Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

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. 4/16

(Certification No.)

Prodotto: **Sottosistema Network Vi.So.Re (SNV) v. 1.0**
(Product)

Sviluppato da: **Kapsch TrafficCom 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

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 20 aprile 2016

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 Network Vi.So.Re (SNV) v. 1.0

OCSI/CERT/TEC/03/2014/RC

Versione 1.0

20 aprile 2016

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	20/04/2016

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
IP	Internet Protocol
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MPLS	Multi Protocol Label Switching
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
SLT	Sottosistema di Lettura Targhe
SNV	Sottosistema Network Vi.So.Re
SVC	Sottosistema di Videosorveglianza Comunale
SW	Software
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
VPN	Virtual Private Network

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 SNV, versione 1.0, 24 febbraio 2016

[MAN] Guida Utente Sottosistema SNV, versione 1.0, 31 gennaio 2016

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

[RFV] Rapporto Finale di Valutazione dell'ODV "Sottosistema Network Vi.So.Re (SNV) v. 1.0", versione 1.1, 9 aprile 2016

[TDS] Security Target del "Sottosistema Network Vi.So.Re (SNV) v. 1.0", versione 1.3, 15 dicembre 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 Network Vi.So.Re (SNV) v. 1.0", 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 Network Vi.So.Re (SNV) 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.

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 Network Vi.So.Re (SNV) v. 1.0
Traguardo di Sicurezza	Security Target del "Sottosistema Network Vi.So.Re (SNV) v. 1.0", v1.3, 15 dicembre 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	9 aprile 2016

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 Network Vi.So.Re (SNV) v. 1.0", nel seguito anche indicato semplicemente come SNV, 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 SVC, dedicato alla Videosorveglianza Comunale;
- il sottosistema SLT, dedicato alla lettura delle targhe;
- il sottosistema SNV, qui descritto, 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.

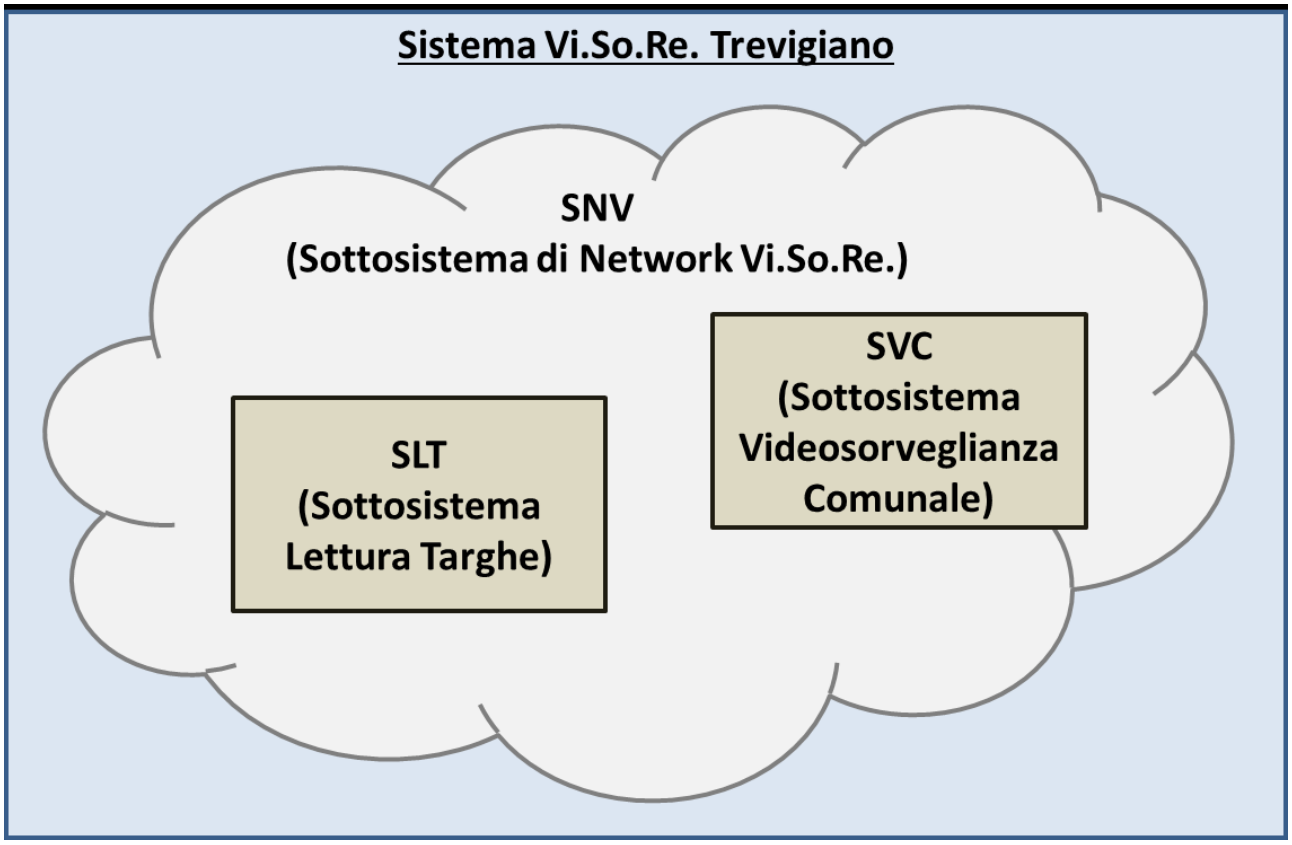

Figura 1 – Ambito del Progetto Vi.So.Re. Trevigiano

In questo ambito, l'ODV è il sottosistema del progetto Vi.So.Re. che fornisce ai sottosistemi SVC e SLT il transito protetto dei dati. Il sottosistema SNV è finalizzato ad assicurare il corretto instradamento di immagini ed informazioni provenienti da telecamere sparse sul territorio e destinate ad operatori specializzati per il loro trattamento.

SNV è costituito, per quasi tutto il suo sviluppo, da una rete in tecnologia wireless ed IP.

7.3.1 Architettura dell'ODV

7.3.1.1 Schema generale dell'ODV e servizi forniti ai sottosistemi SVC e SLT

La rete dati Vi.So.Re. è formata da tre componenti fondamentali:

- **rete di *backbone* o dorsale.**
  La rete di *backbone* è composta da una magliatura di ponti radio, su frequenza

licenziata, il cui "centro stella" è il *data center* di Oderzo, certificato ISO/IEC:27001. Per garantire i vincoli di disponibilità del servizio, si è realizzata una architettura costituita da anelli logici che sono funzionali ad una ridondanza del collegamento, in modo tale che i servizi sottesi non subiscano interruzioni nell'eventualità che un percorso di collegamento sia non disponibile. La rete è basata su logiche derivanti dal protocollo MPLS, che, rispetto ad una implementazione classica, permette di passare ad uno schema di erogazione dei servizi che in letteratura viene definito di tipo N:N (ambiente *full meshed*).

- **rete di raccolta locale geograficamente localizzata in ogni comune.**
  È la rete di distribuzione che a partire dal *backbone* si ramifica nelle varie sedi comunali servite da SLT e SVC; è realizzata tramite tecnologia wireless Hyperlan. Anche in questo caso l'architettura prevede la realizzazione di anelli logici, ove possibile.
  Per ogni sito in cui sono presenti delle telecamere, è realizzata una sottorete dedicata a SLT, incapsulata in una specifica VPN SLT, ed una sottorete dedicata a SVC, incapsulata nella specifica VPN SVC; inoltre le reti SLT e SVC sono fisicamente separate in quanto sono dedicati apparati distinti per la terminazione delle rispettive VPN. In particolare, presso il data center di Oderzo è installata una coppia di *firewall* in HA (*High Availability*) che termina le VPN SVC, mentre le VPN SLT sono terminate presso le Forze di Polizia (Questura). Le VPN SVC/SLT sono VPN IPsec AES-128.

- **rete di collegamento verso le Forze di Polizia**
  La rete di collegamento alle Forze di Polizia è realizzata da tratte su portante fisica in fibra ottica. Presso le forze di Polizia (Questura) è installata una coppia di *firewall* in HA che termina le VPN SLT.

I servizi forniti dall'ODV attraverso le sue componenti (*backbone*, raccolta locale e collegamento alle Forze di Polizia) sono costituiti dalle VPN SVC/SLT instaurate/terminate fra i *firewall* locali direttamente collegati alle telecamere e i *firewall* presso il *data center* di Oderzo e le Forze di Polizia (Questura).

La descrizione dettagliata degli schemi logici e di trasporto dei dati relativi ai sottosistemi SVC e SLT è fornita in [TDS], par. 2.3.1.

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. 2.5.

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**: L'amministrazione dell'ODV rientra nelle attività previste per la gestione del sottosistema SNV, rispettando le regole di distribuzione delle responsabilità stabilite. Tutto il personale indirettamente coinvolto nella gestione dell'ODV deve essere scelto tra personale fidato e addestrato alla corretta gestione dell'ODV.

- **OE.Physical**: i responsabili dell'ODV devono assicurare che l'infrastruttura tecnologica dell'ODV sia custodita in locali nei quali l'accesso è consentito solamente al personale autorizzato.

- **OE.Identif**: l'ambiente dell'ODV deve provvedere alla identificazione e autenticazione degli utenti Amministratore, in modo da disciplinare l'accesso alle apparecchiature del sottosistema SNV, limitandolo a utenti validi ed in base alle funzioni operative stabilite, oltre che di tenere traccia degli accessi degli utenti stessi. Devono essere implementate politiche di gestione della password (scadenza, complessità, non ripetibilità).

7.3.2.2 Funzioni di sicurezza

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

- **Secure Communication**: l'ODV garantisce la protezione del traffico dati, attraverso l'implementazione di VPN dedicate che realizzano l'indipendenza e la separazione dei flussi dei sottosistemi SVC e SLT.

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 configurazione di collaudo, come predisposto dal committente, al momento della chiusura delle attività di valutazione.

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].

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 9 aprile 2016 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 14 aprile 2016. 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 – Indicazioni per l'uso sicuro del prodotto. 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 Network Vi.So.Re (SNV) v. 1.0" 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 – 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.

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 Network Vi.So.Re (SNV) 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 all'ambiente operativo specificato nel capitolo 2.5 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 "Guida Utente Sottosistema SNV, versione 1.0" [MAN] e "Lista di Configurazione Sottosistema SNV, versione 1.0" [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 Network Vi.So.Re (SNV) v. 1.0", versione 1.3, 15 dicembre 2015
- [MAN] Guida Utente Sottosistema SNV, versione 1.0, 31 gennaio 2016
- [CONF] Lista di Configurazione Sottosistema SNV, versione 1.0, 24 febbraio 2016

10 Appendice B – Configurazione valutata

Il nome e il numero di versione identificano univocamente l'ODV e i suoi componenti HW e 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'effettuazione dei test è stato riprodotto, con l'aiuto del Fornitore, un apposito ambiente di test consistente e congruente con la descrizione dell'ODV contenuta nel Traguardo di Sicurezza [TDS].

Prima dell'esecuzione dei test l'ODV è stato installato e configurato seguendo le indicazioni contenute nei documenti "Guida Utente Sottosistema SNV, versione 1.0" [MAN] e "Lista di Configurazione Sottosistema SNV, versione 1.0" [CONF], come indicato in Appendice A – Indicazioni per l'uso sicuro del prodotto.

11.2 Test funzionali ed indipendenti svolti dai Valutatori

Nella predisposizione del programma dei test indipendenti i Valutatori hanno tenuto in conto il Traguardo di Sicurezza [TDS], le specifiche funzionali e la Guida Utente [MAN].

Per l'effettuazione dei test i valutatori hanno creato in laboratorio un ambiente di test riproducente in scala l'ambiente di produzione.

Sono stati riprodotti negli ambienti dell'LVS gli elementi salienti e coerenti degli apparati specificati, tenendo ferme le versioni di software impiegate e gli ambienti di contesto, in modo da assicurare la rispondenza dell'ambiente di test con quello di produzione, rendendo pienamente interscambiabili e ripetibili i test sia nell'ambiente di valutazione che in quello di produzione.

Nello specifico, l'ambiente SNV si compone, a livello logico di 4 elementi funzionali:

1. uno o più *firewall*;
2. elementi di trasporto di rete (*switch*, ponti radio, ecc.);
3. VPN Layer 3;
4. Il software di funzionamento e gestione installato sugli elementi 1) e 2).

I test sono stati effettuati sugli elementi 1) e 2) e 4), ovvero sugli apparati attivi ed il loro relativo software. Le postazioni di operatore sono state tenute fuori dei test e considerate parte dell'ambiente operativo. Le telecamere IP e il sistema centralizzato di controllo, installati e configurati dal Fornitore secondo le specifiche in uso nell'ambiente reale, sono stati considerati ambiente operativo, allo scopo di simulare in maniera migliore l'ambiente reale.

Il team di valutazione ha effettuato i test funzionali sulle interfacce (TSFI) esposte nel documento di Specifiche Funzionali e sui relativi parametri.

In particolare, i test di funzionalità pianificati e svolti dall'LVS sono stati mirati a verificare che l'ODV:

- assicura la profilazione nell'autenticazione;
- implementa correttamente funzionalità di VPN di tipo IPSec;
- utilizza la tipologia di VPN e i protocolli dichiarati (chiavi *pre-shared*, certificati, ecc.);
- garantisce l'isolamento *on-the-wire* tra gli ambienti SVC e SLT;
- cifra e instrada correttamente il traffico tra i diversi sottosistemi;
- applica correttamente il principio del "least privilege".

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.

L'analisi di vulnerabilità e i test di intrusione effettuati sui componenti SNV hanno riguardato i seguenti aspetti:

- vulnerabilità nell'autenticazione;
- confidenzialità della VPN di tipo IPSec;
- verifica sulla qualità crittografica delle chiavi *pre-shared* e dei certificati;
- verifica dell'isolamento *on-the-wire* tra ambienti SVC e SLT;
- verifica del reale offuscamento del traffico sul cavo;
- verifica generale dell'architettura di rete e del principio del "least privilege".

I Valutatori hanno suddiviso i test di vulnerabilità in due macro-categorie. Si è proceduto dapprima in maniera manuale, andando ad "esplorare" il sistema per scoprire le vulnerabilità eventualmente presenti. Successivamente, sono stati utilizzati strumenti automatici in grado di eseguire dei test massivi, opportunamente configurati sulla base delle risultanze dei test manuali.

Nella prima fase di test sono state ricercate vulnerabilità note sui modelli dell'hardware in uso e sul sistema di controllo associato. Non sono stati effettuati test sulle vulnerabilità del contesto, come ad esempio il sistema operativo, in quanto è stato considerato come "ambiente".

Nella fase dei test automatici sono stati effettuati il *port-scanning* degli indirizzi IP e scansioni mediante il *tool* OpenVAS, opportunamente configurato, allo scopo di rilevare eventuali esposizioni degli apparati.

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 individuate nella prima fase dei test può essere effettivamente sfruttata, posto che:

- le normali regole di sicurezza *in-depth* siano seguite nel *setup* e nel *deploy* fisico;
- le regole di *firewalling* segreghino opportunamente sulla rete di *management* l'accesso all'interfaccia degli apparati, che potrebbe esporre in futuro vulnerabilità (ad esempio DROWN attack)
- le password di gestione siano opportunamente complesse.