2] regarding the components of this family:

Management: FDP_ITT.5

No management activities foreseen for this component.

Audit: FDP_ITT.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

No audit activities foreseen for this component.

92 **FDP_ITT.5 Internal transfer integrity protection**

Hierarchical to: No other components.
Dependencies: None

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.

6 Security Requirements for the TOE

6.1 Functional Security Requirements

6.1.1 Data authentication (FDP_DAU)

6.1.1.1 Basic data authentication (FDP_DAU.1)

93 **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+***.

94 **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 8:

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

6.1.2 Internal TOE transfer (FDP_ITT)

6.1.2.1 Internal transfer integrity protection (FDP_ITT.5)

95 **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.

96 **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.

6.1.3 Stored data integrity (FDP_SDI)

6.1.3.1 Stored data integrity monitoring (FDP_SDI.1)

97 **FDP_SDI.1.1** The TSF shall monitor user data stored 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***.

6.1.4 5.1.4 Fault tolerance (FRU_FLT)

6.1.4.1 Degraded fault tolerance (FRU_FLT.1)

98 **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 Assurance Security Requirements

99 The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements:

- EAL1

100 The following table shows the assurance requirements by reference the individual components in [CC31P3]

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.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

101 The EAL1 allows developing the so-called “low assurance” security target. As this ST claims conformance with the [WBIS-PP] and this PP contains:

102 - A security problem definition (Section 3 of the PP);

103 - The specification of the security objectives for the TOE (section 4.1 of the PP) and a rationale to demonstrate that they resolve the security problem defined (section 6.2 of the PP);

104 - The security functional requirements (section 5.1) and a rationale to demonstrate that they are necessary and sufficient to meet the security objectives for the TOE defined (section 6.3 of the PP).

105 This ST has included these mentioned sections providing this way a standard ST rather than the “low assurance ST” required by the EAL1. Therefore, the assurance level EAL1 has been augmented with the following assurance ASE families: ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2.

The inclusion of the augmentations (ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1) do not affect to the conformance with the protection profile [WBIS-PP].

6.3 Rationale for the Security Requirements

6.3.1 Security Requirement Coverage

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

6.3.2 Security Requirement Sufficiency

106 **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.

107 **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 remote server, 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.

108 **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.

6.4 Dependency Rationale

109 The security assurance components are taken exactly as specified by EAL1 and augmented with the following assurance ASE families: ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2. The developer has reviewed the dependencies of the augmented components (ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2) and has confirmed that the dependencies are fulfilled. All dependencies are therefore completely fulfilled.

110 The functional requirements dependencies for the TOE and for the environment are not completely fulfilled:

- FDP_DAU.1, FDP_ITT.5 and FDP_SDI.1 have no dependencies.
- 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.

6.5 Rationale for Assurance Level EAL1

111 The assurance level for this protection profile is EAL1, augmented with the following assurance ASE families: ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2.

112 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.

113 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.

114 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.

115 The assurance level EAL1 augmented with ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2 has been chosen because the developer has decided to write a standard security target, instead of a low assurance security target.

7 TOE Summary Specification

7.1 FDP_DAU.1 (Basic Data Authentication)

116 The TOE encapsulates each collection record AT into a predefined message format by the vehicle computer, generating an AT+ record. Take into account that each AT+ record is only composed of one AT record. Several AT records are not grouped into an AT+ record to be sent.

117 The AT record is passed through a CRC algorithm, as defined in ISO 11785 and both values are sent in a predefined frame format (AT+).

7.2 FDP_ITT.5 (Internal Transfer Integrity Protection)

118 The transmission of the AT1 records between the ID-Tag reader and the vehicle software is integrity secured through comparing the output of the reader with a structured byte frame and CRC of the AT1 record.

119 AT+ records are generated by the vehicle software by encapsulating AT record into a predefined message format, as well as newly generated CRC. The transmission of information is secured by comparing the transmitted message to a predefined format, hence maintaining the records integrity.

120 The transmission of records to the security module is secured through GPRS encryption algorithms and VPN tunnelling, which assure the integrity and confidentiality of the information during transmission. The security module will generate a CRC of the received AT+ record and compare it with the CRC value sent in the frame, hence checking the integrity of the records.

7.3 FDP_SDI.1 (Stored Data Integrity Monitoring)

121 The AT1 records transmitted from the ID-Tag reader are time stamped in and written in non-volatile memory. Each record, after being written, cannot be manipulated as it is read-only. As long as the AT1 records coming from the ID-Tag reader are valid and CRC is checked successfully, AT records with CRC will be written into secondary memory. At every access to the secondary memory, the data that is being written is monitored.

7.4 FRU_FLT.1 (Degraded Fault Tolerance)

122 The vehicle software has two memory mechanisms to protect the information in case of failure: primary memory and secondary memory.

123 If connection errors occur between the vehicle and the security module, the system uses its primary memory, that is, the vehicle computer cache.

124 In case billing information is lost in the primary memory of the vehicle software, are stored into the secondary memory which can be accessed through USB by specific software.