REF: 2013-21-INF-1301 v1 | Created by: CERT3
Target: Expediente | Revised by: CALIDAD
Date: 21.03.2014 | Approved by: TECNICO

CERTIFICATION REPORT

File: 2013-21 Boreal IT Security Platform

Applicant: B64874332 Boreal information technology

References:

[EXT 2273] Certification request of Boreal IT Security Platform

[EXT 2410] Evaluation Technical Report of Boreal IT Security Platform.

The product documentation referenced in the above documents.

Certification report of the product “Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors”, as requested in [EX 2273] dated 10-09-2013, and evaluated by the laboratory Applus LGAI Technological Center S.A., as detailed in the Evaluation Technical Report [EXT 2410] received on 24/02/2014

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

EXECUTIVE SUMMARY **3**
TOE SUMMARY 3
SECURITY ASSURANCE REQUIREMENTS 4
SECURITY FUNCTIONAL REQUIREMENTS 5
IDENTIFICATION **5**
SECURITY POLICIES **6**
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT **6**
CLARIFICATIONS ON NON-COVERED THREATS 7
OPERATIONAL ENVIRONMENT FUNCTIONALITY 8
ARCHITECTURE **9**
DOCUMENTS **11**
PRODUCT TESTING **11**
EVALUATED CONFIGURATION **11**
EVALUATION RESULTS **12**
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM **12**
CERTIFIER RECOMMENDATIONS **12**
GLOSSARY **12**
BIBLIOGRAPHY **12**
SECURITY TARGET **13**

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product “Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors” that is classified as a "Waste Bin Identification System (WBIS)" as defined in the protection profile [WBIS-PP]. The TOE parts are:

- The ID-Tag.
- The vehicle software.
- The security module.

Developer/manufacturer: Boreal Information Technology.

Sponsor: Boreal Information Technology.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF:Applus LGAI Technological Center S.A.

Protection Profile: Protection Profile Waste Bin Identification Systems WBIS-PP Version 1.04.

Evaluation Level: Common Criteria version 3.1 revision 4 EAL1+ ASE_SPD.1.

Evaluation end date: 24/02/2014 (ETR delivery).

All the assurance components required by the evaluation level EAL1+ (augmented with ASE_SPD.1) have been assigned a “PASS” verdict. Consequently, the laboratory Applus LGAI Technological Center S.A. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL1+ ASE_SPD.1, as defined by the Common Criteria version 3.1 revision 4 and the Common Methodology for Information Technology Security Evaluation version 3.1 revision 4.

Considering the obtained evidences during the instruction of the certification request of the product “Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors” v1.0, a positive resolution is proposed.

TOE SUMMARY

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.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL1 and the evidences required by the additional component ASE_SPD.1 according to Common Criteria version 3.1 revision 4.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria version 3.1 revision 4:

Class	Components
FDP: User Data Protection	FDP_DAU.1 Basic Data Authentication
	FDP_ITT.5 Internal transfer integrity protection
	FDP_SDI.1 Stored data integrity monitoring
FRU: Resource utilisation	FRU_FLT.1 Degraded fault tolerance

IDENTIFICATION

Product: “Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors” v1.0

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Security Target: "Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors Security Target v1.0".

Protection Profile: Protection Profile Waste Bin Identification Systems WBIS-PP Version 1.04.

Evaluation Level: Common Criteria version 3.1 revision 4 EAL1+ ASE_SPD.1.

SECURITY POLICIES

The use of the product "Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors" v1.0 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target. In short, it establishes the need of implementing organisational policies related to the following aspects.

Policy 01: 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.

Policy 02: 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 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).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

Assumption 01: 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.

Assumption 02: 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.

Assumption 03: 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.

Assumption 04: 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.

Assumption 05: A.Backup Data backup

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

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product “Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors” v1.0, although the agents implementing attacks have

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

the attack potential according to the basic attack potential of EAL1+ ASE_SPD.1 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

Threat 01: 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.

Threat 02: 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.

Threat 03: T.Create Invalid records of clearance

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

Threat 04: 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.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

Environment objective 01: 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.

Environment objective 02: OE.Trusted Trustworthy personnel

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.

Environment objective 03: 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.

Environment objective 04: 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.

Environment objective 05: OE.Backup Data backup

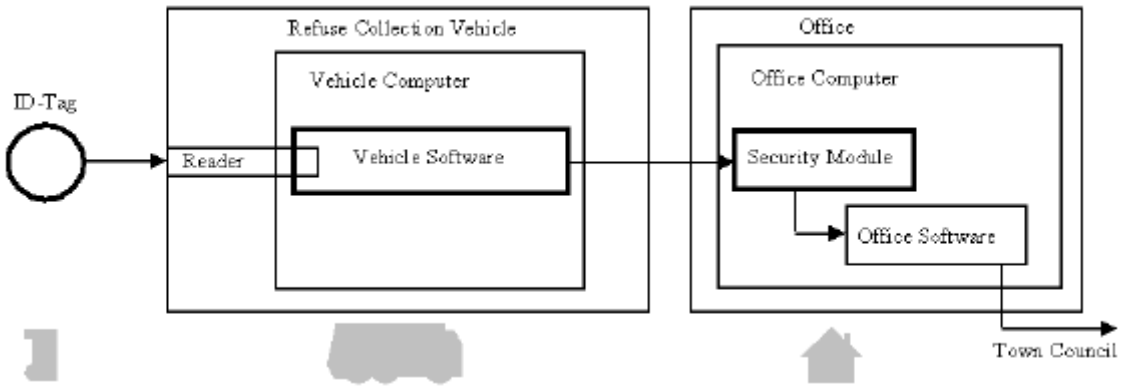
It shall be ensured that the user (S.Trusted) makes backup copies of the data created by the TOE at regular intervals.

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

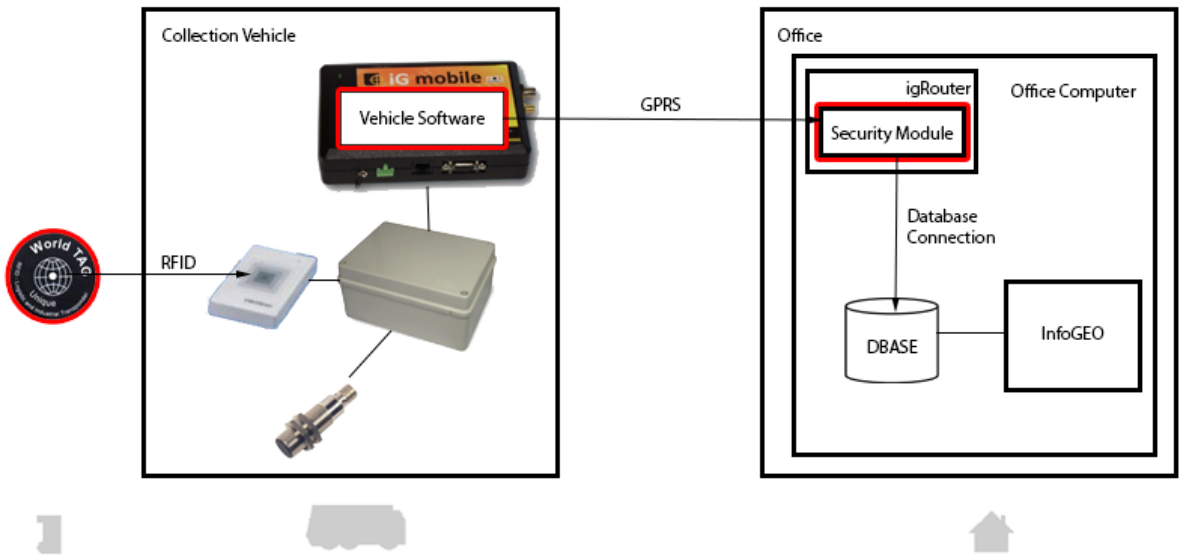
ARCHITECTURE

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

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es



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



The Target of Evaluation (TOE) is a "Waste Bin Identification System (WBIS)" and consists of the following components:

- An ID-Tag containing the identification of the waste container (the waste is not identified).
- 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.
- A security module installed in a remote location that interfaces the refuse collection vehicle with the office computer.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- Preparative Guidance v1.0: The manual used to install the TOE and prepare the operational environment.
- Operational Guidance v1.0: The manual used to operate the TOE.
- Functional Specification v1.0: The functional specification describing TOE interfaces.
- "Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors Security Target v1.0"

PRODUCT TESTING

The evaluator has tested all the SFRs defined through the TOE TSFIs. It has been checked that the obtained results conform to the expected results.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product "Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors" v1.0 it is necessary the disposition of the following components:

The following minimum software versions are installed by the developer as part of the TOE software environment:

Third party:

- Updated Ubuntu 12.04
- PHP 5.3.10
- PostgreSQL 9.1
- Apache 2.2.22

Boreal IT:

- igRouter Software (provided along with the TOE Security module)
- Database v0.3.0

The installation of those environmental components will be performed by Boreal IT personnel.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

EVALUATION RESULTS

The product “Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors” v1.0 has been evaluated against the Security Target “Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors Security Target v1.0”.

All the assurance components required by the evaluation level EAL1+ ASE_SPD.1 have been assigned a “PASS” verdict. Consequently, the laboratory Applus LGAI Technological Center S.A. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL1+ ASE_SPD.1, as defined by the Common Criteria version 3.1 revision 4 and the Common Methodology for Information Technology Security Evaluation version 3.1 revision 4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

There is no additional recommendation from the Laboratory in order to use the evaluated TOE since guidance documentation is enough to make a secure usage of the TOE.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product “Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors” v1.0, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4, September 2012.

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

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: “Secure identification system for the management and control system of actions over urban furniture in the street through RFID sensors Security Target v1.0”

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es