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

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

Arco40 evo v. 1.0

OCSI/CERT/TEC/05/2017/RC

Versione 1.0

30 gennaio 2018

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	30/01/2018

2 Indice

3 Elenco degli acronimi

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

ODV Oggetto della Valutazione

PP Profilo di Protezione

RFID Radio Frequency IDentification

RFV Rapporto Finale di Valutazione

SAR Security Assurance Requirement

SFR Security Functional Requirement

SW Software

TDS Traguardo di Sicurezza

TOE Target of Evaluation

TSF TOE Security Functionality

TSFI TOE Security Functionality Interface

WBIS Waste Bin Identification System

4 Riferimenti

[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 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su http://www.sogisportal.eu.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia indicati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL 2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su http://www.commoncriteriaportal.org.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "RFID Identification and Geolocation system for waste collection - Arco40 evo v. 1.0", nome abbreviato "Arco40 evo v. 1.0", sviluppato dalla società Altares s.r.l.

L'ODV "Arco40 evo v. 1.0" è un Sistema di identificazione per contenitori di rifiuti (WBIS), che consente di identificare i contenitori per mezzo di un'etichetta (ID-TAG): ad es. un chip elettronico che viene indicato come transponder.

Lo scopo di questo tipo di sistemi è quello di contare la frequenza con cui i contenitori di rifiuti sono stati svuotati per consentire la fatturazione e la valutazione delle tariffe per la gestione dei rifiuti stessi.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL1, con aggiunta di ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione riassume l'esito della valutazione di sicurezza del prodotto "Arco40 evo v. 1.0" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

I potenziali acquirenti sono quindi tenuti a consultare il presente Rapporto di Certificazione congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	Arco40 evo v. 1.0
Traguardo di Sicurezza	"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.
Livello di garanzia	EAL1 con aggiunta di ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2
Fornitore	Altares s.r.l.
Committente	Altares s.r.l.
LVS	Technis Blu s.r.l.
Versione dei CC	3.1 Rev. 5
Conformità a PP	PP - Waste Bin Identification Systems (WBIS-PP Version 1.04), BSI-PP-0010-2004, [WBIS-PP]
Data di inizio della valutazione	11 luglio 2017
Data di fine della valutazione	11 gennaio 2018

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "Arco40 evo v. 1.0" è un Sistema di identificazione per contenitori di rifiuti (WBIS), che consente di identificare i contenitori per mezzo di un'etichetta (ID-TAG): ad es. un chip elettronico che viene indicato come transponder (vedi Figura 1).

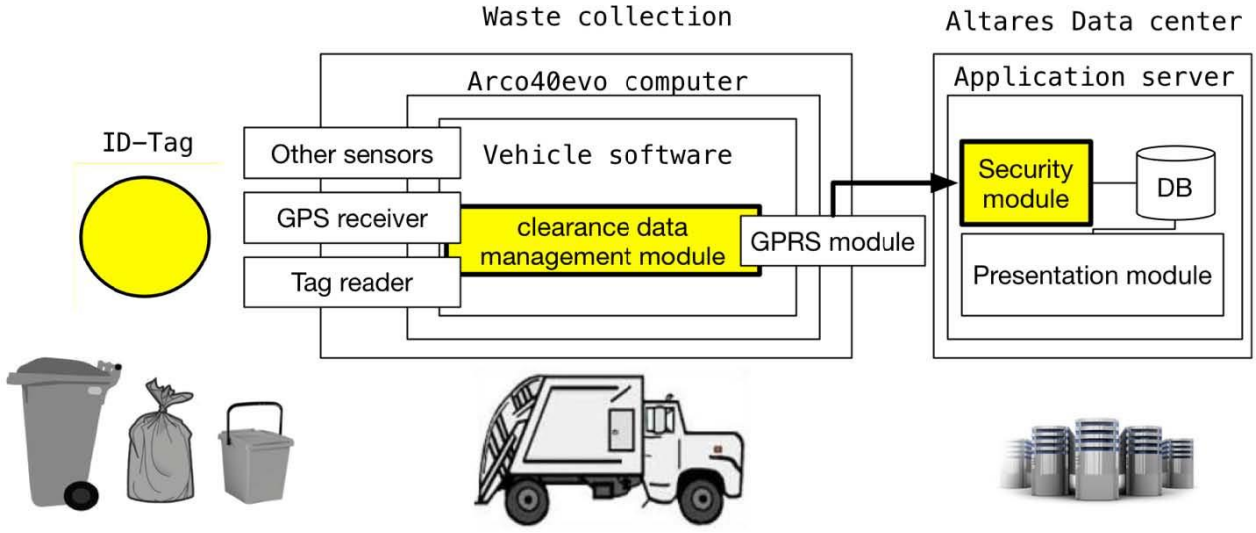

Figura 1 – L'ODV "Arco40 evo v. 1.0" (Waste Bin Identification System)

Lo scopo di questo tipo di sistemi è quello di contare la frequenza con cui i contenitori di rifiuti sono stati svuotati per consentire la fatturazione e la valutazione delle tariffe per la gestione dei rifiuti stessi.

Ogni contenitore di rifiuti è dotato di un supporto dati (ID-TAG), che memorizza i dati utilizzati per l'identificazione del contenitore. Questi dati sono unici e non confidenziali. Di solito c'è una corrispondenza uno a uno tra una serie di dati di identificazione e l'utente (persona fisica, società commerciale o organizzazione) cui verrà addebitato il costo. I dati di identificazione vengono letti da parte del modulo "READER" durante (o prima/dopo) lo svuotamento del contenitore. In questa fase sono rilevati possibili malfunzionamenti durante il trasferimento ed eventuali manipolazioni. I dati di identificazione vengono quindi trasmessi al software del veicolo, che li integra aggiungendo:

- Data e ora della lettura dell'ID-TAG (ottenuta dall'orologio del computer del veicolo sincronizzato con il ricevitore GPS);
- Posizione GPS del veicolo durante la lettura dell'ID-TAG;
- Identificatore univoco ID veicolo;
- Numero identificativo di ciascuno svuotamento (un contatore di letture valide per l'ID del veicolo).

e quindi con tutti questi dati crea un "CLEARANCE DATA RECORD".

I record così creati vengono trasmessi dal modulo "CLEARANCE DATA MANAGEMENT" al "SECURITY MODULE" nel server centrale dell'applicazione. Il modulo CLEARANCE DATA MANAGEMENT garantisce mediante misure adeguate (ad es. Backup dei dati) che il trasferimento sia possibile anche dopo una perdita di dati nella memoria primaria.

Il SECURITY MODULE garantisce il rilevamento di possibili malfunzionamenti durante il trasferimento e ritrasmette i record eventualmente non trasmessi fino al completamento della trasmissione stessa.

Tutti i CLEARANCE DATA RECORD sono trasmessi a sistemi esterni (ad esempio delle autorità comunali) per il processo di fatturazione. Oltre alla funzionalità di fatturazione, tali sistemi esterni possono fornire funzionalità aggiuntive (ad esempio evitare l'uso improprio di eventuali record ripetuti, ecc.) per integrare le funzionalità di sicurezza dell'ODV.

L'ODV consente di certificare che il flusso di dati dall'ID-TAG al software del veicolo e al server centrale dell'applicazione è sicuro durante l'intero processo.

7.3.1 Architettura dell'ODV

L'ODV è costituito da un ID-TAG, dal modulo CLEARANCE DATA MANAGEMENT, incluso nel software del veicolo, e dal SECURITY MODULE (moduli evidenziati in giallo in Figura 1). Tutti gli altri componenti non fanno parte dell'ODV ma dell'ambiente operativo. L'ODV ha un'interfaccia esterna verso le memorie del computer del veicolo, un'interfaccia logica interna tra l'ID-TAG e il software del veicolo, un'interfaccia logica interna tra il software del veicolo e il SECURITY MODULE e un'interfaccia esterna tra il SECURITY MODULE e il software del server centrale. Il canale fisico dall'ID-TAG al software del veicolo e da questo al SECURITY MODULE non fa parte dell'ODV. Ulteriori interfacce, in particolare verso i centri di fatturazione, non fanno parte della valutazione. Anche il DB e il modulo di presentazione nel software applicativo non fanno parte dell'ODV.

Per una descrizione dettagliata dell'ODV, consultare la sezione 1.4 del Traguardo di Sicurezza [TDS]. In particolare, l'ambito fisico dell'ODV è descritto nel par. 1.4.2 e l'ambito logico nel par. 1.4.3.

7.3.2 Caratteristiche di Sicurezza dell'ODV

Le principali funzionalità di sicurezza dell'ODV sono le seguenti:

- **Recognition of invalid identification data**: l'ODV riconoscerà la manipolazione dei dati di identificazione memorizzati nell' ID-TAG o durante il trasferimento dall'ID-TAG al modulo READER nel veicolo.

- **Recognition of invalid clearance data records**: l'ODV riconoscerà qualsiasi tentativo di trasferire CLEARANCE DATA RECORD arbitrari (cioè non validi) al SECURITY MODULE. L'ODV riconoscerà eventuali manipolazioni dei dati durante i processi di elaborazione e di memorizzazione all'interno del veicolo o quelle causate da blocchi casuali durante il trasferimento dal software del veicolo al SECURITY MODULE.

- **Fault tolerance**: il software del veicolo come parte dell'ODV garantirà che i dati dei CLEARANCE DATA RECORD siano protetti da un salvataggio ridondante dei dati stessi in una memoria secondaria in modo tale che il trasferimento dal software del veicolo al SECURITY MODULE sia possibile anche nel caso in cui i dati siano andati perduti nella memoria principale del software del veicolo.

- **Automatic retransmission**: l'ODV verificherà se i dati non sono stati correttamente ricevuti dal SECURITY MODULE e li recupererà ripetendo la trasmissione dei dati.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, che viene fornita al cliente finale insieme al prodotto, contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione (PP)

Il Traguardo di Sicurezza [TDS] dichiara stretta conformità al seguente Profilo di Protezione (PP):

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

Sebbene il Profilo di Protezione [WBIS-PP] sia stato certificato con la versione 2.1 dei Common Criteria, il Traguardo di Sicurezza [TDS] dichiara conformità alla versione 3.1 R5, che fornisce le stesse o maggiori garanzie.

La definizione del problema di sicurezza nel Traguardo di Sicurezza è strettamente conforme alla definizione del problema di sicurezza nel Profilo di Protezione, poiché:

- le minacce nel TDS sono identiche alle minacce nel PP;
- le ipotesi nel TDS sono identiche alle ipotesi del PP;
- le Politiche di sicurezza organizzative nel TDS sono identiche a quelle nel PP.

Gli obiettivi di sicurezza per l'ODV nel TDS sono identici agli obiettivi di sicurezza nel PP.

Gli obiettivi di sicurezza per l'ambiente operativo nel TDS sono identici agli obiettivi di sicurezza per l'ambiente nel PP.

I requisiti di sicurezza SFR sono gli stessi indicati nel PP.

Inoltre, poiché il livello di garanzia di PP contiene requisiti di garanzia diversi da quelli forniti dalla versione corrente dei Common Criteria, il livello di garanzia EAL1, con aggiunta di ASE_SPD.1, ASE_OBJ.2 e ASE_REQ.2, consente di verificare che il problema di sicurezza sia realmente affrontato dall'ODV e dal suo ambiente operativo.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Tutti gli SFR sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2]. In particolare, poiché il TDS dichiara stretta conformità al PP [WBIS-PP], è incluso anche il seguente componente esteso definito in tale PP e precisamente: FDP_ITT.5 Internal transfer integrity protection.

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS Technis Blu s.r.l.

L'attività di valutazione è terminata in data 11 gennaio 2018 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 23 gennaio 2018. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS Technis Blu s.r.l. e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "Arco40 evo v. 1.0" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL1, con aggiunta di ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL1, con aggiunta di ASE_SPD.1, ASE_OBJ.2 and ASE_REQ.2.

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

Tabella 1 – Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 - Dichiarazione di certificazione.

Si raccomanda ai potenziali acquirenti del prodotto "Arco40 evo v. 1.0" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte nel TDS.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata, descritta in Appendice B – Configurazione valutata, le cui modalità di installazione e configurazione sono descritte nel documento "Arco40 evo Manuale Utente" [MAN], fornito insieme all'ODV.

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

I documenti di guida rilevanti ai fini della valutazione o referenziati all'interno dei documenti prodotti e disponibili ai potenziali utilizzatori dell'ODV, sono i seguenti:

- [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 particolare, il Manuale Utente [MAN] contiene tutte le informazioni necessarie all'installazione, all'uso e alla manutenzione di un sistema Arco40evo per la lettura e la geolocazione degli svuotamenti nei sistemi di raccolta rifiuti. Tale documento è indirizzato sia agli installatori che devono mettere in esercizio il sistema, sia ai tecnici di servizio e manutenzione che eseguono analisi di errori o procedono alla sostituzione di componenti.

10 Appendice B – Configurazione valutata

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con il numero di versione 1.0. Il nome e il numero di versione identificano univocamente l'ODV e l'insieme dei suoi componenti, costituenti la configurazione valutata dell'ODV, verificata dai Valutatori all'atto dell'effettuazione dei test e a cui si applicano i risultati della valutazione stessa.

I componenti della configurazione valutata sono elencati dettagliatamente nella Lista di Configurazione, fornita dallo sviluppatore ai Valutatori nel documento [CONF].

Qui di seguito i componenti sono riportati sinteticamente, distinguendo tra quelli del computer del veicolo (Tabella 2) e quelli del server remoto (Tabella 3).

COMPUTER DEL VEICOLO		
	TIPO	**COMPONENTI**
ODV		/opt/arco40evo/arco40evo
AMBIENTE	Solaris BSP	BSP (Board Support Package) Altares 1.0 GSPD Demone gestione GPS 3.16 Digium QT 5.5 SQLite 3.10
	Sistema Operativo	Linux 4.4
	Hardware	CPU Atmel SAMA5D36 – Cortex A5 536 MHz Memoria RAM 256MB DDR2 NAND Flash 256 MB Micro SD 2GB Modem GPRS Bluetooth 2.0 I/O Digitale isolato 3 x RS232 1 x RS485 1 x CAN BUS Porta display RGB GPS

Tabella 2 – Componenti del computer del veicolo

SERVER REMOTO		
	TIPO	**COMPONENTI**
ODV		/opt/altares/arco40evo/sync/Arco40EvoSync
AMBIENTE		Digium QT 5.3 MySQL server5.5.58 PHPMyAdmin 4.2.12deb2+deb8u2 Apache web server 2.3.10 (Debian) con estensione PHP5 mysql 5.5.58 PHP 5.6.30-0+deb8u1 (cli)
	Sistema Operativo	Linux Debian Jessie 8.10 x64 con kernel 3.16.0-4-amd64
	Hardware	Server SMART su cloud Aruba Hypervisor: vmware vSphere CPU: 1 Core intel Xeon E5-2650L v4 RAM: 1GB HDD: 20GB SSD Storage

Tabella 3 – Componenti del server remoto

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL1 con l'aggiunta di ASE_SPD.1, ASE_REQ.2, ASE_OBJ.2, tali attività non prevedono l'esecuzione di test funzionali da parte del Fornitore, ma soltanto test funzionali indipendenti da parte dei Valutatori.

11.1 Configurazione per i Test

Per l'esecuzione dei test è stato predisposto un apposito ambiente di test presso la sede dell'LVS con il supporto del Committente/Fornitore, che ha fornito le risorse necessarie.

Prima dell'esecuzione dei test l'ODV è stato installato e configurato seguendo le indicazioni contenute nel documento "Arco40 evo Manuale Utente" [MAN], come indicato in Appendice A – Indicazioni per l'uso sicuro del prodotto, e tenendo in conto le informazioni riportate nel Traguardo di Sicurezza [TDS] e nella Lista di Configurazione [CONF].

11.2 Test funzionali indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI.

Nella predisposizione del programma dei test indipendenti da effettuare sull'ODV, i Valutatori hanno esaminato le funzioni di sicurezza dell'ODV, così come rappresentate nel Traguardo di Sicurezza [TDS] e, sulla base della loro esperienza, hanno predisposto un insieme di test, con l'obiettivo di verificare l'adeguatezza delle funzioni di sicurezza dell'ODV, nel rispetto di quanto previsto dalla CEM.

In particolare, i test di funzionalità pianificati e svolti dall'LVS sono stati mirati a verificare le seguenti funzionalità di sicurezza dell'ODV:

- Recognition of invalid identification data. Questa classe di test verifica le funzioni di sicurezza per l'individuazione di manipolazioni dei dati di identificazione dei record di svuotamento all'interno dell'unità di identificazione e mentre vengono trasferiti fra l'unità di identificazione ed il software del veicolo. La protezione dell'integrità dei dati di identificazione è richiesta da FDP_SDI.1 e contrasta direttamente manipolazioni casuali di questi dati. La protezione dell'integrità dei dati è richiesta da FDP_ITT.5 per il trasferimento dei dati fra parti fisicamente separate dell'ODV. Assicurando l'integrità dei dati, si proteggono anche i dati stessi da manipolazioni durante il trasferimento.

- Recognition of invalid clearance data records. Questa classe di test verifica le funzioni di sicurezza per l'individuazione di manipolazioni dei dati di svuotamento nel trasferimento dal software del veicolo al modulo di sicurezza. La protezione dei dati è richiesta da FDP_ITT.5 per il trasferimento fra parti fisicamente separate dell'ODV. Questa funzionalità di sicurezza riguarda anche il riconoscimento di record di svuotamento durante l'elaborazione e la memorizzazione nel veicolo. L'ODV, con FDP_DAU.1 ha la capacità di creare evidenze, utilizzate per verificare

la validità dei dati. La protezione dell'integrità dei dati memorizzati nel veicolo è richiesta da FDP_SDI.1 e contrasta direttamente manipolazioni casuali dei dati. I requisiti FDP_ITT.5, FDP_DAU.1 and FDP_SDI.1 realizzano unitamente il supporto per l'autenticità e l'integrità dei dati.

- Fault tolerance. Questa classe di test verifica le funzioni di sicurezza per la disponibilità dei dati per il trasferimento dei blocchi di svuotamento dal software del veicolo al modulo di sicurezza, anche nel caso di perdita all'interno della memoria primaria del software. L'operazione di trasferimento dei suddetti dati con l'ausilio di una memoria secondaria dopo la perdita dei dati nella memoria primaria viene realizzata dall'ODV come stabilito da FRU_FLT.1.

Tutti i test indipendenti eseguiti dai Valutatori hanno dato esito positivo.

11.3 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali (cfr. par. 11.1).

Dall'analisi del Traguardo di Sicurezza [TDS], i soli moduli, appartenenti all'ODV, che possono essere oggetto di attacco diretto, sono i seguenti (vedi anche Figura 1):

- ID-TAG (un chip installato su un contenitore dei rifiuti);
- CLEARANCE DATA MODULE (la parte di software installato sul computer del veicolo che trasmette al server centrale l'ID-TAG corredato dai dati aggiuntivi);
- SECURITY MODULE (è la parte del software nel server centrale che riceve gli ID–TAG e le informazioni aggiuntive).

In particolare l'analisi delle vulnerabilità è stata focalizzata sulle interfacce e sui canali di comunicazione dei diversi moduli, in particolare:

- interfaccia tra ID-TAG e TAG reader;
- connessione GPRS;
- connessione OPENVPN di management;
- indirizzo IP pubblico del server.

In una prima fase, i Valutatori hanno effettuato delle ricerche utilizzando varie fonti di pubblico dominio, quali internet, libri, pubblicazioni specialistiche, atti di conferenze, ecc., al fine di individuare eventuali vulnerabilità note applicabili a tipologie di prodotti simili all'ODV; in questa ricerca è stato considerato anche il sistema operativo Linux 4.4.x installato a bordo del veicolo. Sono state così individuate diverse vulnerabilità potenziali.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (Traguardo di Sicurezza, specifiche funzionali, Manuale Utente) ed utilizzato strumenti di scansione automatica (OPENVAS e NMAP), al fine di evidenziare eventuali ulteriori vulnerabilità potenziali dell'ODV. Da questa analisi, i Valutatori hanno determinato la presenza di altre vulnerabilità potenziali.

I Valutatori hanno quindi analizzato nel dettaglio le potenziali vulnerabilità individuate nelle due fasi precedenti, per verificare la loro effettiva sfruttabilità nell'ambiente operativo dell'ODV. Quest'analisi ha portato a individuare alcune effettive vulnerabilità potenziali.

I Valutatori hanno quindi progettato dei possibili scenari di attacco, con potenziale di attacco Basic, e dei test di intrusione per verificare la sfruttabilità di tali vulnerabilità potenziali candidate, descrivendoli con un dettaglio sufficiente per la loro ripetibilità.

Dall'esecuzione dei test di intrusione, i Valutatori hanno effettivamente riscontrato che nessuno scenario di attacco con potenziale Basic può essere portato a termine con successo nell'ambiente operativo dell'ODV nel suo complesso. Pertanto, nessuna delle vulnerabilità potenziali precedentemente individuate può essere effettivamente sfruttata. Non sono state individuate neanche vulnerabilità residue, cioè vulnerabilità che, pur non essendo sfruttabili nell'ambiente operativo dell'ODV, potrebbero però essere sfruttate solo da attaccanti con potenziale di attacco superiore a Basic.