Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 1/16

(Certification No.)

Prodotto: **nShield HSM Family v11.72.02**
(Product)

Sviluppato da: **Thales e-Security Ltd.**
(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 Rita Forsi)

Roma, 10 marzo 2016

Common Criteria

SOGIS IT SECURITY CERTIFICATE

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 v11.72.02

OCSI/CERT/RES/02/2012/RC

Versione 1.0

10 marzo 2016

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	10/03/2016

2 Indice

3 Elenco degli acronimi

ACS	Administrator Card Set
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
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
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
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
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

[CC1] CCMB-2009-07-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 3, July 2009

[CC2] CCMB-2009-07-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 3, July 2009

[CC3] CCMB-2009-07-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 3, July 2009

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

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

[CEM] CCMB-2009-07-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 2, July 2009

[CMS] nShield V11 Assurance Life-cycle_Configuration Management Scope, r31 – 23 November 2015

[ECG] ASEC1382 nShield HSM family v11.72.02 Common Criteria Evaluated Configuration Guide - Version 1.1 - 18 November 2015

[ETSI1] “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”, ETSI TS102 176-1 V2.0.0 2011-07

[ETSI2] “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices”, ETSI TS102 176-2 V1.2.1 2005-07

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

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

[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

[RFV] Rapporto Finale di Valutazione del prodotto "nShield HSM Family v11.72.02", Versione 1.1, 30 gennaio 2016

[SOGIS] "Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", Version 3, January 2010

[STSAN] "ST sanitising for publication", CCRA Supporting Document, CCDB-2006-04-004, April 2006

[TDS] nShield HSM family v11.72.02 Security Target, Version 0-10, 15 September 2015

[TDS-Pub] nShield HSM family v11.72.02 Public Security Target, Version 1-0, 20 November 2015

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

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

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

[UGSW] nShield Edge and nShield Solo User Guide for Windows, v 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 nuova versione dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

I certificati rilasciati prima dell'8 settembre 2014 sono ancora riconosciuti secondo le regole del precedente accordo [CCRA-2000], cioè fino al livello EAL4 (e ALC_FLR). Queste stesse regole del CCRA-2000 si applicano ai processi di certificazione in corso alla data dell'8 settembre 2014, come pure al mantenimento e alla ri-certificazione di vecchi certificati, per un periodo di transizione fino all'8 settembre 2017.

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

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

Poiché il prodotto certificato è stato accettato nel processo di certificazione prima dell'8 settembre 2014, il presente certificato è riconosciuto secondo le regole del precedente accordo [CCRA-2000], cioè fino a EAL4.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "nShield HSM Family v11.72.02", sviluppato dalla società Thales e-Security.

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

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

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia 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 di questo Rapporto di Certificazione.

La valutazione è stata condotta sulla base del Traguardo di Sicurezza completo [TDS], a cui viene fatto riferimento nel seguito del presente documento. La versione pubblicata del Traguardo di Sicurezza [TDS-Pub] è stata prodotta e verificata in conformità al documento [STSAN] e non contiene differenze sostanziali rispetto alla versione completa.

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 v11.72.02" 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 v11.72.02
Traguardo di Sicurezza	nShield HSM family v11.72.02 Security Target, Version 0-10, 15 September 2015
Livello di garanzia	EAL4 con aggiunta di AVA_VAN.5
Fornitore	Thales e-Security
Committente	Thales UK Limited
LVS	Consorzio RES
Versione dei CC	3.1 Rev. 3
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	8 giugno 2012
Data di fine della valutazione	30 gennaio 2016

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

7.3 Prodotto valutato

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

L'ODV "nShield HSM Family v11.72.02" (nel seguito anche indicato semplicemente come nShield o nShield Family) 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, fisicamente installati in un ambiente sicuro e connessi alla rete

dell'organizzazione stessa. I potenziali ambiti d'uso dell'ODV sono diversi e includono *application server*, Web server SSL/TLS e altri dispositivi di sicurezza.

La famiglia di HSM nShield consente alle aziende di aggiungere protezione crittografica 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 di firme digitali, 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 nShield Family possono essere utilizzati come "Dispositivi sicuri di firma elettronica (Secure Signature-Creation Device, 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 500e	NC4033E-500	• nCore firmware version 2.55.1 • 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 Solo F3 PCIe 500+	NC4433E-500	
nShield Solo F3 PCIe 6000e	NC4033E-6K0	
nShield Solo F3 PCIe 6000+	NC4433E-6K0	
nShield Connect 500	NH2033	• nCore firmware version 2.55.1, nShield Connect firmware image version 0.9.9 • 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 500+	NH2054	
nShield Connect 1500	NH2040	
nShield Connect 1500+	NH2061	
nShield Connect 6000	NH2047	
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. I modelli che presentano il suffisso '+' utilizzano l'acceleratore crittografico "Exar 8204" mentre gli altri utilizzano il "Broadcom 5825".

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.

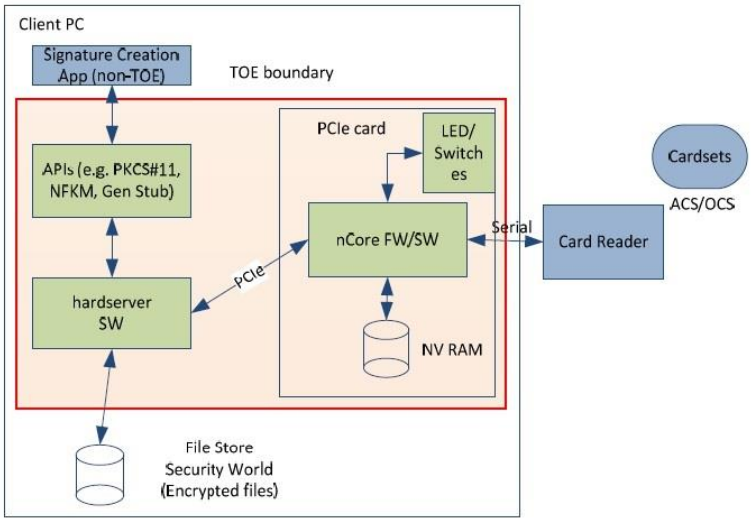

Figura 2 - Architettura del modulo nShield Solo F3 PCIe

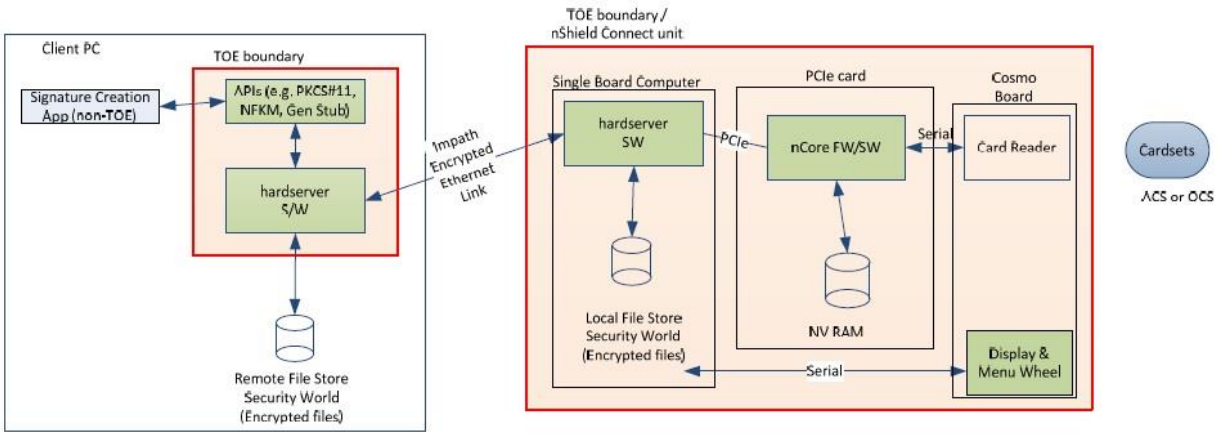

Figura 3 - Architettura dell'apparato nShield Connect

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 dell'apparato nShield Connect, l'unità nShield Solo F3 PCIe viene installata direttamente all'interno di un PC client e viene collegata 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 (gestione dell'ODV, generazione di chiavi o operazioni di firma). Nel caso dell'apparato nShield Connect, il lettore di smart card è inserito all'interno del suo involucro.

I dati relativi al "Security World", che, come descritto più avanti, è in sostanza l'infrastruttura HW/SW per la gestione sicura del ciclo di vita delle chiavi, vengono memorizzati separatamente nella memoria persistente collegata al PC client. Questo *repository* può risiedere su un disco locale, o su un dispositivo di *storage* di rete. La posizione in cui vengono memorizzati i dati del "Security World" non influisce sulla sicurezza dell'ODV in quanto tali dati vengono memorizzati esclusivamente in forma cifrata ed il loro contenuto in chiaro è accessibile solo all'interno dell'unità nShield Solo F3 PCIe.

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 i 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 da chiavi di cifratura presenti nella scheda PCIe. La scheda PCIe è l'unico luogo in cui le chiavi possono essere 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 l'apparato nShield Connect tramite una connessione sicura. La connessione tra il PC client e l'nShield 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 lo schema di 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 tutte 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 privilegiati 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" è costituito da:

- uno o più nShield HSM;
- un set di smart card ACS (*Administrator Card Set*), il cui gestore è l'amministratore e il cui utilizzo combinato dà 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 (*Operator Card Set*) a cui sarà collegata una opportuna *passphrase*, necessaria per il loro utilizzo, i cui gestori sono gli utenti firmatari;
- opzionale: una o più *Softcard* a cui sarà collegata una opportuna *passphrase*, necessaria per il loro 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 Ipotesi

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.

7.3.2.2 Funzioni di sicurezza

Le funzioni di sicurezza implementate dall'ODV sono descritte in dettaglio in [TDS], cap. 1. Di seguito sono riassunti alcuni aspetti ritenuti rilevanti.

Le funzionalità di sicurezza implementate dall'ODV sono categorizzabili come di seguito indicato:

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. 5.2.1, 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. 5.2.1, 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 inizializzato). 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 inibisce l'uso di tutte le interfacce utente.

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 nel capitolo 9 (Appendice A) 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 par. 8.2 di questo rapporto.

7.5 Requisiti funzionali e di garanzia

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

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.

Tutti gli SFR sono stati derivati direttamente dai CC Parte 2 [CC2].

7.6 Conduzione della valutazione

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

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

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

L'attività di valutazione è terminata in data 30 gennaio 2016 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 2 febbraio 2016. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.7 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B. 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 v11.72.02" 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.

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

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: 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 v11.72.02" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nel capitolo 3 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, l'Appendice A del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'installazione 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], par. 3.4 e 3.5, in particolare quelle relative al personale ed ai locali all'interno dei quali andrà ad operare l'ODV.

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

Quando il cliente effettua l'ordine dell'ODV riceve una conferma che contiene un numero d'ordine univoco.

La consegna dell'ODV avviene direttamente presso la sede del cliente. Il cliente deve verificare che sulla nota di consegna applicata sulla parte esterna della scatola sia riportato correttamente lo stesso numero d'ordine.

Al momento della consegna, il prodotto si trova nello stato "Factory State", cioè non è stato ancora installato e non è accessibile dagli utenti finali. L'ODV deve essere installato e configurato dall'amministratore seguendo le indicazioni fornite nelle apposite Guide (v. cap. 9.2).

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, v 6.0 - 13 March 2015.
- [IGS] nShield Solo Installation Guide, v 6.0 - 13 March 2015.
- [ECG] ASEC1382 nShield HSM family v11.72.02 Common Criteria Evaluated Configuration Guide - Version 1.1 - 18 November 2015.
- [UGCU] nShield Connect User Guide for Unix, v 11.0 - 13 March 2015.
- [UGCW] nShield Connect User Guide for Windows, v 11.0 - 13 March 2015.
- [UGSU] nShield Solo User Guide for Unix, v 11.0 - 13 March 2015.
- [UGSW] nShield Edge and nShield Solo User Guide for Windows, v 11.0 - 13 March 2015.

10 Appendice B – Configurazione valutata

Nel seguito sono elencati i componenti HW/SW, con le rispettive versioni, costituenti la configurazione valutata dell'ODV, come riportato in [CMS], a cui si applicano i risultati della valutazione.

In [TDS], cap. 1.2.7**,** sono elencati i componenti HW/SW non facenti parte dell'ODV, ma richiesti per il suo corretto funzionamento.

10.1 Hardware

La Tabella 3 riporta gli HardWare Configuration Items dell'ODV valutato.

Componente HW	Numero di serie
nShield Solo F3 PCIe 500e	NC4033E-500
nShield Solo F3 PCIe 500+	NC4433E-500
nShield Solo F3 PCIe 6000e	NC4033E-6K0
nShield Solo F3 PCIe 6000+	NC4433E-6K0
nShield Connect 500	NH2033
nShield Connect 500+	NH2054
nShield Connect 1500	NH2040
nShield Connect 1500+	NH2061
nShield Connect 6000	NH2047
nShield Connect 6000+	NH2068

Tabella 3 – Componenti HW dell'ODV

10.2 Software

La Tabella 4 che segue riporta la versione dei componenti software dell'ODV valutato.

Componente SW	Descrizione	Versione
fwsign	nCore firmware	2.55.1
nhsig2	nShield Connect firmware image	0.9.9
nfserv	Hardserver	2.92.1
sworld	NFKM and RQCard client libraries	1.86.1

Componente SW	Descrizione	Versione
hilibs	Generic stub client library	3.30.5
nfuser	Client utilities	2.54.1
pkcs11	PKCS#11 client library	2.14.1

Tabella 4 – Componenti SW dell'ODV

Le utility client parte dell'ODV sono ([TDS], par. 1.2.5): nopclearfail, fwcheck, loadrom, nfloadmon, ppmk, cardpp, createocs, generatekey, new-world, racs.

10.3 Ambiente operativo dell'ODV

Di seguito si riportano gli elementi HW e SW che devono essere presenti nell'ambiente operativo dell'ODV per consentire la corretta operatività ([TDS], par. 1.2.7):

- Utility aggiuntive rispetto a quelle elencate in Tabella 4 (queste sono descritte nelle Guide per l'Utente [UGCU], [UGCW], [UGSU] e [UGSW], fornite insieme all'ODV):
  - Utility per operazioni generali.
  - Utility hardware.
  - Utility di test.
  - Utility del Security World.
- Applicazioni client.
- Uno dei seguenti Sistemi Operativi:
  - Microsoft Windows Server 2012 R2.
  - Microsoft Windows Server 2012.
  - Microsoft Windows Server 2008 R2 x64.
  - Microsoft Windows 7 IA-32/x64.
  - Red Hat Enterprise Linux AS/ES 6 x64.
  - Red Hat Enterprise Linux AS/ES 5 x86.
- Hardware client su cui girano le applicazioni client e l'*hardserver* client.
- Lettore di smart card: già incluso nell'unità nShield Connect o separato nel caso dell'nShield Solo – numero di serie A-018000-L (SMARTCARD READER TL ASSY).

- Smart card per ACS e OCS: incluse con l'ODV – numero di serie AC3148T (pacchetto di 5 smartcard) o AC3155T (pacchetto di 10 smartcard).

Il software facente parte dell'ODV non richiede particolari requisiti hardware oltre quelli richiesti per eseguire il sistema operativo e le applicazioni client scelte.

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 durante due sessioni di test effettuate nei periodi 27-31 luglio 2015 e 9-13 novembre 2015, presso la sede della società Thales e-Security situata a Jupiter House, Station Rd - Cambridge (UK), dove è stato allestito il "Test Bed" del Fornitore.

11.1 Configurazione per i Test

Durante le sessioni di test sono state rese disponibili ai Valutatori due differenti versioni dell'ODV, identificate come segue:

- nShield HSM Family ,Version 11.72.00 (equivalente a 11.72).
- nShield HSM Family ,Version 11.72.02.

Durante le sessioni di test i Valutatori hanno utilizzato anche un Laptop DELL VOSTRO V131, dotato di Sistema operativo Kali Linux 2.0 con la dotazione standard del SW installato. Sono stati utilizzati anche i seguenti *tool* software, entrambi installati su macchine appartenenti al Fornitore:

- Wireshark v2.0 (installato in ambiente Microsoft Windows)
- Coverity v7.0.0 (versione 9.3.1 del database)

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

Il "Test Bed" allestito dal Fornitore ha una architettura basata su un ambiente di test sviluppato *in-house* che gira in ambiente 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 l'esecuzione dei test, l'ambiente necessita di un file di configurazione, installato su una macchina server dedicata, che fornisce le informazioni necessarie per la connessione dei dispositivi/macchine da testare.

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

Nello specifico, i test sono stati effettuati sulle seguenti configurazioni di sistema:

Prima sessione di test:

a) Per i test automatici:

- Windows Server 2012 R2 (64-bit) con HSM nShield Solo 6000+ v11.72.
- Red Hat Enterprise Linux Release 6.4 (64-bit) con HSM nShield Solo 6000+ v11.72.
- Red Hat Enterprise Linux Release 6.4 (32-bit) con HSM nShield Solo 6000e v11.72.

Con il seguente software installato:

- Security World and Cipher Tools v11.72.
- Server SSH.

b) Per i test manuali:

- Windows 7 Enterprise (64-bit) con HSM nShield Connect 6000.

Seconda sessione di test:

a) Per i test automatici:

- Windows Server 2012 R2 (64-bit) con HSM nShield Solo 6000+ v11.72.02.
- Red Hat Enterprise Linux Release 6.4 (64-bit) with HSM nShield Solo 6000+ v11.72.02.
- Red Hat Enterprise Linux Release 6.4 (32-bit) with HSM nShield Solo 6000e v11.72.02.

Con il seguente software installato:

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

b) Per i test manuali:

- Windows 7 Enterprise (64-bit) con HSM nShield Connect 6000 v11.72.02.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i Test

I test, eseguiti nelle due sessioni indicate in precedenza, sono stati divisi in categorie relative alle due attività di analisi considerate, in particolare si è adottata la seguente classificazione:

a) Attività di esecuzione dei test funzionali:

- Verifica dell'ambiente di test (1ª e 2ª sessione).
- Esecuzione dei test automatici del Fornitore (1ª e 2ª sessione).
- Esecuzione dei test manuali del Fornitore (1ª e 2ª sessione).
- Esecuzione dei test indipendenti ideati dai Valutatori.

b) Attività di analisi delle vulnerabilità ed esecuzione dei test di intrusione:

- Esecuzione di test scaturiti dal processo di Valutazione, in particolare dall'analisi dei documenti di sviluppo e di guida dell'ODV (2ª sessione).
- Test aggiuntivi o di intrusione, al fine di verificare la possibilità di sfruttare alcune delle vulnerabilità ipotizzate o riscontrate (1ª e 2ª sessione).

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, incluse le informazioni relative alle diverse classi in cui sono suddivisi i test automatici, corrispondenti ai diversi componenti SW dell'ODV (FrontPanel, GenericStub, Hardserver, nCoreAPI, NFKM, nShieldUtilities, PKCS11, RQCard);
- i risultati attesi e i risultati ottenuti per ogni test;
- 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.

11.2.3 Risultati dei test

Le attività svolte durante la prima sessione di test sono state le seguenti:

a) Installazione e configurazione dell'ODV sulle macchine messe a disposizione dal Fornitore.

b) Verifica dell'ambiente di test.

c) Esecuzione dei test automatici sulle macchine configurate durante la attività (a).

d) Analisi dei risultati dei test automatici, esecuzione dei test manuali e relativa analisi dei risultati.

Durante la verifica dell'ambiente di test, i Valutatori si sono accertati che questo non contenesse elementi distinti da quelli dichiarati nei documenti consegnati dal Fornitore, 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 stato inserito nella LAN costituente il "Test Bed" un laptop con SO Kali Linux, mediante il quale i Valutatori hanno potuto effettuare le opportune verifiche.

In parallelo all'esecuzione dei test automatici, che hanno richiesto tempi di elaborazione piuttosto lunghi, i Valutatori, coadiuvati da personale del Fornitore, hanno svolto un'analisi dettagliata di alcune porzioni di codice dell'ODV, allo scopo di evidenziare alcune potenziali vulnerabilità dell'ODV. Tale analisi ha inoltre fornito lo spunto per la definizione dei test indipendenti da eseguire durante la seconda fase di test.

In seguito agli approfondimenti fatti sul codice sorgente messo a disposizione dal Fornitore, i Valutatori hanno definito una serie di test indipendenti e di test per l'analisi di vulnerabilità che sono stati svolti durante la seconda sessione di test.

Le attività svolte durante la seconda sessione di test sono state le seguenti:

a) Verifica della corretta installazione e configurazione dell'ODV sulle macchine messe a disposizione dal Fornitore.

b) Verifica dell'ambiente di test.

c) Esecuzione dei test del Fornitore.

d) Esecuzione dei test indipendenti ideati dai Valutatori e analisi dei risultati.

e) Analisi delle potenziali vulnerabilità riscontrate durante l'intero processo di Valutazione.

f) Verifica dei risultati dei test del Fornitore con particolare attenzione a quelli in cui erano state riscontrate anomalie durante la prima sessione di test.

L'analisi effettuata durante la verifica dell'ambiente di test non ha evidenziato la presenza di vulnerabilità dell'ambiente operativo tali da rendere necessarie ulteriori analisi di approfondimento.

Avendo riscontrato diverse problematiche durante la prima sessione di test, i Valutatori hanno deciso di eseguire la totalità dei test proposti dal Fornitore, al fine di verificare le correzioni da esso apportate in seguito alle osservazioni scaturite. Tali verifiche non hanno evidenziato ulteriori anomalie, consentendo ai Valutatori di emettere un verdetto positivo per questa attività.

11.3 Test funzionali indipendenti svolti dai Valutatori

Per quanto riguarda i test indipendenti, i Valutatori hanno eseguito test specifici, mirati ad una ulteriore verifica delle funzionalità di sicurezza implementate dall'ODV. Tali test sono

stati ideati dai Valutatori durante la fase di analisi dei documenti relativi al processo di Valutazione, e nella prima fase di test.

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

- verificare che nel caso in cui si ha un surriscaldamento del modulo nShield Solo lo stesso entra in uno stato di errore (se lo stesso è all'interno di nShield Connect ciò propaga lo stato di errore a tutto il dispositivo).
- 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 quando lo stesso è in uno dei seguenti stati: "Pre-Initialisation", "Pre-Maintenance" e "Maintenance".
- verificare che i vincoli di sicurezza previsti per il "Security World" nella configurazione valutata dell'ODV sono effettivamente applicati.

I Valutatori hanno potuto verificare per ogni test il risultato atteso.

11.4 Analisi delle vulnerabilità e test di intrusione

Gli approfondimenti eseguiti sul codice sorgente, assieme all'analisi fatta in precedenza su tutti i "deliverable" del processo di Valutazione (in particolare sulla documentazione di sviluppo), hanno consentito ai Valutatori di evidenziare alcune potenziali vulnerabilità dell'ODV da verificare mediante opportune analisi eseguite in questa fase.

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

- Analisi del meccanismo che implementa la verifica di robustezza della password/passphrase (requisito funzionale di sicurezza FIA_SOS.1).
- Analisi della possibilità di esportare in chiaro una chiave privata generata dall'ODV.
- Analisi del meccanismo che fornisce una indicazione visiva di un tentativo di manomissione dell'ODV mediante protezione con rivestimento di resina epossidica (requisito funzionale di sicurezza FPT_PHP.1).
- Analisi del meccanismo di distruzione delle chiavi crittografiche (requisito funzionale di sicurezza FCS_CKM.4).
- Analisi del meccanismo di protezione dell'integrità dei DTBS/R nel trasferimento tra parti separate dell'ODV (requisito funzionale di sicurezza 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.

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

Le analisi effettuate dai Valutatori hanno evidenziato alcune anomalie che sono state prontamente segnalate al Fornitore, il quale ha provveduto ad aggiornare il SW dell'ODV.

La riesecuzione dei test di intrusione sulla versione aggiornata dell'ODV e l'esame del corrispondente codice sorgente ha permesso ai Valutatori di verificare che le anomalie precedentemente riscontrate non erano più presenti nell'ODV.

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