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. 8/19

(Certification No.)

Prodotto: **nShield HSM Family v11.72.03**
(Product)

Sviluppato da: **nCipher Security Limited**
(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 Dirigente
(Dott. Antonello Cocco)

Roma, 17 settembre 2019

Common Criteria

SOGIS IT SECURITY CERTIFIED

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

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

nShield HSM Family v11.72.03

OCSI/CERT/LEO/01/2019/RC

Versione 1.0

17 settembre 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	17/09/2019

2 Indice

1 Revisioni del documento 5
2 Indice 6
3 Elenco degli acronimi 8
4 Riferimenti 10
4.1 Criteri e normative 10
4.2 Documenti tecnici 11
5 Riconoscimento del certificato 12
5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA) 12
5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA) 12
6 Dichiarazione di certificazione 13
7 Riepilogo della valutazione 14
7.1 Introduzione 14
7.2 Identificazione sintetica della certificazione 14
7.3 Prodotto valutato 14
7.3.1 Architettura dell'ODV 15
7.3.2 Caratteristiche di Sicurezza dell'ODV 18
7.4 Documentazione 21
7.5 Conformità a Profili di Protezione 22
7.6 Requisiti funzionali e di garanzia 22
7.7 Conduzione della valutazione 22
7.8 Considerazioni generali sulla validità della certificazione 22
8 Esito della valutazione 24
8.1 Risultato della valutazione 24
8.2 Raccomandazioni 25
9 Appendice A – Indicazioni per l'uso sicuro del prodotto 26
9.1 Consegna 26
9.2 Installazione e utilizzo sicuro dell'ODV 26
10 Appendice B – Configurazione valutata 28
11 Appendice C – Attività di Test 29
11.1 Configurazione per i test 29

11.2 Test funzionali svolti dal Fornitore 31
11.2.1 Approccio adottato per i test 31
11.2.2 Copertura dei test 31
11.2.3 Risultati dei test 31
11.3 Test funzionali indipendenti svolti dai Valutatori 32
11.4 Analisi delle vulnerabilità e test di intrusione 32

3 Elenco degli acronimi

ACS	Administrator Card Set
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DPCM	Decreto del Presidente del Consiglio dei Ministri
DTBS/R	Data To Be Signed / Representation
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory
FW	Firmware
HSM	Hardware Security Module
HW	Hardware
IT	Information Technology
LAN	Local Area Network
LED	Light Emitting Diode
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
NVRAM	Non-Volatile Random Access Memory
OCS	Operator Card Set
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PCIe	Peripheral Component Interconnect Express
PKI	Public Key Infrastructure
PP	Profilo di Protezione

RAM	Random Access Memory
RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCD	Signature Creation Data
SEE	Secure Execution Environment
SFR	Security Functional Requirement
SO	Sistema Operativo
SSCD	Secure Signature-Creation Device
SSH	Secure SHell
SSL	Secure Socket Layer
SVD	Signature Verification Data
SW	Software
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

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

[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

[ECG] nShield HSM family v11.72.03 Common Criteria Evaluated Configuration Guide, ASEC1382, Version 1.3, 11 June 2019

[IGC] nShield Connect Installation Guide, Version 6.0, 13 March 2015

[IGS] nShield Solo Installation Guide, Version 6.0, 13 March 2015

[RC] Rapporto di Certificazione “nShield HSM Family v11.72.02”, OCSI/CERT/RES/02/2012/RC, Versione 1.0, 10marzo 2016

[RFV] Rapporto Finale di Valutazione “nShield HSM Family v11.72.03”, ER4AA2201V12, Rev 00, 28 giugno 2019

[TDS] nShield HSM family v11.72.03 Security Target, Version 1-1, 12 August 2019

[UGCU] nShield Connect User Guide for Unix, Version 11.0, 13 March 2015

[UGCW] nShield Connect User Guide for Windows, Version 11.0, 13 March 2015

[UGSU] nShield Solo User Guide for Unix, Version 11.0, 13 March 2015

[UGSW] nShield Edge and nShield Solo User Guide for Windows, Version 11.0, 13 March 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 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 EAL 2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

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

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

Il presente certificato è riconosciuto in ambito CCRA fino a EAL2.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "nShield HSM Family v11.72.03", sviluppato dalla società nCipher Security Limited.

L'ODV è costituito da una serie di dispositivi di tipo HSM (*Hardware Security Module*) "general purpose" progettati per offrire funzionalità di elaborazione crittografica e gestione di chiavi di cifratura e di firma elettronica all'interno di un'organizzazione.

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).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV (nShield HSM Family v11.72.02), già certificato dall'OCSI (Certificato n. 1/16 del 10 marzo 2016 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore nCipher (in precedenza Thales e-Security) è stato necessario procedere a una ri-certificazione dell'ODV. L'LVS Leonardo (ex Consorzio RES) ha potuto riutilizzare parte della documentazione e delle evidenze già fornite nella precedente valutazione.

Si noti che le modifiche effettuate hanno comportato anche la revisione del Traguardo di Sicurezza [TDS]. Gli utenti della precedente versione dell'ODV sono quindi invitati a prendere visione anche del nuovo TDS.

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente ODV, per facilità di lettura il presente Rapporto di Certificazione è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo ODV "nShield HSM Family v11.72.03".

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 EAL4, con l'aggiunta di AVA_VAN.5, in conformità a quanto indicato 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 "nShield HSM Family v11.72.03" 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	nShield HSM Family v11.72.03
Traguardo di Sicurezza	nShield HSM family v11.72.03 Security Target, Version 1-1, 12 August 2019
Livello di garanzia	EAL4 con aggiunta di AVA_VAN.5
Fornitore	nCipher Security Limited
Committente	nCipher Security Limited
LVS	LVS Leonardo
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	19 febbraio 2019
Data di fine della valutazione	26 luglio 2019

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].

I dispositivi appartenenti alla "nShield HSM family", che costituiscono l'ODV, sono dispositivi di tipo HSM (*Hardware Security Module*) "general purpose" in grado di offrire funzionalità di elaborazione crittografica e gestione di chiavi per application server, SSL/TLS Web server e dispositivi di sicurezza.

La famiglia di HSM nShield consente alle aziende di aggiungere protezione hardware per sistemi critici, come le infrastrutture a chiave pubblica (PKI), sistemi di gestione delle identità, database, server Web e server di applicazioni.

La famiglia di HSM nShield mette a disposizione una serie di operazioni crittografiche che comprende cifratura e decifratura, *hashing* e autenticazione dei messaggi, generazione e verifica della firma digitale, funzioni di gestione e scambio chiavi che sono mantenute in forma sicura e il cui accesso è limitato a specifici gruppi di utenti autorizzati.

In particolare, i dispositivi della famiglia nShield sono progettati per essere utilizzati come dispositivi sicuri per la creazione di firme elettroniche (SSCD).

In Tabella 1 sono elencati i modelli dei dispositivi appartenenti a tale famiglia, facenti parte dell'ODV (con corrispondente numero di serie) ed i relativi software (con la versione corrispondente).

Modello	Numero di serie	Versioni dei componenti software
nShield Solo F3 PCIe 500+	NC4433E-500	• nCore firmware version 2.55.4 • Hardserver version 2.92.1 • Client libraries: Generic stub version 3.30.5, NFKM and RQCard version 1.86.1, and PKCS#11 version 2.14.1 • Client utilities version 2.54.1
nShield Solo F3 PCIe 6000+	NC4433E-6K0	
nShield Connect 500+	NH2054	• nCore firmware version 2.55.4, nShield Connect firmware image version 12.45.1 • Hardserver version 2.92.1 • Client libraries: Generic stub version 3.30.5, NFKM and RQCard version 1.86.1, and PKCS#11 version 2.14.1 • Client utilities version 2.54.1
nShield Connect 1500+	NH2061	
nShield Connect 6000+	NH2068	

Tabella 1 – Identificazione dei modelli della famiglia nShield

L'ODV si presenta in due varianti principali: in forma di scheda PCIe, denominata nShield Solo F3, o come apparato nShield Connect. Tutti i modelli elencati utilizzano l'acceleratore crittografico "Exar 8204". In questa ri-certificazione dell'ODV il Fornitore non ha più preso in considerazione i dispositivi che adottavano l'acceleratore crittografico "Broadcom 5825".

Inoltre, i modelli PCIe indicati sono certificati FIPS a livello 2 e livello 3, ma nella configurazione certificata viene considerata la certificazione FIPS a livello 2.

7.3.1 Architettura dell'ODV

In Figura 1 sono mostrati il modulo nShield Solo F3 PCIe (a sinistra) e l'apparato nShield Connect (a destra).

Figura 1 - Modulo nShield Solo F3 PCIe e apparato nShield Connect

La loro architettura software ed hardware è mostrata rispettivamente in Figura 2 e Figura 3.

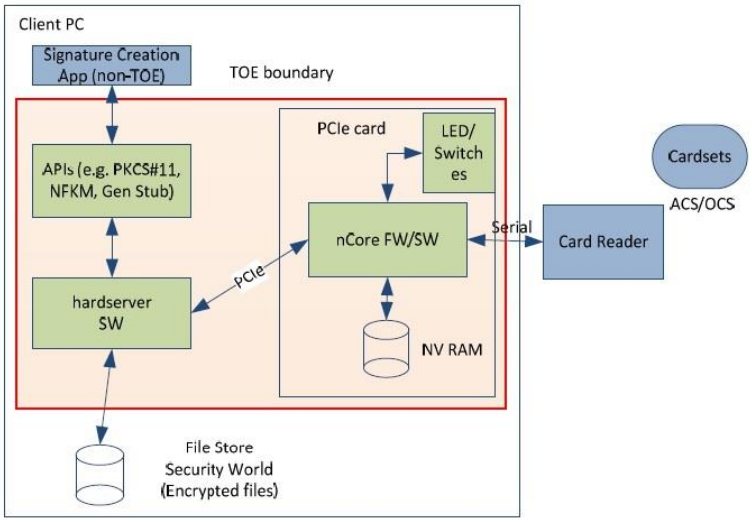

Figura 2 - Architettura del modulo nShield Solo F3 PCIe

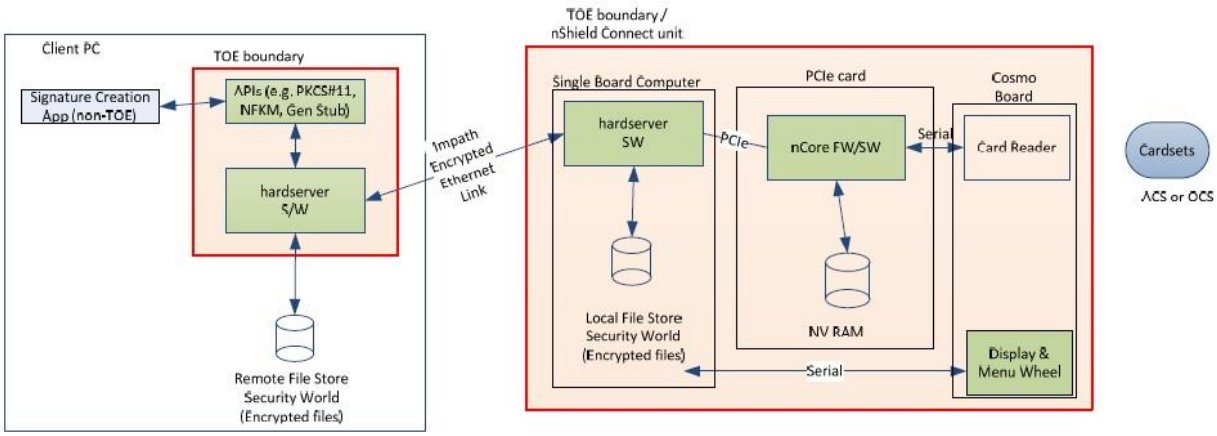

Figura 3 - Architettura dell'apparato nShield Connect

Come si può vedere da tali schemi, il dispositivo nShield Connect contiene al suo interno un modulo nShield Solo F3 PCIe.

Nell'utilizzo al di fuori del dispositivo nShield Connect, l'unità nShield Solo F3 PCIe è installata in un PC Client ed è collegata direttamente tramite un cavo seriale ad un lettore di smart card che viene utilizzato con le smart card inserite dagli amministratori e dai firmatari per autorizzare le varie operazioni (operazioni di gestione, generazione di chiavi o operazioni di firma). Il dispositivo nShield Connect, invece, ha il lettore di smart card inserito all'interno del suo involucro.

Il "Security World", che contiene, tra le altre cose, le SCD (Signature Creation Data, ovvero le chiavi private per generare la firma elettronica), viene memorizzato separatamente nella memoria persistente collegata al PC client. Questo *repository* potrebbe risiedere su un disco locale, o su un dispositivo di *storage* di rete. I dati del "Security World" vengono memorizzati in forma cifrata e il loro contenuto in chiaro è accessibile solo all'interno dell'unità nShield Solo F3 PCIe. Pertanto, la posizione in cui vengono memorizzati tali dati non influisce sulla sicurezza dell'ODV.

In particolare, nello schema di Figura 2, il PC client in cui è installato l'ODV esegue le librerie e le *utility* del client che richiedono il software *hardserver*, che a sua volta comunica con l'unità nShield Solo F3 PCIe per utilizzare suoi servizi di crittografia forniti dal *firmware* nCore. L'*hardserver* gestisce i dati del "Security World", che sono contenuti nel *repository* collegato al PC client. Tali dati sono protetti dalle chiavi presenti nella scheda PCIe. La scheda PCIe è l'unico luogo in cui le chiavi sono presenti in chiaro. Le chiavi utilizzate dalle applicazioni vengono prelevate in forma cifrata dal "Security World", passate alla scheda PCIe da parte della SCA (*Signature-Creation Application*) e quindi, una volta decifrate, vengono mantenute in chiaro nella scheda PCIe durante il loro utilizzo.

Nello schema di Figura 3, sia il PC client, sia l'unità nShield Connect eseguono istanze separate dello stesso software *hardserver*, che consente la comunicazione tra il PC client e il dispositivo nShield Connect tramite una rete sicura. La connessione tra il client e il Connect è implementata da un protocollo proprietario chiamato 'impath', che protegge la riservatezza e l'integrità dei dati. In questo caso il client *hardserver* gestisce i dati del "Security World" che si trovano nel *repository* collegato al PC client. La protezione dei dati del "Security World" mediante le chiavi presenti nella scheda PCIe si applica allo stesso modo del caso descritto per la Figura 2. Il PC client collegato a un'unità nShield Connect gestisce librerie client e *utility* client che accedono all'*hardserver* del PC client, proprio come in Figura 2. Le *utility* del client possono anche essere eseguite e comunicare con l'*hardserver* situato nell'nShield Connect (vengono eseguite sulla scheda madre dell'nShield Connect, al di fuori della scheda PCIe).

L'ODV utilizza due chiavi principali (K_{MSW} e K_{NSO}), che consentono la gestione sicura delle funzionalità di sicurezza dell'ODV, l'accesso ad ognuna delle quali è consentito solo mediante un apposito "Token" di accesso (*Logical Token*). Nel dettaglio:

- K_{MSW} (*Security World Module Key*): è la chiave di livello più alto usata per la protezione di tutti gli oggetti presenti in un "Security World" (ad eccezione della chiave K_{NSO}). Essa è conservata in modo permanente nella scheda PCIe.

- K_{NSO} (*Security Officer Key*): è la chiave utilizzata per autorizzare alcuni comandi privileggiati ed è conservata in una particolare struttura identificata con il nome di "encrypted Key Blob"

Tali chiavi sono generate durante la creazione del “Security World”.

In generale, il “Security World”, che è l’infrastruttura utilizzata per la gestione sicura del ciclo di vita delle chiavi crittografiche, è costituito da:

- uno o più nShield HSM;
- un set di smart card ACS, il cui gestore è l’amministratore, e la cui combinazione dà l’accesso alle chiavi che consentono la gestione sicura delle funzionalità di sicurezza dell’ODV (K_{MSW} e K_{NSO});
- un *repository* contenente le SCD cifrate e tutte le informazioni di supporto ad esse associate;
- opzionale: uno o più set di smart card OCS (ad ognuno di essi sarà collegata una opportuna *passphrase*, necessaria per il suo utilizzo), i cui gestori sono gli utenti firmatari;
- opzionale: una o più Softcard (ad ognuna di esse sarà collegata una opportuna *passphrase*, necessaria per il suo utilizzo), i cui gestori sono gli utenti firmatari.

Per il “Security World” generato esistono solo due ruoli (tipologie di utenti):

- Amministratore: colui che possiede il set di smart card ACS, con relativa passphrase e K_{MSW}. Esso ha anche accesso alla chiave K_{NSO} e quindi possiede anche il ruolo astratto di “Security Officer”.
- Firmatario (*Signatory*): colui che possiede i set di smart card OCS o la Softcard (con relativa *passphrase*).

7.3.2 Caratteristiche di Sicurezza dell’ODV

7.3.2.1 Politica di sicurezza

La politica di sicurezza dell’ODV è espressa dall’insieme dei Requisiti Funzionali di Sicurezza (SFR) implementati dallo stesso. Essa copre i seguenti aspetti:

- Ruoli degli Utenti e loro autenticazione
- Gestione delle chiavi
- Servizi crittografici
- Protezione dei dati dell’utente
- Protezione delle funzionalità di sicurezza dell’ODV
- Canali sicuri
- Limiti delle sessioni operative

7.3.2.2 Obiettivi di sicurezza dell'ambiente operativo

Le ipotesi definite nel Traguardo di Sicurezza [TDS] ed alcuni aspetti delle minacce e delle politiche di sicurezza organizzative non sono coperte dall'ODV stesso. Tali aspetti implicano che specifici obiettivi di sicurezza debbano essere soddisfatti dall'ambiente operativo dell'ODV. In particolare in tale ambito i seguenti aspetti sono da considerare di rilievo:

- le funzionalità di sicurezza dell'ODV sono gestite da uno o più individui competenti. Coloro che sono responsabili per la gestione dell'ODV non sono disattenti, volutamente negligenti o ostili e seguiranno e si atterranno alle istruzioni fornite dalla documentazione di guida;

- si assume che tutti i sistemi IT remoti e fidati sui quali l'ODV si basa per supportare la realizzazione della sua politica di sicurezza siano in grado di realizzare correttamente le funzioni richieste dall'ODV in modo consistente con quanto definito;

- si assume che l'ambiente operativo dell'ODV fornisca allo stesso un'appropriata sicurezza fisica, commisurata con il valore dei beni che l'ODV deve proteggere;

- si assume che tutte le connessioni da e verso sistemi IT remoti e fidati e tra parti fisicamente separate delle funzioni di sicurezza dell'ODV, non protette dalle stesse, siano fisicamente o logicamente protette all'interno dell'ambiente operativo dell'ODV per assicurare l'integrità e la confidenzialità dei dati trasmessi e per assicurare l'autenticità degli estremi della comunicazione;

- si assume che gli utenti autorizzati possiedano le necessarie autorizzazioni per accedere almeno ad alcune delle informazioni gestite dall'ODV e agiscano in maniera cooperativa in un ambiente benevolo;

- si assume che gli utenti siano sufficientemente addestrati e fidati per svolgere alcuni compiti o gruppi di compiti all'interno di un ambiente IT sicuro, esercitando il completo controllo sui loro dati utente.

Per una descrizione completa degli obiettivi di sicurezza per l'ambiente dell'ODV, si faccia riferimento al capitolo 5.2 del Traguardo di Sicurezza [TDS]

7.3.2.3 Funzioni di sicurezza

Le funzioni di sicurezza implementate dall'ODV sono descritte in dettaglio nel capitolo 7 del Traguardo di Sicurezza [TDS]. Di seguito sono riassunte le principali caratteristiche di sicurezza del prodotto che sono state oggetto di valutazione:

a) **Ruoli degli Utenti e autenticazione**:

- **Identificazione e autenticazione** - Gli utenti vengono identificati solo in contesti in cui è richiesta anche l'autenticazione. In tal caso è necessario che l'utente immetta una o più smart card nel lettore di smart card o fornisca una *passphrase* per una Softcard. L'ODV quindi autentica gli utenti in uno dei seguenti modi:

i. come amministratore, in locale, inserendo un *quorum* (sufficiente numero di smart card) del set ACS di smart card nel lettore di smart card. All'utente viene quindi richiesto di inserire la *passphrase* tramite il PC client se si utilizza l'unità nShield Solo F3 PCIe, o tramite il pannello frontale per il dispositivo nShield Connect.

ii. Come utente firmatario (Signatory), in locale, inserendo un quorum (sufficiente numero di smart card) del set OCS di smart card nel lettore di smart card. All'utente viene quindi richiesto di inserire la *passphrase* tramite il PC client se si utilizza l'unità nShield Solo F3 PCIe, o tramite il pannello frontale per il dispositivo nShield Connect.

iii. Come utente firmatario (Signatory), da locale o da remoto utilizzando una applicazione per la creazione della firma (SCA), inserendo la *passphrase* per la Softcard.

- **Creazione dei set di carte e protezione degli SCD** - L'ODV è in grado di creare un set di carte Operator (OCS) o Softcard per proteggere un SCD e per l'approvazione di alcune operazioni. Durante la generazione di carte OCS o Softcard, il firmatario imposta la *passphrase* che può essere successivamente modificata solo se viene inserita la *passphrase* corrente, limitando quindi la capacità di modificare la *passphrase* al solo firmatario.

b) **Gestione delle chiavi**:

- **Generazione delle chiavi** – l'ODV è in grado di generare chiavi crittografiche come indicato in [TDS], cap. 6.2.1, Tabella 2 (*SCD/SVD Generation Table*).

- **Distruzione delle chiavi** – L'ODV è in grado di distruggere le chiavi crittografiche presenti in chiaro nella RAM dell'unità nShield Solo F3 PCIe utilizzando un processo di "zeroization" conforme ai requisiti FIPS 140-2.

c) **Servizi crittografici**:

- **Operazioni crittografiche** – L'ODV è in grado di fornire operazioni crittografiche di generazione di firme digitali come descritto in [TDS], cap. 6.2.1, Tabella 3 (*Digital Signature Generation Table*).

d) Protezione dei dati dell'utente:

- **Integrità dei dati** – l'ODV è in grado di conservare in modo sicuro le coppie di chiavi (privata/pubblica) generate in supporti di memoria permanente. Il "key blob", che rappresenta il format utilizzato dall'ODV per memorizzare in modo sicuro le chiavi, ne protegge l'integrità e la confidenzialità.

e) **Protezione delle funzionalità di sicurezza dell'ODV**:

- **Protezione fisica** – I componenti elettronici che costituiscono il modulo nShield Solo F3 PCIe sono protetti da un rivestimento di resina epossidica che fornisce una indicazione visiva di un eventuale tentativo di manomissione. L'ODV è progettato per resistere all'applicazione di tensioni e

temperature al di fuori delle normali condizioni di funzionamento. Se L'ODV rileva una deviazione significativa dalle condizioni di funzionamento previste, entra in uno stato di errore nel quale non esegue alcuna operazione crittografica, inibisce l'uso di tutte le interfacce utente e dà una indicazione visiva dell'evento tramite il LED presente sul modulo fino a quando non viene riavviato (ciò consente la cancellazione di qualsiasi chiave privata presente in chiaro nella RAM del modulo e la richiesta di una nuova autenticazione da parte di un qualsiasi firmatario).

- **Self-Test** – l'ODV esegue una serie di auto-test durante l'avvio, che comprendono test dell'hardware, test degli algoritmi crittografici, test di integrità del codice, test della validità della memoria EEPROM della scheda PCIe, e che la EEPROM contiene una chiave K_{NSO} valida (che indica che la scheda PCIe è stata inizializzata). Un amministratore può eseguire questi test in qualsiasi momento durante lo stato operativo dell'ODV. Se uno di questi test fallisce, l'ODV entra in uno stato di errore nel quale non esegue alcuna operazione crittografica e non risponde ad alcuna interfaccia.

f) Canali sicuri:

- **Sicurezza delle comunicazioni tra componenti dell'ODV** - Nel caso dell'utilizzo del solo modulo nShield Solo F3 PCIe (Figura 2), esiste un canale protetto tra l'*hardserver* ed il modulo stesso in virtù del ambiente sicuro in cui è gestito l'ODV. Infatti, in questo caso l'ODV beneficia della comunicazione tra processi e bus PCIe nella piattaforma client su cui risiede che è parte dell'ambiente operativo. Nel caso di utilizzo dell'nShield Connect (Figura 3), l'ODV implementa un canale protetto tra la componente dell'*hardserver* presente nel PC client e la componente dell'*hardserver* presente nel dispositivo nShield Connect tramite il protocollo sicuro proprietario 'impath'. Questo canale offre protezione della riservatezza e dell'integrità dei dati scambiati tra le parti separate dell'ODV. La protezione delle comunicazioni tra la SCA e l'ODV è a carico dell'ambiente operativo.

g) Limiti delle sessioni operative:

- **Gestione delle sessioni** – È possibile stabilire vincoli sulle sessioni che si instaurano tra SCA e ODV. Tali vincoli sono legati alla possibilità di risolvere la sessione attiva quando l'ultima smart card viene rimossa dal lettore di schede.

7.4 Documentazione

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

Devono inoltre essere seguiti gli ulteriori obblighi o note per l'utilizzo sicuro dell'ODV contenuti nel capitolo 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione,

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 (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

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

7.7 Conduzione della valutazione

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

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

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS Leonardo.

L'attività di valutazione è terminata in data 28 giugno 2019 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 26 luglio 2019. 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 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 "nShield HSM Family v11.72.03" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con l'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 2 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 l'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
Delivery procedures	ALC_DEL.1	Positivo

Classi e componenti di garanzia		Verdetto
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: security enforcing modules	ATE_DPT.2	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 2 – 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 "nShield HSM Family v11.72.03" 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 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 nelle Guide per l'Installazione [IGC] e [IGS], nella Guida per la Configurazione Valutata Common Criteria [ECG] e nelle Guide per l'Utente [UGCU], [UGCW], [UGSU] e [UGSW], fornite insieme all'ODV.

Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto nella documentazione citata. 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.

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 in [TDS], cap. 4.4 e 4.5, in particolare quelle relative al personale ed ai locali all'interno dei quali andrà ad operare l'ODV e al personale ed ai dispositivi che interagiscono con l'ODV da remoto.

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

Le varie componenti dell'ODV (HW, FW e SW), vengono assemblate e verificate presso il sito di produzione di proprietà della società Plexus Corp., situato a Kelso, Regno Unito, dove viene gestita anche la fase di consegna fisica dell'ODV all'utente finale.

Quando il cliente effettua l'ordine dell'ODV riceve una conferma dell'ordine con la descrizione di quanto ordinato ed una data di consegna stimata.

La consegna viene effettuata tramite corriere privato. Il cliente riceve via Email un messaggio di conferma della consegna contenente i dettagli dell'ordine, l'indirizzo di consegna, le informazioni per la tracciatura, i numeri seriali delle varie unità che compongono l'ODV e informazioni sull'etichetta antimanomissione, in modo da consentire al cliente di verificare l'integrità di quanto ricevuto.

Le immagini ISO contenenti il firmware dell'ODV vengono consegnate unitamente all'unità fisica ordinata (nShield Solo+ F3 o nShield Connect+) e sono altresì disponibili per il download dal portale di supporto Web del Fornitore. Il resto del software (*hardserver*, librerie e *utility* client) è invece disponibile unicamente tramite download.

Le immagini del firmware dell'ODV sono cifrate con una chiave Triple-DES e firmate con chiavi di proprietà di nCipher memorizzate in maniera sicura all'interno di HSM. Il valore di *hash* dell'intera immagine ISO è disponibile pubblicamente e può essere verificato dal cliente.

9.2 Installazione e utilizzo sicuro dell'ODV

L'installazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo in accordo agli obiettivi di sicurezza indicati nel [TDS], devono avvenire seguendo le istruzioni contenute nelle apposite sezioni dei seguenti documenti:

- [IGC] nShield Connect Installation Guide, Version 6.0, 13 March 2015.
- [IGS] nShield Solo Installation Guide, Version 6.0, 13 March 2015.
- [ECG] nShield HSM family v11.72.03 Common Criteria Evaluated Configuration Guide, ASEC1382, Version 1.3, 11 June 2019.
- [UGCU] nShield Connect User Guide for Unix, Version 11.0, 13 March 2015.
- [UGCW] nShield Connect User Guide for Windows, Version 11.0, 13 March 2015.
- [UGSU] nShield Solo User Guide for Unix, Version 11.0, 13 March 2015.

- [UGSW] nShield Edge and nShield Solo User Guide for Windows, Version 11.0, 13 March 2015.

I parametri del “Security World” impostati in fase di inizializzazione determinano, tra le altre cose, le caratteristiche dell’infrastruttura di sicurezza e le chiavi utilizzate per proteggere gli SCD. Nella configurazione valutata vengono applicate al “Security World” le seguenti restrizioni (per maggiori dettagli fare riferimento al documento [ECG]):

- per creare il “Security World” o per aggiungere un HSM nShield a un “Security World” esistente deve essere utilizzata unicamente l’*utility* CLI ‘new-world’;
- gli algoritmi di cifratura utilizzati per proteggere il “Security World” devono essere AES-256, DSA con chiavi a 3072-bit e funzione di *hash* SHA-256.
- tutte le chiavi crittografiche (inclusi gli SCD) debbono essere protette da un set di smart card OCS o mediante Softcard (con relativa *passphrase*).
- solo il firmatario deve avere accesso al set di smart card OCS;
- la funzionalità Remote Operator deve essere disabilitata;
- la sostituzione delle smart card OCS deve essere disabilitata;
- la sostituzione della *passphrase* per le smart card OCS deve essere disabilitata;
- la funzione di *key recovery* deve essere disabilitata;
- le opzioni NVRAM devono essere disabilitate;
- il Secure Execution Environment (SEE), incluso il *debugging* SEE, deve essere disabilitato.

Si raccomanda inoltre agli utilizzatori dell’ODV di fare particolare attenzione, durante la creazione del “Security World”, alla definizione delle regole che riguardano la robustezza delle *passphrase*. Di fatto l’ODV da la possibilità di creare *passprhase* che soddisfino vincoli sulla lunghezza (numero minimo di caratteri) e sulla tipologia di caratteri utilizzabili (lettere maiuscole e minuscole, caratteri numerici, caratteri non alfanumerici), ma non vi è alcuna imposizione nella scelta dell’utilizzo di tali regole da parte dell’ODV. Pertanto tale scelta è a completa discrezione dell’utilizzatore dell’ODV al quale si raccomanda l’uso di *passphrase* sufficientemente robuste.

10 Appendice B – Configurazione valutata

L'ODV è il prodotto "nShield HSM Family v11.72.03", costituito da una serie di dispositivi di tipo HSM.

In Tabella 3 sono elencati i componenti HW, FW e SW, con le rispettive versioni, che costituiscono la configurazione valutata dell'ODV, come riportato Traguardo di Sicurezza [TDS], a cui si applicano i risultati della valutazione.

Tipo	Nome	Identificativo	Fattore di forma	Tipo di consegna
Hardware	nShield Solo F3 PCIe 500+	Model number NC4433E-500	Scheda PCIe	Fisica (corriere)
	nShield Solo F3 PCIe 6000+	Model number NC4433E-6K0	Scheda PCIe	Fisica (corriere)
	nShield Connect 500+	Model number NH2054	Apparato di rete	Fisica (corriere)
	nShield Connect 1500+	Model number NH2061	Apparato di rete	Fisica (corriere)
	nShield Connect 6000+	Model number NH2068	Apparato di rete	Fisica (corriere)
Firmware	nCore firmware	Version 2.55.4	File immagine binario	Incluso in nShield Solo+ F3 o download
	nShield Connect firmware image	Version 12.45.1	File immagine binario	Incluso in nShield Connect+ o download
Software	Hardserver	Version 2.92.1	Immagine ISO	Download
	Generic stub library	Version 3.30.5	Immagine ISO	Download
	NFKM and RQ card library	Version 1.86.1	Immagine ISO	Download
	PKCS#11 library	Version 2.14.1	Immagine ISO	Download
	Client utilities: nopclearfail, fwcheck, loadrom, nfloadmon, ppmk, cardpp, createocs, generatekey, new-world, racs.	Version 2.54.1	Immagine ISO	Download
Documentazione	nShield HSM family v11.72.03 Common Criteria Evaluated Configuration Guide	v1.3	File PDF	Download

Tabella 3 – Lista dei componenti HW, FW e SW dell'ODV

Gli elementi HW e SW non facenti parte dell'ODV, ma richiesti per il suo corretto funzionamento, sono elencati nel cap. 2.2.7 del Traguardo di Sicurezza [TDS].

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 l'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.

Le attività relative all'esecuzione dei test funzionali e dei test di intrusione sono state svolte dai Valutatori mediante l'analisi effettuata sulla documentazione durante tutto il processo di Valutazione (tutte le evidenze messe a disposizione dal Fornitore sono state oggetto di indagine, in particolare per l'analisi delle vulnerabilità) e attraverso una sessione di test che si è svolta nel periodo 3-7 luglio 2019 presso la sede di nCipher Security Limited situata a Cambridge, Regno Unito, dove è stato allestito il "Test Bed" del Fornitore.

11.1 Configurazione per i test

Durante la sessione test è stata resa disponibile ai Valutatori la seguente versione dell'ODV:

- nShield HSM Family, Version 11.72.03

Inoltre, i Valutatori hanno utilizzato i seguenti strumenti software:

- nmap v7.70;
- Nessus v 8.4.0 (#193) WINDOWS con Plugin Set (201906050042);
- Wireshark v2.6.6 (v2.6.6.-0-gdf942cd8).

Tali strumenti sono stati installati ed utilizzati dai Valutatori su una macchina facente parte del "Test Bed" allestito dal Fornitore presso la propria sede.

Inoltre i Valutatori hanno avuto a disposizione il codice sorgente costituente l'ODV per ulteriori approfondimenti sulla analisi delle vulnerabilità.

Per l'analisi statica del codice i Valutatori hanno adottato il seguente *tool*, anche questo installato su una macchina appartenente al Fornitore:

- Coverity v2018.12 (versione 10.4 del relativo database interno).

Il "Test Bed" allestito dal Fornitore ha una architettura basata su un ambiente di test proprietario denominato ASV, che viene gestito da una macchina con sistema operativo Microsoft Windows, in grado di eseguire i test utilizzando il protocollo di rete SSH. Tale ambiente è anche responsabile della definizione delle specifiche del test e della definizione dei risultati.

Per eseguire i test, l'ambiente ASV necessita di un file di configurazione che fornisca le informazioni necessarie per la connessione dei dispositivi/macchine da testare. Tali file di configurazione sono presenti su un'altra macchina denominata "Perforce Server".

In particolare, i test sono stati effettuati sulle seguenti configurazioni di sistema:

a) Per i test automatici macchine client ASV con le seguenti configurazioni:

   - Windows Server 2012 R2 Datacenter (64-bit) con HSM nShield Solo F3 PCIe 6000+ v11.72.03;
   - Red Hat Enterprise Linux Release 6 (64-bit) con HSM nShield Solo F3 PCIe 6000+ v11.72.03;
   - Windows 7 Enterprise (64-bit) con HSM nShield Solo F3 PCIe 6000+ v11.72.03;
   - Windows 7 Enterprise (32-bit) con HSM nShield Solo F3 PCIe 6000+ v11.72.03.

   Con il seguente software installato:

   - Security World and Cipher Tools v11.72.02;
   - Server SSH.

b) Per i test manuali una macchina client ASV con la seguente configurazione di sistema:

   - Windows 7 Enterprise (64-bit) con HSM HSM nShield Connect 6000+ v11.72.03;

Tutte le machine client in realtà sono machine virtuali definite su una "macchina ospite" su cui è installato il software VMware ESXI 6.5.0. Le macchine virtuali accedono ad un unico HSM nShield Solo connesso ad uno degli slot PCIe della medesima "macchina ospite" mediante "PCI Passthrough". Questo implica che nei test effettuati può apparire solo una macchina virtuale per volta, collegata all'unico HSM nShield Solo presente sulla macchina ospite.

Il "Test Bed" comprende anche un dispositivo MUX, costituito da una serie di lettori di smart card, necessario per la simulazione dell'utilizzo di una definita sequenza di smart card nei test automatici.

Tutti i test effettuati dai Valutatori sono stati eseguiti utilizzando una connessione mediante protocollo RDP (*Remote Desktop Protocol*) da una ulteriore macchina del Fornitore, connessa agli altri dispositivi mediante uno *switch*.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

I Valutatori hanno effettuato una prima fase di analisi solo sulla documentazione di Test messa a disposizione dal Fornitore prima di effettuare la sessione di test presso il "Test Bed" allestito dal Fornitore.

Tale sessione si è articolata nelle seguenti macro fasi:

1. Verifica dell'ambiente di test.
2. Esecuzione dei test del Fornitore, sia quelli automatici, sia quelli manuali e relativa analisi dei risultati.
3. Esecuzione dei test indipendenti predisposti dai Valutatori e analisi dei risultati.
4. Analisi delle potenziali vulnerabilità riscontrate durante l'intero processo di Valutazione.

11.2.2 Copertura dei test

I Valutatori hanno verificato che la documentazione di test presentata dal Fornitore comprende:

- l'insieme dei test funzionali svolti dal Fornitore;
- le evidenze circa la copertura dei test svolti dal Fornitore e cioè che tutte le TSF sono state testate in relazione alle loro Specifiche Funzionali;
- Le evidenze circa la profondità con cui i test del Fornitore sono stati condotti e cioè che tutti i moduli presentati nella documentazione di specifiche funzionali e di progetto ad alto livello dell'ODV siano stati tenuti in considerazione durante lo svolgimento dei test.

11.2.3 Risultati dei test

Nella fase di verifica dell'ambiente di test (fase 1) i Valutatori hanno verificato la corretta installazione e configurazione dell'ODV sulle macchine messe a disposizione dal Fornitore e si sono accertati che l'ambiente di test configurato dal Fornitore non contenesse elementi distinti da quelli dichiarati nei documenti consegnati dal Fornitore stesso, al fine di evitare che i risultati dei test fossero falsati dalla eventuale presenza di dispositivi HW o applicativi SW estranei a quelli dichiarati.

A tale scopo è stata utilizzata l'applicazione Nmap (Network Mapper v7.70) installata su una delle macchine del "Test Bed" (ASV Test Runner), mediante la quale i Valutatori hanno potuto analizzare la rete per verificare l'eventuale presenza di dispositivi HW non dichiarati. Il risultato di tale verifiche è stato positivo in quanto non sono stati riscontrati apparati diversi da quelli attesi.

Nella fase di esecuzione dei test automatici (fase 2) i Valutatori, coadiuvati dal personale del Fornitore, hanno mandato in esecuzione in sequenza i test automatici sulle macchine configurate durante la fase 1.

A causa delle tempistiche necessarie per l'ottenimento dei risultati, i Valutatori hanno parallelizzato tale attività con approfondite interviste con gli sviluppatori software del Fornitore, al fine di analizzare nel dettaglio alcune porzioni di codice che potevano essere impattate dalle modifiche dell'ODV rispetto alla precedente versione certificata. Le analisi hanno riguardato le implementazioni delle funzioni/comandi suddivisi per i moduli di appartenenza definiti nella documentazione di sviluppo (nCoreAPI, HARDSERVER, NFKM, PKCS11, nShield Utilities).

Al termine dei Test automatici i Valutatori hanno potuto verificare che tutti i risultati erano coerenti con quelli attesi.

11.3 Test funzionali indipendenti svolti dai Valutatori

Alla luce dei risultati ottenuti durante le varie sotto attività della fase 2 dei test e considerando opportunamente le modifiche dell'ODV evidenziate nel Traguardo di Sicurezza [TDS] rispetto alla versione precedente, i Valutatori hanno deciso di eseguire unicamente alcuni dei test indipendenti già identificati durante il precedente processo di certificazione durante la terza fase di test.

I test indipendenti definiti dai Valutatori hanno avuto i seguenti principali obiettivi:

- verificare che nel caso in cui l'ODV entra in uno stato di errore non è possibile eseguire alcun comando;
- verificare che durante la fase di avvio dell'ODV la porta USB presente sulla parte frontale dell'ODV è disabilitata (non alimentata);
- verificare che solo alcuni comandi sono accettati dall'ODV quanto lo stesso è in uno dei seguenti stati: "Pre-Initialisation", "Pre-Maintenance" e "Maintenance";
- verificare che le restrizioni al "Security World" descritte nel cap. 9.2 del presente Rapporto sono applicate correttamente nella configurazione valutata dell'ODV.

I Valutatori hanno potuto verificare per ciascun test i risultati attesi.

11.4 Analisi delle vulnerabilità e test di intrusione

Tutti gli approfondimenti effettuati in aggiunta all'analisi fatta in precedenza su tutti i "deliverable" del processo di valutazione (in particolare sulla documentazione di sviluppo), hanno consentito ai Valutatori di concludere che nessuna nuova potenziale vulnerabilità fosse presente nell'ODV.

Pertanto, i Valutatori hanno deciso di effettuare nuovamente alcune delle verifiche introdotte dalla precedente certificazione al fine di verificare unicamente se le modifiche introdotte nella nuova versione dell'ODV potessero avere qualche impatto sui risultati dei test precedentemente effettuati.

In particolare, le analisi svolte hanno riguardato i seguenti aspetti:

- Analisi del meccanismo che implementa la verifica di robustezza della *passphrase* (SFR FIA_SOS.1).
- Analisi della possibilità di esportare in chiaro una chiave privata generata dall'ODV.
- Analisi del meccanismo di distruzione delle chiavi crittografiche (SFR FCS_CKM.4).
- Analisi del meccanismo di protezione dell'integrità dei DTBS/R nel trasferimento tra parti separate dell'ODV (SFR FDP_ITT.1).
- Analisi della possibilità di modificare il *firmware* dell'ODV.
- Analisi della possibile esecuzione di codice non autorizzato da parte di un utente dell'ODV.
- Analisi statica del codice sorgente.

I risultati delle analisi non hanno portato alla necessità di ulteriori approfondimenti, consentendo quindi ai Valutatori di concludere questa attività con esito positivo.