Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

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. 1/21

(Certification No.)

Prodotto: Primus HSM FW 2.8.21 Series E, Series X

(Product)

Sviluppato da: Securosys SA

(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:

EAL4+
(AVA_VAN.5)

Il Direttore
(Dott.ssa Eva Spina)

EVA SPINA

EVA SPINA
14 apr 2021 15:58

Roma, 14 aprile 2021

Fino a EAL2 *(Up to EAL2)*

Common Criteria

SOGIS IT SECURITY CERTIFIED

Fino a EAL4 *(Up to EAL4)*

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

Primus HSM FW 2.8.21 Series E, Series X

OCSI/CERT/CCL/04/2020/RC

Versione 1.0

14 aprile 2021

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	14/04/2021

2 Indice

3 Elenco degli acronimi

AES	Advanced Encryption Standard
AES-GCM	Advanced Encryption Standard - Galois/Counter Mode
API	Application Programming Interface
CAD	Computer Aided Design
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CNG	Cryptography API: Next Generation
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DPCM	Decreto del Presidente del Consiglio dei Ministri
DSA	Digital Signature Algorithm
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
eIDAS	Electronic IDentification, Authentication and Signature
EMS	Electronic manufacturing service
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
FW	Firmware
HSM	Hardware Security Module
HW	Hardware
ID	Identifier
IT	Information Technology
JCA/JCE	Java Cryptography Architecture / Java Cryptography Extension

KAS	Key Agreement Scheme
KDF	Key Derivation Function
KEK	Key Encryption Key
LCD	Liquid Crystal Display
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MS CSP	Microsoft Cloud Solution Provider
NIS	Nota Informativa dello Schema
NTP	Network Time Protocol
OCSI	Organismo di Certificazione della Sicurezza Informatica
PCB	Printed Circuit Board
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SAM	Signature Activation Module
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SKA	Smart Key Attributes
SO	Security Officer
SOGIS	Senior Officials Group Information Systems Security
ST	Security Target

SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	Trust Service Provider
USB	Universal Serial Bus

4 Riferimenti

4.1 Criteri e normative

[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

[eIDAS] “Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE”, Gazzetta ufficiale dell’Unione europea L 257, 28 agosto 2014

[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

4.2 Documenti tecnici

[PP] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, EN 419221-5:2018, May 2018

[LC] “Primus HSM Life-cycle support”, v1.01, Securosys SA, 16 February 2021

[RFV] “PRIMUS HSM FW 2.8.21 Series E, Series X” Evaluation Technical Report, v2, CCLab Software Laboratory, 25 March 2021

[TDS] “PRIMUS HSM Security Target”, v1.02, Securosys SA, 19 March 2021

[UG] “Primus HSM User Guide”, V2.8 Edition 08, Securosys SA, December 2020

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 https://www.sogis.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 fino a EAL4.

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 EAL2, 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 https://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 fino a EAL2.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Primus HSM FW 2.8.21 Series E, Series X", sviluppato dalla società Securosys SA, nel seguito del documento anche indicato come "Primus HSM".

L'ODV è un HSM fisicamente sicuro, ovvero un dispositivo informatico fisico che crea, protegge e gestisce chiavi digitali per firme elettroniche e altre operazioni crittografiche, con funzionalità di *toolkit* crittografico accessibili mediante diverse API (PKCS #11, JCE, CNG). L'ODV include tutti i modelli di Primus HSM delle Serie E e X.

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 e/o utilizzatori. 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 EAL4, con l'aggiunta di AVA_VAN.5, 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 specifica l'esito della valutazione di sicurezza del prodotto "Primus HSM FW 2.8.21 Series E, Series X" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori 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	Primus HSM FW 2.8.21 Series E, Series X
Traguardo di Sicurezza	"PRIMUS HSM Security Target", v1.02 [TDS]
Livello di garanzia	EAL4 con l'aggiunta di AVA_VAN.5
Fornitore	Securosys SA
Committente	Securosys SA
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	EN 419221-5:2018 [PP]
Data di inizio della valutazione	23 giugno 2020
Data di fine della valutazione	25 marzo 2021

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 "Primus HSM FW 2.8.21 Series E, Series X" (Primus HSM) è un HSM fisicamente sicuro, ovvero un dispositivo informatico fisico che crea, protegge e gestisce chiavi digitali per firme elettroniche e altre operazioni crittografiche, con funzionalità di *toolkit* crittografico accessibili mediante diverse API (PKCS #11, JCE, CNG).

L'ODV include tutti i modelli di Primus HSM delle Serie E e X (indicati anche come E-Module e X-Module, rispettivamente).

Tutti i moduli dell'ODV eseguono lo stesso firmware e differiscono solo per quanto riguarda le risorse di archiviazione e di elaborazione. Stando a quanto dichiarato dal produttore, Primus HSM soddisfa i requisiti generali di sicurezza FIPS 140-2 Livello 3 ed è stato certificato secondo questo standard.

Oltre alla gestione delle chiavi, l'ODV implementa una serie di funzioni di autenticazione e crittografiche. Primus HSM supporta algoritmi crittografici simmetrici (AES, Camellia), asimmetrici (RSA, DSA, ECC, Diffie-Hellman) e di *hashing* (SHA-2, SHA-3). Primus HSM contiene anche un *secure vault* implementato all'interno di un chip di sicurezza dedicato e offre anche protezione antimanomissione conforme a FIPS 140-2 Livello 3.

L'ODV può essere utilizzato da TSP come modulo crittografico per l'apposizione di firme o sigilli elettronici e per operazioni e servizi di autenticazione, come specificato nel Regolamento (UE) 910/2014 [eIDAS]. L'ODV può anche essere utilizzato come modulo crittografico generico, in quanto fornisce interfacce di rete ad applicazioni esterne per molte funzioni crittografiche, tra cui cifratura semplice dei dati, gestione di identità digitali, PKI, autenticazione forte e generazione e verifica di firme elettroniche.

Per una descrizione dettagliata dell'ODV, si consulti il par. 3.4 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

Le forme fisiche dell'ODV sono illustrate in Figura 1, Figura 2, Figura 3 e Figura 4. Il confine di un modulo include lo chassis e tutti gli elementi al suo interno. Non sono inclusi nei confini dell'ODV gli alimentatori rimovibili e sostituibili dell'X-Module, che fa anche uso di smart card come dispositivi di input/output esterni, per l'autenticazione dell'operatore.

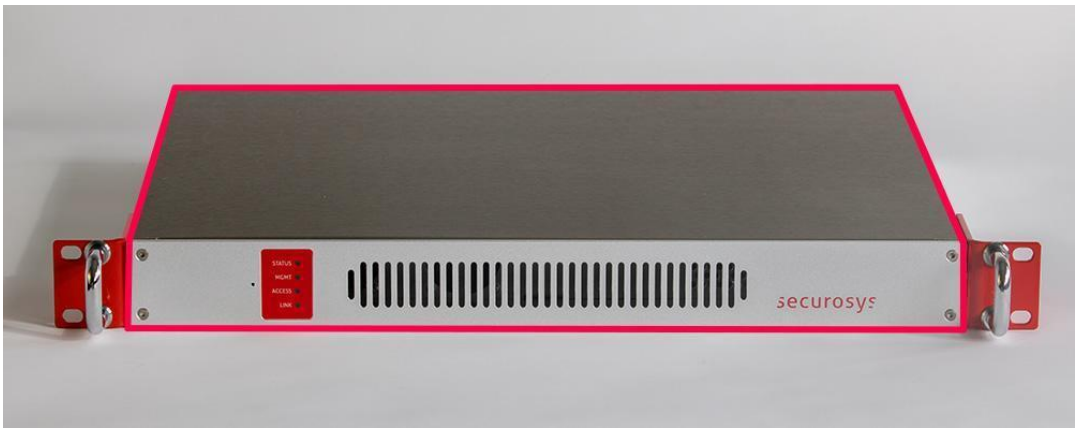

Figura 1 – Vista frontale di un E-Module con il confine crittografico in rosso

Figura 2 - Vista posteriore di un E-Module con il confine crittografico in rosso

Figura 3 - Vista frontale di un X-Module con il confine crittografico in rosso

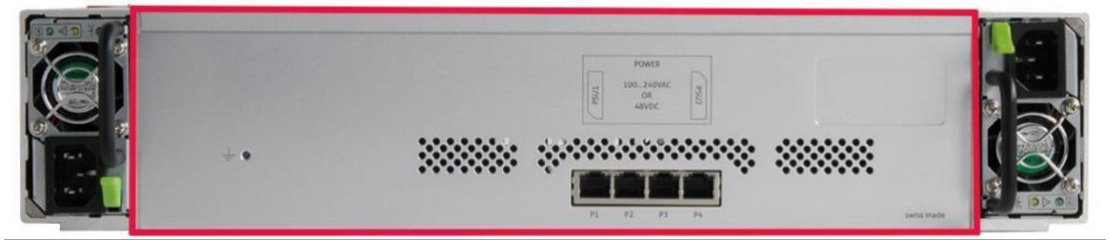

Figura 4 - Vista posteriore di un X-Module con il confine crittografico in rosso

Il confine logico dell'ODV è mostrato in Figura 5.

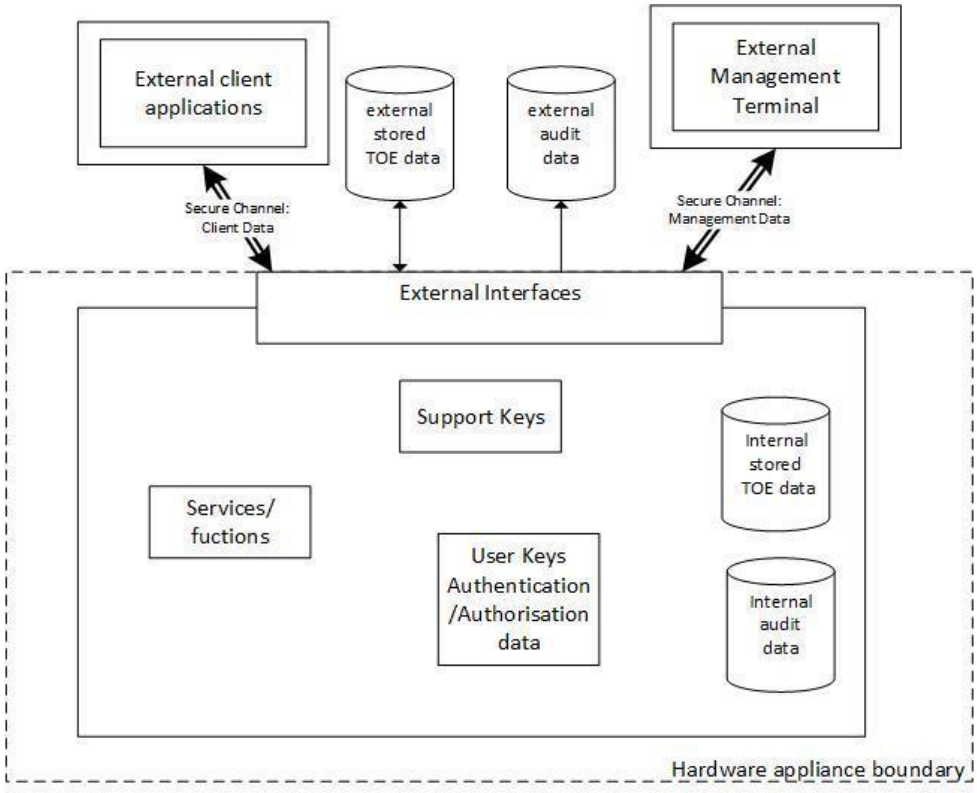

Figura 5 - Architettura dell'ODV

Il confine dell'apparato hardware in Figura 5 rappresenta l'involucro del dispositivo di elaborazione che ospita l'ODV.

L'ODV implementa autenticazione o autorizzazione separate dei seguenti tipi distinti di entità:

- amministratori dell'ODV;
- utenti applicativi delle funzioni crittografiche dell'ODV (applicazioni client esterne, autenticate mediante l'utilizzo di canali sicuri);
- utenti di chiavi segrete (il cui uso, almeno in alcuni casi, deve essere limitato ad una determinata persona fisica o giuridica).

7.3.1.1 Ruoli e funzioni disponibili

Primus HSM supporta i seguenti ruoli:

- **Genesis**: ruolo amministrativo. Configura il modulo ed effettua il ripristino di fabbrica.
- **Security Officer (SO)**: ruolo amministrativo che gestisce il modulo.
- **User** (applicazione client): utente tecnico. Questo ruolo è accessibile tramite API e fornisce funzionalità crittografiche generiche all'applicazione client.
- **Partition SO** (Partition Security Officer): ruolo amministrativo che gestisce una singola partizione.

Secondo la terminologia del PP EN 419221-5 [PP], i ruoli Genesis, SO e Partition SO sono gli amministratori dell'ODV.

L'ODV supporta applicazioni client esterne. Queste usano un canale che fornisce autenticazione degli *endpoint* e protegge la riservatezza e l'integrità dei dati trasmessi.

L'autorizzazione come utente (proprietario) di una chiave segreta, necessaria per poterla utilizzare in una funzione crittografica (o esportarla), può essere effettuata da Primus HSM mediante le chiavi SKA (Smart Key Attributes), indipendentemente da qualsiasi altra autorizzazione che potrebbe essere stata stabilita per gli amministratori o le applicazioni client. Se l'applicazione client è un SAM certificato secondo il PP EN 419241-2, è consentito l'utilizzo delle normali chiavi anche per le firme senza autorizzazione dell'utente (*key owner*) poiché in tal caso il controllo esclusivo è garantito dal SAM.

È possibile registrare più utenti (applicazioni client) nell'ODV. Ad ogni utente (applicazione client) viene assegnata una partizione separata dell'ODV, ognuna con i corrispondenti Partition Security Officer definiti.

7.3.1.2 Funzionalità non-ODV

Primus HSM include le funzioni di clonazione e *clustering* ad alta disponibilità. Tuttavia, il PP di riferimento [PP] non include per l'ODV requisiti specifici per queste funzionalità, che non fanno quindi parte dell'ODV e non rientrano nell'ambito della valutazione.

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nei capp. 4 e 5 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il cap. 9 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.2.1 Autorizzazione

L'ODV richiede che gli utenti siano identificati e autenticati prima di poter accedere a qualsiasi funzione rilevante per la sicurezza. Ci sono quattro diversi ruoli in Primus HSM: Genesis, Security Officer, Partition Security Officer e User (applicazione client). Genesis, Security Officer (SO) e Partition Security Officer (Partition SO) sono considerati gli amministratori dell'ODV. Gli utenti nel ruolo User rappresentano le applicazioni client remote che accedono all'ODV tramite le sue API.

Amministratori

Gli amministratori (Genesis, SO e Partition SO) si autenticano mediante l'uso di una smart card personale e di un PIN. In alcuni modelli di ODV (Serie E) gli amministratori utilizzano carte "virtuali", ma il processo di autenticazione/autorizzazione è lo stesso. L'operatore inserisce una carta e fornisce un PIN. Il modulo recupera e decifra il PIN corretto dalla carta e lo confronta con il PIN inserito dall'operatore. Il PIN è di 8 cifre.

È impossibile autenticarsi con questo metodo senza possedere una carta valida. Un'autenticazione fraudolenta richiederebbe lo *spoofing* di una carta. L'integrità della carta è fornita da un CRC a 32 bit calcolato sui dati interni; entrambi sono archiviati in forma cifrata con una delle chiavi della smart card. Dopo quattro tentativi errati di immissione del PIN, la smart card viene bloccata insieme al suo account di amministratore e non è possibile sbloccarla.

User

I Security Officer possono creare nuovi utenti (partizioni). A ciascuna identità appartenente a questo ruolo viene assegnata alla creazione una User Setup Password. Si tratta di una password temporanea che consiste di 25 caratteri alfanumerici, ciascuno dei quali può assumere 36 valori (A-Z, 0-9). Questa password scade dopo tre giorni per impostazione predefinita.

Dopo il primo utilizzo della User Setup Password, viene scambiato tra l'ODV e l'utente User uno User Secret che consiste in un valore casuale a 256 bit per l'autenticazione *machine-to-machine*. Lo User Secret viene utilizzato insieme al nome utente per derivare il percorso sicuro per gli utenti in modalità operativa. Per impostazione predefinita, dopo 100 tentativi di accesso all'ODV falliti entro 5 minuti, l'utente viene bloccato per 5 minuti. Questi valori sono configurabili dagli amministratori. Inoltre, vengono registrati tutti i tentativi di connessione falliti.

Key Owner

Nel caso di chiavi SKA, il proprietario della chiave è identificato mediante la sua firma digitale. Le chiavi pubbliche delle persone che possono autorizzare operazioni sulle chiavi

sono memorizzate all'interno degli attributi delle chiavi stesse. Queste possono essere diverse per le operazioni di blocco, sblocco, utilizzo e modifica delle impostazioni di autorizzazione. Ad ogni richiesta di utilizzo della chiave SKA, l'applicazione client inoltra l'autorizzazione (firma). Se la firma di autorizzazione non può essere verificata con successo per le operazioni selezionate, il richiedente l'autorizzazione viene bloccato per 5 minuti e durante questo periodo non è in grado di autorizzare alcuna chiave nell'ODV.

Ogni volta che un utente nel ruolo User tenta di utilizzare una delle sue chiavi private, gli viene richiesta una nuova autenticazione.

7.3.2.2 Gestione delle chiavi

L'ODV supporta la gestione sicura delle chiavi crittografiche necessarie per le funzioni crittografiche implementate, incluso:

- scambio di chiavi (compresa la generazione di chiavi);
- protezione delle chiavi custodite sia all'interno dell'ODV, sia esternamente (per l'uso da parte dell'ODV);
- controllo dell'accesso e dell'utilizzo delle chiavi da parte delle funzioni crittografiche interne dell'ODV;
- cancellazione delle chiavi all'interno dell'ODV.

L'ODV gestisce sia Chiavi di Sistema (*System key*), sia Chiavi Utente (*User key*).

Chiavi di Sistema

Le Chiavi di Sistema supportano l'operatività dell'ODV per quanto riguarda la cifratura del *keystore*, il backup, il supporto all'autenticazione, ecc. Alcune Chiavi di Sistema vengono generate durante la procedura guidata di configurazione e non possono essere modificate (KEK, Keystore Key, Genesis PIN, SO Card Keys, Backup Key). I PIN degli SO vengono creati durante la creazione di un nuovo SO. Le chiavi delle API vengono generate quando viene creato un nuovo utente nel ruolo User (applicazione client). Le Chiavi Utente vengono create dalle applicazioni client in modalità operativa. Le chiavi di partizione degli SO vengono generate dai Security Officer durante la creazione di nuovi utenti (nuove partizioni). Tutte queste chiavi hanno il loro formato e dimensione predefiniti.

Gli amministratori possono effettuare il backup del *keystore*, e quindi anche delle chiavi, e possono ripristinare il backup sullo stesso dispositivo o anche su altri dispositivi. Le chiavi possono essere esportate anche per l'archiviazione esterna, ma non è possibile che una chiave possa essere estratta dall'ODV in chiaro. Sia i backup, sia le chiavi *wrapped* possono uscire dall'ODV solo in formato cifrato e protetto in integrità e riservatezza. Le operazioni di backup e ripristino devono sempre essere eseguite da almeno due Security Officer per effetto del doppio controllo.

Chiavi Utente

Le Chiavi Utente vengono generate dagli utenti nel ruolo User (applicazioni client) e possono essere utilizzate per diversi scopi mediante apposite chiamate a funzioni API. Le Chiavi Utente possono essere generate, utilizzate e cancellate dagli utenti User. Gli

algoritmi, le dimensioni delle chiavi e le operazioni crittografiche supportate dall'ODV sono indicati nel par. 3.4.2.3 del Traguardo di Sicurezza [TDS] (Tabella 7).

Alle Chiavi Utente sono associati svariati attributi e funzioni, memorizzati insieme alle chiavi. Tali funzioni e attributi contengono tutte le informazioni relative alle chiavi. Ad esempio, se la chiave può essere esportata o meno, se la chiave è modificabile o cancellabile, se si tratta di una chiave privata o pubblica, ecc. Le funzioni definiscono cosa può essere fatto con le chiavi. Ad esempio, una chiave può essere utilizzata per cifrare, decifrare, firmare, ecc.

I diversi tipi di chiavi hanno i loro valori predefiniti per tutte le funzioni e *flag*, ma alcuni valori possono essere modificati al momento della creazione (non tutti, ad esempio una chiave assegnata non può mai essere estraibile).

La distruzione delle chiavi è effettuata mediante il metodo di azzeramento definito da FIPS 140-2 Livello 3.

Chiavi SKA

Le Chiavi SKA sono Chiavi Utente speciali implementate da Securosys. La funzionalità Smart Key Attributes consente un'autorizzazione granulare per l'utilizzo della chiave privata.

Le Chiavi SKA hanno proprietà di autorizzazione aggiuntive che definiscono chi può autorizzare le chiavi per scopi diversi. È possibile definire chi può bloccare/sbloccare la chiave, chi può usarla e chi può modificare le regole di autorizzazione. Con le Chiavi SKA è possibile identificare l'utente firmatario (Signer), ossia il proprietario della chiave, non l'applicazione client.

7.3.3 Funzioni crittografiche

L'ODV fornisce le seguenti funzioni crittografiche:

- generazione e verifica di firme elettroniche;
- generazione di *message digest*;
- generazione e verifica di codici di autenticazione dei messaggi;
- cifratura e decifratura (simmetrica e asimmetrica);
- generazione di chiavi;
- scambio e distribuzione di chiavi;
- derivazione di chiavi;
- generazione di valori segreti condivisi;
- supporto crittografico per password monouso e altri meccanismi di autenticazione non basati su PKI;

- generazione di numeri casuali.

L'ODV implementa le funzioni crittografiche approvate e consentite elencate nel par. 3.4.2.3 (Cryptographic Algorithms) del Traguardo di Sicurezza [TDS].

7.3.3.1 Crypto API

Primus HSM fornisce un'ampia selezione di interfacce di programmazione delle applicazioni (PKCS #11, JCA/JCE, MS CSP), potendo così essere utilizzato con quasi tutte le applicazioni aziendali per operazioni che vanno dalla semplice cifratura dei dati alla gestione delle identità, PKI, autenticazione forte, generazione e verifica di firme elettroniche.

Le operazioni crittografiche sono disponibili agli utenti nel ruolo User (applicazioni client) tramite le API menzionate in precedenza. Il ruolo User è accessibile tramite API (ad esempio, da applicazioni aziendali o client) e serve per gestire e utilizzare le Chiavi Utente. Il ruolo User può generare queste chiavi, caricarle ed eseguire operazioni crittografiche con esse.

Le Chiavi Utente, private, segrete e pubbliche sono accessibili solo se l'utente (applicazione client o, nel caso di Chiavi SKA, il proprietario della chiave) è autenticato. L'autenticazione è necessaria per ottenere la lista delle chiavi disponibili e per effettuare qualsiasi tipo di operazione con le chiavi.

La distruzione delle chiavi è effettuata mediante il metodo di azzeramento definito da FIPS 140-2 Livello 3.

7.3.3.2 Generazione di numeri casuali

Il generatore di numeri casuali (RNG) utilizzato dall'ODV è composto da due blocchi principali:

- Sorgente di entropia conforme a PTG.3, `block_cipher_df` (basato su AES 256), SP800-90Ar1.

- Generatore di numeri casuali conforme a DRG.4 con seme derivato dalla suddetta sorgente di entropia, HMAC-DRBG SP800-90Ar1 con SHA-256.

L'RNG fornisce *forward secrecy*, *backward secrecy* e *enhanced forward secrecy* come definiti nella classe DRG.4.

7.3.4 Audit e Amministrazione dell'ODV

L'ODV gestisce i seguenti ruoli: Amministratore (Genesis, SO, Partition SO) e User (applicazione client esterna).

In accordo col PP di riferimento [PP], gli utenti User proprietari delle chiavi possono essere identificati da un modulo SAM certificato esterno all'ODV o dall'ODV stesso se l'applicazione client utilizza le Chiavi SKA. Le Chiavi SKA consentono all'ODV di identificare anche il proprietario della chiave, non solo l'applicazione client.

L'SO può bloccare gli account degli utenti User (applicazioni client) mettendoli offline e sbloccarli mettendoli di nuovo online. Inoltre, una Chiave SKA può essere bloccata/sbloccata se l'utente User (proprietario della chiave) ha le regole di blocco/sblocco configurate sulla chiave specifica, ma questa operazione viene gestita dall'applicazione client; l'ODV fornisce solo le API corrispondenti.

L'ODV registra tutti gli eventi rilevanti per la sicurezza come l'avvio, l'arresto, l'autenticazione degli utenti, tutte le operazioni crittografiche e molti altri. Vengono anche registrati tutti gli errori che si verificano durante l'esecuzione di qualsiasi funzione rilevante per la sicurezza. Ogni record di audit contiene una marcatura temporale affidabile (configurazione NTP disponibile), l'ID dell'utente che ha causato l'evento e il tipo di evento. I dati di audit vengono archiviati in modo sicuro in un buffer circolare. Non viene eseguita alcuna operazione di cancellazione, ma i record più vecchi vengono sovrascritti quando la memoria dei record di audit è piena. I record di audit possono essere eliminati solo tramite il ripristino delle impostazioni di fabbrica, operazione riservata al ruolo di amministratore. Non è possibile modificare i record di audit. Gli amministratori possono esportare in qualsiasi momento i log di audit su dispositivi USB a scopo di backup. Inoltre, possono configurare un server di audit esterno (ad esempio, syslog). L'ODV può inoltrare i record di audit al server esterno mediante un canale che consente la sola comunicazione in uscita. Il server esterno non ha accesso all'ODV.

7.3.5 Canali sicuri e protezione dei dati

7.3.5.1 Canali sicuri

L'ODV utilizza un protocollo speciale per proteggere la comunicazione con le applicazioni client esterne e anche con il terminale remoto Decanus. Questo protocollo garantisce autenticazione e accordo chiave Diffie-Hellmann tra l'ODV e le entità esterne. Il protocollo che protegge la comunicazione utilizza diversi algoritmi crittografici per rendere sicuro il canale: KAS per l'accordo chiave, KDF per derivare la chiave di sessione e AES-CGM per la cifratura dei messaggi.

7.3.5.2 Protezione dell'integrità

L'integrità dei dati del TSF è protetta da un *checksum* (*hash* a 64 bit), che viene verificato prima di ogni utilizzo di una chiave. I file delle chiavi (Keyfile) includono gli attributi standard (*flag* e funzioni) e gli attributi SKA estesi (autorizzazioni). Nel caso in cui l'*hash* non corrisponda, l'operazione non può essere effettuata e l'utente User (applicazione client) viene informato che i suoi dati sono danneggiati.

Ogni volta che una chiave viene eliminata, vengono eliminati anche tutti i suoi attributi. Ogni volta che un utente User (applicazione client con la corrispondente partizione) viene eliminato, tutte le sue chiavi e i dati di configurazione vengono eliminati.

7.3.5.3 Self-test

Ad ogni accensione il modulo verifica che gli algoritmi crittografici funzionino ancora correttamente e che i dati sensibili non siano stati danneggiati (integrità). I test automatici all'accensione sono disponibili su richiesta spegnendo e riaccendendo il modulo. All'accensione, il modulo esegue molti test automatici di controllo. Verifica tutti gli algoritmi crittografici supportati (cifratura, decifratura, generazione di chiavi, verifica della firma, ecc.). Il test all'accensione esegue anche un controllo di integrità sul firmware. Tutti i test

devono essere completati con successo prima che il modulo possa utilizzare qualsiasi funzionalità crittografica. Se uno dei test fallisce, il modulo va in stato di errore. Solo dopo che i test automatici di controllo all'accensione sono stati eseguiti con successo, la rete Ethernet si attiva e l'HSM diviene disponibile per gli utenti (applicazioni client).

L'ODV effettua anche test condizionali. Questi test vengono eseguiti ogni volta che si verifica una particolare condizione.

7.3.5.4 Protezione fisica

Tutti i CSP critici memorizzati nell'HSM vengono cifrati con la Chiave di Sistema KEK. Primus HSM è fornito di sigilli antimanomissione montati in fabbrica e implementa un meccanismo di risposta antimanomissione che può azzerare la chiave KEK e il sigillo digitale in caso di violazione fisica, rendendo inutilizzabili tutte le chiavi memorizzate nell'HSM. L'ODV è anche fornito di svariati sensori per rilevare diversi tipi di attacchi di manomissione. L'ODV è protetto da attacchi fisici quali la rimozione della copertura, il rilevamento delle luci o il congelamento della memoria sia a bassa, sia ad alta temperatura. La protezione è conforme a FIPS 140-2 Livello 3.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, 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

Il Traguardo di Sicurezza [TDS] dichiara conformità *strict* al seguente Profilo di Protezione:

- EN 419221-5:2018, Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services [PP]

7.6 Requisiti funzionali e di garanzia

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

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2]. Poiché il TDS dichiara conformità *strict* al Profilo di Protezione EN 419221-5:2018 [PP], sono inclusi anche tutti gli SFR definiti in tale PP.

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, gli 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 CCLab Software Laboratory (sede di Debrecen).

L'attività di valutazione è terminata in data 25 marzo 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 30 marzo 2021. 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 CCLab Software Laboratory 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 "Primus HSM FW 2.8.21 Series E, Series X" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con aggiunta di AVA_VAN.5, 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 EAL4, con aggiunta di AVA_VAN.5.

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
Security architecture description	ADV_ARC.1	Positivo
Complete functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	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
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo

Classi e componenti di garanzia		Verdetto
Delivery procedures	ALC_DEL.1	Positivo
Identification of security measures	ALC_DVS.1	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: basic design	ATE_DPT.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Advanced methodical vulnerability analysis	AVA_VAN.5	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 "Primus HSM FW 2.8.21 Series E, Series X" 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 cap. 5.2 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 rispettivamente nel par. 4.4 e nel par. 4.5 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, in Appendice A – Indicazioni per l'uso sicuro del prodotto sono incluse una serie di raccomandazioni relative alla consegna, all'inizializzazione e all'utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([UG]).

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

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

Le fasi di consegna e le procedure necessarie per mantenere la sicurezza durante la distribuzione dell'ODV all'utente finale sono descritte nel cap. 7 del documento [LC].

I prodotti che costituiscono l'ODV sono progettati da Securosys. I prodotti hardware sono realizzati da un partner EMS (Electronic Manufacturing Service). L'EMS riceve i file CAD della documentazione di progettazione per la meccanica, il progetto della PCB (Printed Circuit Board) e la lista dei materiali necessari per la produzione. La responsabilità dell'EMS è quella di procurarsi le parti, produrre e assemblare la PCB, assemblare la meccanica e garantire la qualità.

I prodotti parzialmente assemblati vengono trasferiti in imballaggi sfusi da un fornitore di servizi logistici di fiducia dall'EMS all'area di preparazione nella sede di Securosys, dove vengono eseguiti l'assemblaggio finale, la verifica e l'accoppiamento col software sicuro.

Nel processo di preparazione viene eseguita la configurazione iniziale con software critico per la sicurezza. Il processo viene eseguito da personale verificato e in possesso di nulla osta di sicurezza, in quanto fondamentale per la sicurezza del dispositivo. Durante questa fase avviene l'assemblaggio finale del prodotto.

Dopo aver acquistato un modulo Primus HSM da Securosys SA, il cliente riceve gli elementi dell'ODV elencati in Tabella 2.

Tipo	Descrizione	Metodo di consegna
Modulo HSM	Serie E o Serie X	Corriere
Accessori	Serie E: • 1 cavo di alimentazione • 1 chiavetta USB Serie X: • 2 cavi di alimentazione • 1 chiavetta USB • 2 smart card Genesis (GN) • 3 smart card Security Officer (SO)	Corriere
Documentazione	QuickStart guide (formato PDF)	Corriere
Documentazione	User Guide (formato PDF)	Download via Web
Firmware	Primus HSM Firmware 2.8.21 (.hsm – formato di file cifrato)	Corriere (se preinstallato) o download via Web

Tabella 2 - Elementi dell'ODV consegnati al cliente

Per verificare l'integrità del dispositivo il cliente deve seguire i passaggi descritti nel cap. 3 della guida per l'utente [UG] (Setup). L'identificazione dell'ODV può essere effettuata con le seguenti misure:

- L'ODV è fisicamente etichettato in modo che il tipo di ODV (Primus HSM E o X) possa essere verificato.

- L'ODV è protetto dal sistema antimanomissione durante l'intero processo di consegna. Un'eventuale manomissione può essere verificata alla ricezione mediante ispezione visiva dei sigilli adesivi antimanomissione e convalida del sigillo digitale sul portale di assistenza di Securosys.

- Il firmware dell'ODV può essere scaricato dal portale di Securosys. Dopo l'installazione la versione del FW può essere verificata tramite console (comando `hsm_diagnostics frw`), sul pannello frontale o tramite Decanus nel menu System/Diagnostic/Firmware.

- Il cliente può convalidare il sigillo digitale come descritto nella sez. 3.1.4 guida per l'utente [UG]. Questo garantisce che il dispositivo non sia stato manomesso durante il trasporto. Dopo aver esaminato il sigillo digitale sull'ODV, per la convalida l'utente deve aprire un ticket sul portale di supporto di Securosys, specificando numero di serie e codice su una singola riga per ogni dispositivo ricevuto.

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, i seguenti documenti contengono informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- "Primus HSM User Guide", V2.8 Edition 08, December 2020 [UG]

10 Appendice B – Configurazione valutata

L'oggetto di valutazione (ODV) è il prodotto "Primus HSM FW 2.8.21 Series E, Series X", sviluppato dalla società Securosys SA. L'ODV è stato valutato nella configurazione descritta nella sez. 3.4.1 del Traguardo di Sicurezza [TDS].

L'ODV include i seguenti modelli di Primus HSM:

- Serie E: E20, E60, E150
- Serie X: X200, X400, X700, X1000

Tutti i modelli dell'ODV includono la seguente versione del firmware:

- FW 2.8.21

I vari modelli dell'ODV differiscono solo per quantità di memoria e risorse di calcolo.

I seguenti componenti HW e SW non fanno parte dell'ODV e sono esclusi dalla valutazione:

- Alimentatori (X-Module): l'alimentazione non è considerata rilevante per la sicurezza.
- Decanus - Remote access Terminal: terminale di amministrazione remota utilizzato da Primus HSM.

10.1 Modalità operative dell'ODV

L'ODV può funzionare in tre diverse modalità operative:

- Normal
- FIPS 140-2
- Restricted

Ciascuna modalità e le sue caratteristiche sono descritte nella sez. 3.2.1. della guida per l'utente [UG]. Nella configurazione valutata, l'ODV deve essere impostato sulla modalità Normal o FIPS durante la configurazione iniziale. La modalità Restricted non è stata valutata e non deve essere utilizzata nella configurazione conforme ai CC.

Inoltre, per la conformità ai CC l'utente deve seguire le istruzioni aggiuntive e applicare le impostazioni speciali descritte nella sez. 25.1 della guida per l'utente [UG] (Appendix - Common Criteria operating instructions and conditions).

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 EAL4, con aggiunta di AVA_VAN.5, tali attività prevedono tre passi successivi:

- valutazione in termini di copertura e livello di approfondimento dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

Tutte le attività di test sono state eseguite presso la sede dell'LVS su campioni dell'ODV messi a disposizione dei Valutatori dal Fornitore.

I Valutatori hanno ricevuto due istanze funzionali dell'ODV, una della Serie E e una della Serie X:

- PRIMUS HSM FW 2.8.21 Serie E150 in modalità operativa Normal, versione Firmware RE-2.8.21, versione Rollback V2.8.21, versione Bootloader V02.08.0000-rel.
- PRIMUS HSM FW 2.8.21 Serie X700 with operation mode normal, versione Firmware RX-2.8.21, versione Rollback V2.8.21, versione Bootloader V02.08.0000-rel.

Le funzionalità principali dei due modelli dell'ODV sono le stesse; l'unica differenza sta nelle risorse computazionali e in più la Serie X è dotata di uno schermo LCD per la configurazione.

I Valutatori hanno esaminato l'ODV e hanno verificato che fosse coerente con la configurazione in corso di valutazione, specificata nel Traguardo di Sicurezza [TDS].

I Valutatori hanno creato l'ambiente di test in base alla descrizione nel Traguardo di Sicurezza [TDS] e nella documentazione di test del Fornitore. I Valutatori hanno configurato un solo ODV Master in quanto le funzionalità di alta disponibilità e clonazione sono fuori dai confini dell'ODV e non sono incluse nella valutazione.

I Valutatori hanno verificato l'integrità dell'ODV, quindi hanno inizializzato e configurato i moduli HSM applicando le procedure di preparazione descritte in [UG] che forniscono informazioni dettagliate per l'installazione sicura dell'ODV e tutti i passaggi di configurazione necessari. I Valutatori sono stati in grado di configurare l'ODV in modo sicuro utilizzando esclusivamente le procedure preparative fornite.

Successivamente, i Valutatori hanno verificato che l'ODV fosse installato correttamente e in uno stato noto.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

Per la verifica delle funzionalità dell'ODV, il Fornitore ha eseguito test sia manuali, sia automatizzati. I test coprono tutte le TSFI e forzano l'applicazione di tutti i requisiti funzionali (SFR) dell'ODV.

Il Fornitore ha progettato casi di test automatici e manuali. I test vengono effettuati dal Fornitore mediante l'esecuzione di script di test e di un'applicazione di test. I test automatizzati possono anche essere ripetuti manualmente sulla base delle descrizioni dei casi di test.

11.2.2 Copertura dei test

I Valutatori hanno esaminato il piano di test presentato dal Fornitore e hanno verificato la completa copertura degli SFR e delle TSFI descritte nelle specifiche funzionali.

11.2.3 Risultati dei test

I Valutatori hanno eseguito i casi di test automatizzati del Fornitore sull'ambiente di test messo a disposizione dal Fornitore.

I Valutatori hanno verificato il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

I Valutatori hanno selezionato i test con l'obiettivo di verificare in profondità l'ODV e hanno creato i propri casi di test per aumentare ulteriormente le funzionalità testate, risultando in una copertura più rigorosa delle funzionalità di sicurezza dell'ODV. I Valutatori hanno anche cercato di selezionare i casi di test che coprono la maggior parte dei moduli correlati.

I Valutatori hanno eseguito le operazioni di firma elettronica e sigillo elettronico fornite dall'ODV verificando che le firme e i sigilli restituiti dall'ODV corrispondessero ai DTBS corretti.

Dato che l'ODV supporta gli aggiornamenti del software e/o del firmware, i Valutatori hanno effettuato dei test per garantire che solo gli aggiornamenti con firme digitali valide possano essere installati sull'ODV.

I risultati dei test mostrano che l'ODV si comporta come previsto. I Valutatori non hanno riscontrato deviazioni rispetto ai risultati attesi.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività i Valutatori hanno lavorato sugli stessi campioni dell'ODV già utilizzati per le attività dei test funzionali, verificando che la configurazione di test fosse congruente con la versione dell'ODV in valutazione.

I Valutatori hanno progettato test per soddisfare i requisiti di AVA_VAN.5. I Valutatori hanno basato l'analisi su una revisione del codice sorgente e hanno impiegato una strategia di *fuzzing* per testare la funzionalità di un sottoinsieme delle TSFI invece di testare tutte le interfacce.

I Valutatori hanno esaminato la documentazione del Fornitore allo scopo di individuare alcune aree di interesse e hanno quindi condotto ricerche su fonti di informazione pubbliche, identificando una serie di potenziali vulnerabilità. I Valutatori hanno verificato durante la visita al sito del Fornitore che le *patch* corrispondenti sono già state applicate e che quindi l'ODV non risulta affetto da nessuna vulnerabilità nota.

I Valutatori hanno quindi eseguito un'analisi metodica avanzata delle vulnerabilità dell'ODV utilizzando la documentazione di guida, le specifiche funzionali, i documenti di progetto dell'ODV, la descrizione dell'architettura di sicurezza e la rappresentazione dell'implementazione al fine di identificare potenziali vulnerabilità nell'ODV.

L'analisi dei Valutatori si è concentrata sui seguenti aspetti, portando all'identificazione di diverse vulnerabilità potenziali:

- *buffer overflow*;
- iniezione di codice;
- iniezione di stringhe di formato;
- iniezione di byte nulli.

I Valutatori hanno riscontrato una vulnerabilità di tipo *buffer overflow* durante l'attività di revisione del codice sorgente effettuata in occasione della visita al sito del Fornitore; questa vulnerabilità è stata prontamente corretta dal Fornitore, che ha fornito una nuova versione del firmware dell'ODV. I Valutatori hanno anche verificato la presenza di altri possibili *buffer overflow*, ma nessuno di questi è risultato sfruttabile con successo.

I Valutatori hanno esaminato il codice sorgente alla ricerca di potenziali iniezioni di codice, ma non hanno trovato casi in cui l'input dell'utente potesse raggiungere una funzione pericolosa.

I Valutatori hanno provato diversi *payload* che potrebbero rivelare vulnerabilità di tipo iniezione di stringhe di formato e hanno anche esaminato il codice sorgente, ma non hanno trovato alcun caso che potesse essere sfruttato in pratica.

Al termine di tutte le sessioni di test di intrusione svolte, i Valutatori hanno potuto concludere che nessuno scenario di attacco con potenziale High o inferiore 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.

I Valutatori hanno esaminato manualmente ulteriori porzioni del codice sorgente dell'ODV e la relativa documentazione e hanno identificato due vulnerabilità residue:

- iniezione di byte nulli con conseguente registrazione insufficiente dei log;

- Iniezione di byte nulli con conseguente impossibilità di cancellazione di alcune chiavi.

Entrambe queste vulnerabilità possono essere sfruttate solo da un attaccante con un potenziale di attacco superiore ad High.