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. 6/15

(Certification No.)

Prodotto: *(Product)* **Sottosistema Lettura Targhe (SLT) v1.0**

Sviluppato da: *(Developed by)* **Kapsch TrafficCom S.r.l.**

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

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 24 novembre 2015

Common Criteria

SOGIS

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

Sottosistema Lettura Targhe (SLT) v1.0

OCSI/CERT/TEC/01/2014/RC

Versione 1.0

24 novembre 2015

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	24/11/2015

2 Indice

3 Elenco degli acronimi

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

COTS Commercial Off The Shelf

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

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

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

4 Riferimenti

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

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

[CCRA-2000] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, May 2000

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[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] Lista di Configurazione Sottosistema SLT, v1.1, 28 settembre 2015

[MAN] Manuale Utente Sottosistema SLT, v1.0, 25 agosto 2015

[RF1] Capitolato speciale di appalto Progetto Vi.So.Re Trevigiano

[RFV] Rapporto Finale di Valutazione dell'ODV "Sottosistema Lettura Targhe (SLT) v1.0", v1.0, 30 ottobre 2015

[TDS] Security Target del "Sottosistema Lettura Targhe (SLT) v1.0", v2.3, 30 settembre 2015

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 assurance indicati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La nuova versione 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).

I certificati rilasciati prima dell'8 settembre 2014 sono ancora riconosciuti secondo le regole del precedente accordo [CCRA-2000], cioè fino al livello EAL 4 (e ALC_FLR). Queste stesse regole del CCRA-2000 si applicano ai processi di certificazione in corso alla data dell'8 settembre 2014, come pure al mantenimento e alla ri-certificazione di vecchi certificati, per un periodo di transizione fino all'8 settembre 2017.

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.

Poiché il prodotto certificato è stato accettato nel processo di certificazione prima dell'8 settembre 2014, il presente certificato è riconosciuto secondo le regole del precedente accordo [CCRA-2000], cioè per tutti i componenti di assurance indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Sottosistema Lettura Targhe (SLT) v1.0", sviluppato dalla società Kapsch TrafficCom S.r.l.

La valutazione è stata di tipo concomitante, cioè effettuata durante lo sviluppo dell'ODV, ed 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, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B 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 specifica l'esito della valutazione di sicurezza del prodotto "Sottosistema Lettura Targhe (SLT) v1.0" 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.

Il presente Rapporto di Certificazione deve essere consultato 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	Sottosistema Lettura Targhe (SLT) v1.0
Traguardo di Sicurezza	Security Target del "Sottosistema Lettura Targhe (SLT) v1.0", v2.3, 30 settembre 2015
Livello di garanzia	EAL1
Fornitore	Kapsch TrafficCom S.r.l.
Committente	Kapsch TrafficCom S.r.l.
LVS	Technis Blu S.r.l.
Versione dei CC	3.1 Rev. 4
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	28 gennaio 2014
Data di fine della valutazione	30 ottobre 2015

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 "Sottosistema Lettura Targhe (SLT) v1.0", nel seguito anche indicato semplicemente come SLT, fa parte del più ampio Progetto Vi.So.Re. Trevigiano, costituito da tre diversi sottosistemi che, integrati tra di loro, e unitamente al proprio ambiente operativo, si prefiggono l'obiettivo di rispondere ai requisiti ed alle funzioni operative previste nel Capitolato Speciale di Appalto Progetto Vi.So.Re. Trevigiano [RF1].

La Figura 1 mostra l'ambiente operativo complessivo del progetto Vi.So.Re. Trevigiano, all'interno del quale l'ODV agisce, e in particolare i tre sottosistemi che lo costituiscono:

- il sottosistema SLT, qui descritto, dedicato alla lettura delle targhe;
- il sottosistema SVC, dedicato alla Videosorveglianza Comunale;
- il sottosistema SNV, adibito all'infrastruttura dedicata di collegamento che garantisce il collegamento sicuro tra le diverse componenti dell'ODV tramite la cifratura e la separazione dei flussi dati in transito tra sistemi periferici e centrali.

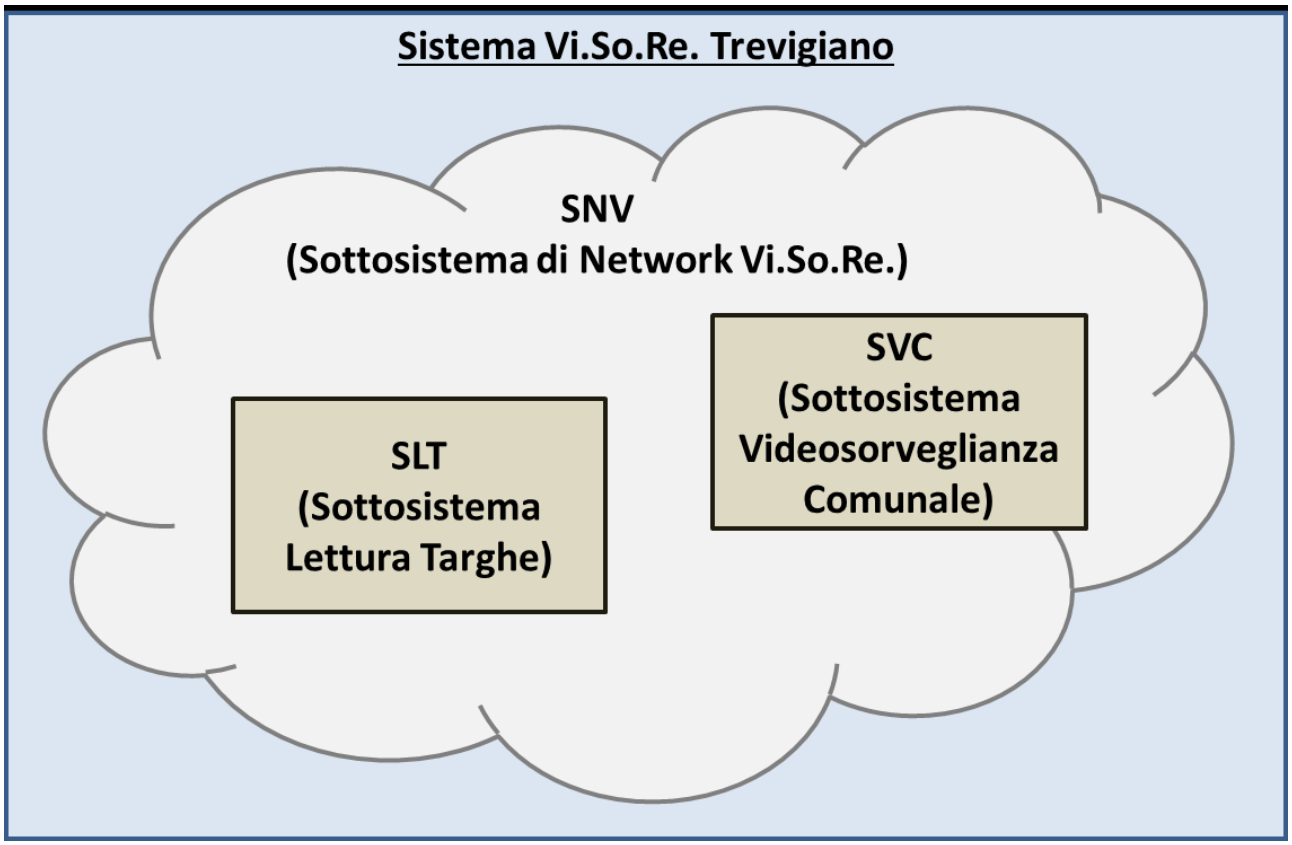

Figura 1 – Ambito del Progetto Vi.So.Re. Trevigiano

In questo ambito, l'ODV è un Sottosistema di Lettura Targhe operante lungo i principali nodi stradali nell'ambito di diversi comuni della provincia di Treviso e avente la finalità di effettuare la lettura delle targhe e rilevare l'immagine di contesto dei veicoli in transito così da consentire la segnalazione del transito alle forze di Polizia dello Stato territoriali e al Sistema Centralizzato Nazionale Targhe e Transiti (SCNTT). L'ODV prevede un certo numero di telecamere installate presso i principali nodi stradali dei comuni interessati, collegate con posti di visualizzazione/controllo e il sistema centrale di elaborazione (SCE) mediante il sottosistema di comunicazione SNV. L'ODV garantisce la riservatezza dei dati mediante la profilazione degli utenti, consentendo solo agli utenti autorizzati di accedere, 24 ore su 24, alle immagini acquisite dalle telecamere installate presso i siti identificati nei comuni interessati dal progetto Vi.So.Re. Trevigiano.

Gli obiettivi dell'ODV e del suo ambiente operativo sono quelli di effettuare la lettura automatica delle targhe e rilevare l'immagine di contesto dei veicoli in transito lungo i

principali nodi stradali delle zone interessate per consentire la segnalazione del transito dei veicoli al SCNTT, in particolare:

- invio al SCNTT della foto in B/N della targa e dei metadati collegati (numero targa, data e ora, ecc.) di tutti i mezzi in transito,
- invio al SCNTT, oltre alle informazioni di cui al primo punto, anche della foto a colori del veicolo per le targhe appartenenti alle categorie:
  - A1 (lista veicoli privi di assicurazione);
  - A2 (lista veicoli privi di revisione);
  - C (lista veicoli segnalati per furto ed altro).

7.3.1 Architettura dell'ODV

7.3.1.1 Flusso operativo delle immagini e delle informazioni correlate.

Il flusso operativo relativo all'acquisizione delle immagini parte dai sistemi su strada, dispositivi di acquisizione delle immagini (foto) composti da un unico apparato al cui interno sono assemblate diverse componenti.

All'interno dei sistemi su strada sulle foto acquisite in formato RAW al passaggio di un veicolo vengono svolte le seguenti elaborazioni locali:

- elaborazione dell'immagine B/N della targa e di quella a colori del veicolo per la creazione dei relativi file in formato standard JPEG;
- elaborazione OCR dell'immagine B/N della targa per il riconoscimento dei caratteri alfanumerici componenti la stessa;
- valorizzazione dei metadati dei due file JPEG (targa e contesto) con le informazioni di transito (data, ora, targa, id della telecamera, ecc.);
- creazione di un messaggio unico contenente entrambi i file identificati dai relativi header;
- invio dal sistema su strada alla componente server CPS del CSE del messaggio unico mediante l'apertura di una socket, con protocollo di comunicazione di tipo proprietario, mediante SNV, che garantisce la sicurezza delle comunicazioni e la separazione dai flussi rispetto a SVC.
- in assenza di collegamento di rete il messaggio unico viene memorizzato nella memoria SD locale, per essere poi trasmesso, alla riconnessione, con la modalità sopra indicata in maniera completamente trasparente all'utente e senza che l'utente possa avere accesso in alcun modo alla memoria SD.

7.3.1.2 Hardware

La descrizione dell'ambito fisico dell'ODV è fornita in [TDS], par. 2.4.1.

7.3.1.3 Software

La descrizione dell'ambito logico dell'ODV è fornita in [TDS], par. 2.4.2.

7.3.1.4 Componenti di ambiente

La descrizione delle componenti di ambiente dell'ODV è fornita in [TDS], par. 2.4.1.2.

7.3.2 Caratteristiche di Sicurezza dell'ODV

Trattandosi di una valutazione a livello di garanzia EAL1, nel Traguardo di Sicurezza [TDS] non viene descritto completamente il problema di sicurezza, ma ci si limita a definire i Requisiti Funzionali di Sicurezza (SFR), per i quali si rimanda al par. 6.3 del [TDS], gli obiettivi di sicurezza per l'ambiente operativo e le funzioni di sicurezza realizzate dall'ODV, che sono riportati qui di seguito.

7.3.2.1 Obiettivi di sicurezza per l'ambiente operativo

Gli obiettivi di sicurezza per l'ambiente operativo sono descritti in [TDS], par. 4.1.

- **OE.Admin**: gli amministratori dell'ODV devono essere scelti tra il personale fidato e addestrati al corretto utilizzo dell'ODV.
- **OE.Physical**: i responsabili del sottosistema SLT devono assicurare che l'infrastruttura tecnologica dell'ODV sia custodita in locali nei quali l'accesso è consentito solamente al personale autorizzato.
- **OE.External**: i responsabili del sottosistema SLT devono assicurare la protezione e sorveglianza agli apparati posti all'esterno.
- **OE.Crypto**: i sistemi su strada devono provvedere alla cifratura delle immagini raccolte dalle telecamere e non immediatamente trasmesse al Sistema Centralizzato di Controllo, con l'obiettivo di preservarne la riservatezza.
- **OE.Network**: il sottosistema SNV ha il compito di assicurare la connettività fra le seguenti componenti dell'ODV:
  - Sistema Centrale di Elaborazione;
  - Telecamere;
  - Utenti dell'ODV.

  Il sottosistema SNV protegge la trasmissione dei dati raccolti dalle telecamere realizzando canali cifrati e separati in base alla destinazione dei dati stessi.
- **OE.Policy**: l'organizzazione deve assicurare, per quanto di competenza, la conformità alle leggi e normative in vigore sulla privacy.
- **OE.Time**: l'ambiente operativo dell'ODV deve fornire riferimenti temporali affidabili per le operazioni sotto il controllo dell'ODV.

7.3.2.2 Funzioni di sicurezza

Le funzioni di sicurezza implementate dall'ODV sono descritte in [TDS], par. 2.7.

- **Autenticazione utenti**: l'ODV deve provvedere alla identificazione ed autenticazione degli utenti, mediante funzioni di:
  - controllo userid e password;
  - controllo della composizione delle password;
  - controllo di validità;
  - controllo di prima autenticazione;
  - controllo del numero dei tentativi di autenticazione.
- **Controllo d'accesso**: l'ODV consente agli amministratori di configurare l'accesso alle funzioni, alle telecamere ed ai dati in base al ruolo di ciascun utente.
- **Auditing**: l'ODV genera log relativi agli accessi degli utenti alle funzioni dell'ODV, sia ai tentativi positivi sia a quelli falliti (operazioni di autenticazione). L'ODV genera log relativi alla gestione delle immagini inviate dalla telecamere.
- **Gestione**: l'ODV provvede al controllo delle seguenti operazioni:
  - operazioni su ruoli e utenti;
  - operazioni sulle telecamere;

  ed all'assegnazione di un riferimento temporale affidabile per ciascuna delle operazioni suddette.
- **Protezione dati**: l'ODV garantisce la disponibilità delle immagini anche in caso di interruzione dei collegamenti fra telecamere e Sistema Centralizzato di Controllo, mediante il salvataggio delle stesse nella memoria SD delle telecamere. L'ODV provvede alla cancellazione delle immagini registrate dopo il periodo di tempo stabilito dalle politiche di accesso, nel rispetto della privacy.

7.3.3 Configurazioni dell'ODV

L'ODV valutato è identificato in [TDS] nel suo complesso come versione 1.0. Tale versione corrisponde all'ODV in esercizio al momento della chiusura delle attività di valutazione.

7.4 Documentazione

La documentazione specificata in Appendice A, 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].

7.5 Requisiti funzionali e di garanzia

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati selezionati dai CC Parte 2 [CC2] e tutti i Requisiti di Garanzia (SAR) dai CC Parte 3 [CC3].

Trattandosi di una valutazione a livello di garanzia EAL1, nel Traguardo di Sicurezza [TDS] non viene descritto completamente il problema di sicurezza, ma ci si limita a definire gli obiettivi di sicurezza per l'ambiente operativo, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza realizzate dall'ODV.

7.6 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.

L'attività di valutazione è terminata in data 30 ottobre 2015 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 12 novembre 2015. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.7 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 A. 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 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 "Sottosistema Lettura Targhe (SLT) v1.0" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL1, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B.

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.

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 for the operational environment	ASE_OBJ.1	Positivo
Stated security requirements	ASE_REQ.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 "Sottosistema Videosorveglianza Lettura Targhe (SLT) v1.0" 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 all'ambiente operativo specificato nel capitolo 4 del Traguardo di Sicurezza [TDS]. Si consiglia ai potenziali acquirenti di verificare la rispondenza ai requisiti identificati e di prestare attenzione alle raccomandazioni contenute in questo Rapporto.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata, le cui modalità di installazione e configurazione sono descritte nei documenti "Manuale Utente Sottosistema SLT, v1.0" [MAN] e "Lista di Configurazione Sottosistema SLT, v1.1" [CONF], forniti insieme all'ODV. Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto in tale documentazione.

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] Security Target del "Sottosistema Lettura Targhe (SLT) v1.0", v2.3, 30 settembre 2015
- [MAN] Manuale Utente Sottosistema SLT, v1.0, 25 agosto 2015
- [CONF] Lista di Configurazione Sottosistema SLT, v1.1

10 Appendice B – Configurazione valutata

Il nome e il numero di versione identificano univocamente l'ODV e i suoi componenti SW, costituenti la configurazione valutata dell'ODV, a cui si applicano i risultati della valutazione stessa.

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, 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, riproducendo in scala un ambiente operativo reale. In particolare, sono stati predisposti alcune telecamere di tipo IP "intelligenti", cioè capaci di rielaborare in autonomia numeri di targa, e un sistema centralizzato di controllo.

Prima dell'esecuzione dei test l'ODV è stato installato e configurato seguendo le indicazioni contenute nei documenti "Manuale Utente Sottosistema SLT, v1.0" [MAN] e "Lista di Configurazione Sottosistema SLT, v1.1" [CONF], come indicato in Appendice A.

11.2 Test funzionali ed indipendenti svolti dai Valutatori

Nella predisposizione del programma dei test indipendenti da effettuare sull'ODV, i Valutatori hanno tenuto in conto il Traguardo di Sicurezza [TDS] e le specifiche funzionali.

I Valutatori hanno quindi esaminato le funzioni di sicurezza dell'ODV, così come rappresentate nel TDS e, sulla base della propria 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 che l'ODV:

- provvede all'identificazione e all'autenticazione degli utenti (funzione di sicurezza ODV_IDAU);
- assicura il rispetto delle regole di controllo accesso su immagini e telecamere, rispetto alle funzionalità di gestione utenti e ruoli, gestione delle immagini, gestione delle telecamere (funzione di sicurezza ODV_AC);
- implementa delle funzioni che registrano nei propri log ogni operazione positiva o negativa del tipo specificato rispettando le modalità e le caratteristiche di auditing corrette ed attese (funzione di sicurezza ODV_AUD);
- applica le regole che restringono la possibilità di modificare gli attributi di sicurezza, quali ruoli, tempo di conservazione delle immagini, lista di controllo accesso (funzione di sicurezza ODV_MGMT);
- mette in campo delle funzioni atte alla protezione dei dati (funzione di sicurezza ODV_DP).

I Valutatori hanno dimostrato che l'ODV si comporta come descritto nella documentazione di progetto e che realizza i requisiti funzionali di sicurezza descritti nel TDS. L'ODV ha quindi superato con verdetto positivo la fase di test indipendenti.

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. I Valutatori hanno innanzitutto verificato che la configurazione di test fosse congruente con la versione dell'ODV in valutazione, cioè quella indicata nel [TDS], par. 2.4.

In una prima fase, i Valutatori hanno effettuato delle ricerche tramite internet al fine di individuare eventuali vulnerabilità note applicabili all'ODV, in particolare ai modelli di telecamere utilizzati e al sistema di controllo associato, con esito negativo.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza e documentazione operativa) al fine di evidenziare eventuali vulnerabilità potenziali dell'ODV. Anche da questa analisi, non sono emerse vulnerabilità potenziali.

Successivamente, è stata effettuata una ricerca di vulnerabilità di rete, utilizzando strumenti di scansione automatica; nel corso di questa attività sono state effettivamente individuate alcune vulnerabilità potenziali sulle telecamere, in particolare la presenza di alcuni servizi che potrebbero permettere ad un attaccante esperto di tentare l’accesso alla rete per poter poi eseguire dei processi sulle telecamere stesse.

I Valutatori hanno quindi progettato dei possibili scenari di attacco, con potenziale di attacco Basic, come previsto per il livello di valutazione EAL1, e dei test di intrusione per verificare la sfruttabilità delle vulnerabilità potenziali individuate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità.

Dall'esecuzione dei test di intrusione, i Valutatori hanno riscontrato che nessuno scenario di attacco con potenziale Basic può essere portato a termine con successo nell’ambiente operativo dell’ODV. Pertanto, nessuna delle vulnerabilità potenziali precedentemente individuate può essere effettivamente sfruttata. Tuttavia i servizi individuati sulle telecamere, descritti in precedenza, sono da considerarsi vulnerabilità residue, in quanto potrebbero essere sfruttate, ma solo da attaccanti con potenziale di attacco superiore a Basic, cioè quello previsto per il livello di valutazione EAL1.