REPUBBLICA ITALIANA

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 1/18

(Certification No.)

Prodotto: **Arco40 evo v. 1.0**
(Product)

Sviluppato da: **Altares s.r.l.**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL1+

(ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 30 gennaio 2018

Common Criteria

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Arco40 evo v. 1.0

OCSI/CERT/TEC/05/2017/RC

Version 1.0

30 January 2018

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	30/01/2018

2 Table of contents

3 Acronyms

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
HW	Hardware
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
PP	Protection Profile
RFID	Radio Frequency IDentification
RFV	Rapporto Finale di Valutazione (Evaluation Technical Report)
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SW	Software
TDS	Traguardo di Sicurezza (Security Target)
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
WBIS	Waste Bin Identification System

4 References

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

[CONF] “Arco40 evo Configuration List”, versione 1.1, 29 dicembre 2017, Altares s.r.l.

[MAN] “Arco40 evo Manuale Utente”, versione 1.0, 16 ottobre 2017, Altares s.r.l.

[RFV] “Rapporto Finale di Valutazione del prodotto Arco40 evo”, versione 1.0, 11 gennaio 2018, LVS Technis Blu

[TDS] “RFID Identification and Geolocation system for waste collection Arco40 evo v. 1.0” Security Target, version 1.4, 14 december 2017, Altares s.r.l.

[WBIS-PP] Protection Profile - Waste Bin Identification Systems (WBIS-PP Version 1.04), BSI-PP-0010-2004, 27 May 2004

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on http://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all assurance components selected.

5.2 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL 2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on http://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all assurance components selected.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “RFID Identification and Geolocation system for waste collection - Arco40 evo v. 1.0”, short name “Arco40 evo v. 1.0”, developed by Altares s.r.l.

The TOE “Arco40 evo v. 1.0” is a "Waste Bin Identification System (WBIS)", which allows to identify waste bins by an ID-TAG (e.g. an electronic chip which is referred to as transponder).

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 and assessment of fees for waste management.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [TDS]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL1, augmented with ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, according to the information provided in the Security Target [TDS] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “Arco40 evo v. 1.0” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [TDS], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

Name of TOE	Arco40 evo v. 1.0
Security Target	“RFID Identification and Geolocation system for waste collection - Arco40 evo v. 1.0” Security Target, Version 1.4, 14 december 2017, Altares s.r.l.
Evaluation Assurance Level	EAL1 augmented with ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2
Developer	Altares s.r.l.
Sponsor	Altares s.r.l.
LVS	Technis Blu s.r.l.
CC version	3.1 Rev. 5
PP claim	PP - Waste Bin Identification Systems (WBIS-PP Version 1.04), BSI-PP-0010-2004, [WBIS-PP]
Kickoff date	11 July 2017
Completion date	11 January 2018

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [TDS] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of TOE; for a detailed description, please refer to the Security Target [TDS].

The TOE “Arco40 evo v. 1.0” is a "Waste Bin Identification System (WBIS)", which allows to identify waste bins by an ID-TAG (e.g. an electronic chip which is referred to as transponder) (see Figure 1).

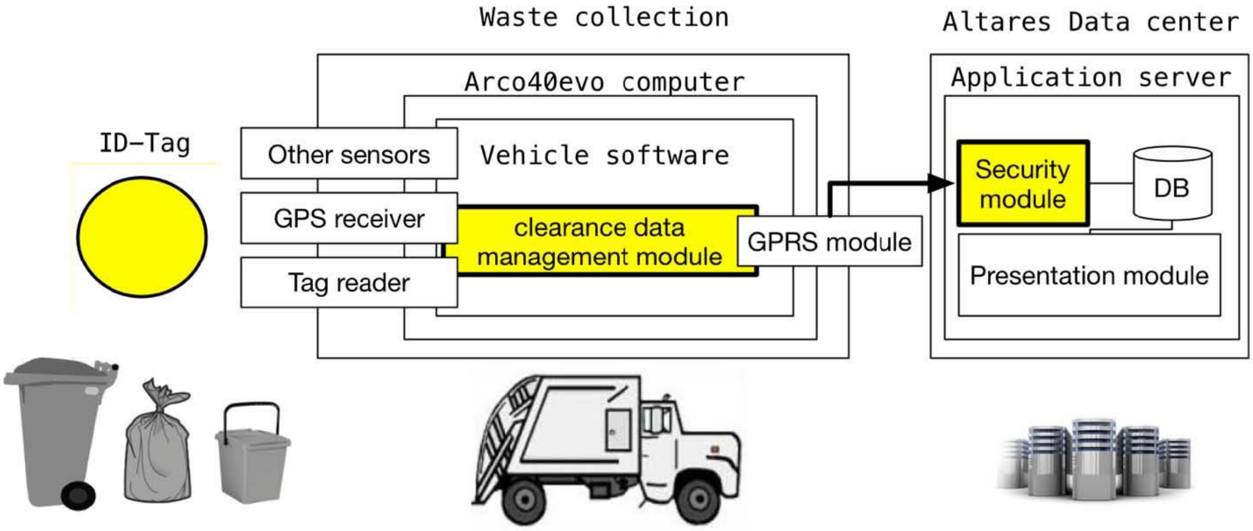

Figure 1 – The TOE “Arco40 evo v. 1.0” (Waste Bin Identification System)

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 and assessment of fees for waste management.

Each waste bin is equipped with a data carrier (ID-TAG), which stores data 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 user (person, business company or organisation) who is subject to charge. The identification data are read during (or before/after) clearance of the waste bin by the “READER” module. Possible malfunctions during transfer and manipulations are detected. The identification data is then transmitted to the vehicle software, which supplements these data by adding:

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

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

The records are transmitted by the CLEARANCE DATA MANAGEMENT MODULE to the SECURITY MODULE in the application Server. The CLEARANCE DATA MANAGEMENT MODULE ensures by means of adequate measures (e.g. backup of data) that the transfer is even possible after a loss of data in the primary memory.

The SECURITY MODULE ensures that possible malfunctions during transfer are detected and the failed records are retransmitted until the transmission succeeds.

The clearance records are transmitted to external systems (e.g. of the town council authorities) for the billing process. Such external systems can provide additional functionality (e.g. detection of possible misuse in replayed clearance data record etc.) aside from the billing functionality to supplement the security functionality of the TOE.

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

7.3.1 TOE Architecture

The TOE consists of an ID-TAG, the CLEARANCE DATA MANAGEMENT MODULE included in vehicle software and the SECURITY MODULE (modules highlighted in yellow in Figure 1). All other components are not part of the TOE but of the TOE environment. The TOE has an external interface to the memories of the vehicle computer, a logical internal interface between the ID-TAG and the vehicle software, a logical internal interface between the vehicle software and the security module, and an external interface between the security module and the server software. The physical channel from the ID-TAG to the vehicle software and from the vehicle software to the SECURITY MODULE are not part of the TOE. Additional interfaces, especially to the accounting centers, are not part of the evaluation. The DB and the Presentation module in application software are also not part of the TOE.

For a detailed description of the TOE, consult section 1.4 of the Security Target [TDS]. In particular, the physical scope of the TOE is described in par. 1.4.2 and the logical scope in par. 1.4.3.

7.3.2 TOE security features

The main security features of the TOE are the following:

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

- **Recognition of invalid clearance data records**: The TOE will recognize any attempt to transfer arbitrary (i.e. invalid) clearance data records to the security module. The TOE will recognize manipulations of clearance record during processing and storage within the vehicle and manipulations of the clearance data records by random jam during transfer from the vehicle software to the security module.

- **Fault tolerance**: The vehicle software as a part of the TOE will ensure that the data of the clearance data records is secured by a redundant saving of the data in a secondary memory in such a way that the transfer of the clearance data records from the vehicle software to the security module is possible in a case that clearance data records 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.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product, which is delivered to the customer together with the product, contains all the information for secure installation, configuration and secure use the TOE in accordance with the requirements of the Security Target [TDS].

Customers should also follow the recommendations for the safe use of the TOE contained in par. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [TDS] claims strict conformance to the following Protection Profile:

- Protection Profile - Waste Bin Identification Systems (WBIS-PP Version 1.04), BSI-PP-0010-2004, 27 May 2004 [WBIS-PP].

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

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

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

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

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

The Security Requirements SFR are the same stated in the PP.

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

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the Security Functional Requirements (SFR) have been selected or derived by extension from CC Part 2 [CC2]. In particular, considering that the Security Target claims strict conformance to the [WBIS-PP] PP, the following extended component from such PP is included: FDP_ITT.5 Internal transfer integrity protection.

Please refer to the Security Target [TDS] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [TDS]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) Technis Blu s.r.l.

The evaluation was completed on 11 January 2018 with the issuance by LVS of the Evaluation Technical Report [RFV], which was approved by the Certification Body on 23 January 2018. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [TDS], with reference to the operating environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [RFV] issued by the LVS Technis Blu s.r.l. and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE “Arco40 evo v. 1.0" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL1, augmented with ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2, with respect to the security features described in the Security Target [TDS] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL1, augmented with ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Classe ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Classe ADV**	Pass
Basic functional specification	ADV_FSP.1	Pass
Guidance documents	**Classe AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Classe ALC**	Pass
Labelling of the TOE	ALC_CMC.1	Pass
TOE CM coverage	ALC_CMS.1	Pass
Test	**Classe ATE**	Pass
Independent testing - conformance	ATE_IND.1	Pass
Vulnerability assessment	**Classe AVA**	Pass
Vulnerability survey	AVA_VAN.1	Pass

Table 1 – Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body OCSI are summarized in Section 6 - Statement of Certification.

Potential customers of the product "Arco40 evo v. 1.0" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [TDS].

The TOE must be used according to the Security Objectives for the operational environment specified in par. 4.2 of the Security Target [TDS]. It is assumed that, in the operating environment of the TOE, all the assumptions and the organizational security policies described in the TDS are respected.

This Certification Report is valid for the TOE in the evaluated configuration, reported in Annex B – Evaluated configuration; in particular, the procedures for initialization, configuration and safe use of the product are described in the guidance documentation (User Manual [MAN]) provided together with the TOE.

9 Annex A – Guidelines for the secure usage of the product

The guidance documents relevant to the evaluation or referenced within the documents produced and available to potential users of the TOE are the following:

- [TDS] “RFID Identification and Geolocation system for waste collection Arco40 evo v.1.0” Security Target, version 1.4, 14 december 2017, Altares s.r.l.
- [MAN] “Arco40 evo Manuale Utente”, versione 1.0, 16 ottobre 2017, Altares s.r.l.

In particular, the User Manual [MAN] contains all the information necessary for installation, use and maintenance of an Arco40evo system for reading and geolocation of emptying in waste collection systems. This document is addressed both to installers who need to start up the system, and to service and maintenance technicians who perform error analysis or replace components.

10 Annex B – Evaluated configuration

The TOE is identified in the Security Target [TDS] with the version number 1.0. The name and version number uniquely identify the TOE and the set of its components, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

The components of the evaluated configuration are listed in detail in the Configuration List, provided by the developer to the Evaluators in the document [CONF].

The components are summarized below, for both the vehicle computer (Table 2) and the remote server (Table 3).

VEHICLE COMPUTER		
	TYPE	**COMPONENTS**
TOE		/opt/arco40evo/arco40evo
ENVIRONMENT	Solaris BSP	BSP (Board Support Package) Altares 1.0 GSPD Demon management GPS 3.16 Digium QT 5.5 SQLite 3.10
	Operating System	Linux 4.4
	Hardware	CPU Atmel SAMA5D36 – Cortex A5 536 MHz Memory RAM 256MB DDR2 NAND Flash 256 MB Micro SD 2GB Modem GPRS Bluetooth 2.0 I/O Digital isolated 3 x RS232 1 x RS485 1 x CAN BUS Display RGB GPS

Table 2 – Vehicle computer components

REMOTE SERVER		
	TYPE	**COMPONENTS**
TOE		/opt/altares/arco40evo/sync/Arco40EvoSync
ENVIRONMENT		Digium QT 5.3 MySQL server5.5.58 PHPMyAdmin 4.2.12deb2+deb8u2 Apache web server 2.3.10 (Debian) with extension PHP5 mysql 5.5.58 PHP 5.6.30-0+deb8u1 (cli)
	Operating System	Linux Debian Jessie 8.10 x64 with kernel 3.16.0-4-amd64
	Hardware	Server SMART on cloud Aruba Hypervisor: vmware vSphere CPU: 1 Core intel Xeon E5-2650L v4 RAM: 1GB HDD: 20GB SSD Storage

Table 3 – Remote server components

11 Annex C – Test activity

This annex describes the task of both the evaluators and the developer in testing activities. For the assurance level EAL1, augmented with ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2, such activities do not require the execution of functional tests by the developer, but only independent functional tests by the Evaluators.

11.1 Test configuration

For the execution of these activities a test environment has been placed at the LVS site with the support of the developer, which provided the necessary resources. Before the tests, the software application has been initialized and configured in accordance with the guidance documentation (User Manual [MAN], as indicated in Annex A – Guidelines for the secure usage of the product, and taking into account the information reported in the Security Target [TDS] and in the Configuration List [CONF].

11.2 Functional independent tests performed by the evaluators

Therefore, the evaluators have designed independent testing to verify the correctness of the TSFI.

In the design of independent tests, the evaluators have considered the security functions of the TOE, as described in the Security Target [TDS] and, on the basis of their experience, they have prepared a set of tests, with the aim of verifying the adequacy of the security functions of the TOE, in compliance with the provisions of the CEM.

In particular, the functional tests planned and performed by the LVS were aimed at verifying the following security functions of the TOE:

- Recognition of invalid identification data. This test class verifies the security functions for the identification of manipulations of the identification data of the clearance records inside the identification unit and while they are transferred between the identification unit and the vehicle software. The protection of the integrity of the identification data is required by FDP_SDI.1 and directly addresses random manipulation of these data. Data integrity protection is required by FDP_ITT.5 for data transfer between physically separated parts of the TOE. By ensuring data integrity, data are also protected from manipulation during transfer.

- Recognition of invalid clearance data records. This test class checks the security functions for detecting tampering data manipulation in the transfer from the vehicle software to the security module. Data protection is required by FDP_ITT.5 for the transfer between physically separate parts of the TOE. This secusity feature also applies to the recognition of clearance records during processing and storage in the vehicle. The TOE, with FDP_DAU.1 has the ability to create evidence, used to verify the validity of the data. The protection of the integrity of the data stored in the vehicle is required by FDP_SDI.1 and directly addresses random manipulations of the data. The FDP_ITT.5, FDP_DAU.1 and FDP_SDI.1 requirements together provide support for data authenticity and integrity.

- Fault tolerance. This test class checks the security functions for data availability for the transfer of the clearance blocks from the vehicle software to the security module, even in case of loss within the primary memory of the software. The operation of transferring such data with the aid of a secondary memory after the loss of data in the primary memory is performed by the TOE as established by FRU_FLT.1

All tests performed by independent evaluators generated positive results.

11.3 Vulnerability analysis and penetration tests

For the execution of these activities the same test environment already used for the activities of the functional tests has been used (see. par. 11.1)

From the analysis of the Security Target [TDS], the only modules belonging to the TOE that can be the target of direct attack are the following (see also Figure 1):

- ID-TAG (a chip installed on a waste bin);
- CLEARANCE DATA MODULE (the part of software installed on the vehicle computer that transmits the ID-TAG with additional data to the central server);
- SECURITY MODULE (the part of the software on the central server that receives the ID-TAG and additional information).

So, the analysis of vulnerabilities has been focused on the interfaces and communication channels of the various modules, in particular:

- interface between ID-TAG and TAG reader;
- GPRS connection;
- OPENVPN management connection;
- public IP address of the server.

In a first phase, the evaluators have carried out research using various sources of public domain, such as the Internet, books, specialist publications, conference proceedings, etc., in order to identify any known vulnerabilities applicable to types of products similar to the TOE; in this research the Linux 4.4.x operating system installed on board the vehicle has been also considered. Several potential vulnerabilities have thus been identified.

In a second phase, the evaluators examined the evaluation documents (Security Target, functional specifications, User Manual) and used automatic scanning tools (OPENVAS and NMAP), in order to highlight any further potential vulnerabilities of the TOE. From this analysis, the evaluators determined the presence of other potential vulnerabilities.

Then, the evaluators analyzed in detail the potential vulnerabilities identified in the two previous phases, to verify their effective exploitation in the operating environment of the TOE. This analysis led to identify some actual potential vulnerabilities.

The evaluators then designed possible attack scenarios, with potential for attack Basic, and penetration tests to verify the exploitability of such potential candidate vulnerabilities, describing them with sufficient detail for their repeatability.

From the execution of the penetration tests, the evaluators have effectively found that no attack scenario with Basic potential can be successfully completed in the operating environment of the TOE as a whole. Therefore, none of the previously identified potential vulnerabilities can actually be exploited. Moreover, no residual vulnerabilities have been identified, i.e. vulnerabilities that, although not exploitable in the operating environment of the TOE, could be exploited only by attackers with attack potential higher than Basic.