Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica -
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)
Organismo designato, ai sensi del comma 1 dell'articolo 30 del Regolamento (UE) n. 910/2014, e notificato, ai sensi del comma 2 dello stesso articolo, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo di firma elettronica e di un sigillo elettronico qualificati ai requisiti di sicurezza espressi nell'Allegato II al suddetto Regolamento.

Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche e di Sigilli Elettronici qualificati ai Requisiti di Sicurezza Previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Attestato di Conformità n. 4/19

Dispositivo: nShield Connect 500+, nShield Connect 1500+, nShield Connect 6000+ (v11.72.03)

Sviluppato da: nCipher Security Limited

Il dispositivo per la creazione di firme elettroniche e di sigilli elettronici qualificati indicato in questo attestato è risultato conforme ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Il Direttore
(Dott.ssa Eva Spina)

Roma, 28 novembre 2019

Il presente Attestato di Conformità è stato emesso dall'Organismo di Certificazione della Sicurezza Informatica (OCSI) in conformità al comma 5 dell'articolo 35 del DL 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale", modificato ed integrato dal DL 26 agosto 2016, n. 179.
La validità del presente Attestato di Conformità è soggetta alle condizioni e alle ipotesi esplicitate nel Rapporto di Accertamento (OCSI/ACC/NCS/04/2019/RA) ad esso allegato, che ne costituisce parte integrante e sostanziale.

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica –
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Procedura di Accertamento di Conformità di un dispositivo per la creazione di firme e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Rapporto di Accertamento

nShield Connect 500+, nShield Connect 1500+, nShield Connect 6000+ (v11.72.03)

OCSI/ACC/NCS/04/2019/RA

Versione 1.0

28 novembre 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	28/11/2019

2 Indice

3 Elenco degli acronimi

ACS Administrator Card Set

CC Common Criteria

DL Decreto Legislativo

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

EC-DSA Elliptic Curve - Digital Signature Algorithm

eIDAS electronic IDentification Authentication and Signature

HSM Hardware Security Module

OCS Operator Card Set

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto della Valutazione

PCIe Peripheral Component Interconnect Express

PP Profilo di Protezione (Protection Profile)

RSA Rivest, Shamir, Adleman

SCA Signature Creation Application

SCD Signature Creation Data

SFR Security Functional Requirement

SHA Secure Hash Algorithm

SVD Signature Verification Data

TDS Traguardo di Sicurezza (Security Target)

TSF TOE Security Functions

4 Riferimenti

[CAD] Decreto legislativo 7 marzo 2005, n. 82, recante “Codice dell'amministrazione digitale”, modificato ed integrato dal decreto legislativo 26 agosto 2016, n. 179, G.U. n. 214 del 13 settembre 2016

[DE] “Decisione di esecuzione (UE) 2016/650 della Commissione, del 25 aprile 2016, che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno”, Gazzetta ufficiale dell’Unione Europea L 109/40, 26 aprile 2016

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

[ESI-CS] “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”, ETSI TS 119 312 V1.2.2 (2018-09)

[PR] “Procedura di Accertamento di Conformità di un dispositivo per la creazione di firme e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall’Allegato II al Regolamento (UE) n. 910/2014”, OCSI/ACC/01/2016/PROC, versione 1.0, 21 dicembre 2016

[RA] Rapporto di Accertamento, “nShield Connect 500, nShield Connect 500+, nShield Connect 1500, nShield Connect 1500+, nShield Connect 6000, nShield Connect 6000+”, OCSI/ACC/THL/02/2017/RA, versione 1.0, 5 febbraio 2018

[RC] Rapporto di Certificazione, “nShield HSM Family v11.72.03”, OCSI/CERT/LEO/01/2019/RC, versione 1.0, 17 settembre 2019

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

5 Ambito dell'Accertamento di Conformità

L'OCSI (Organismo di Certificazione della Sicurezza Informatica) è l'organismo designato, ai sensi del comma 1 dell'articolo 30 del Regolamento (UE) n. 910/2014 sull'identità digitale – eIDAS (*Electronic IDentification, Authentication and Signature*) [eIDAS] e notificato ai sensi del comma 2 dello stesso articolo, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo per la creazione di una firma elettronica e di un sigillo elettronico qualificati ai requisiti di sicurezza espressi nell'Allegato II al suddetto Regolamento (UE) n. 910/2014.

L'affidamento all'OCSI dell'accertamento di cui sopra è specificato dal comma 5 dell'articolo 35 del DL 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" [CAD], modificato ed integrato dal DL 26 agosto 2016, n. 179.

L'Accertamento è stato condotto dall'OCSI in accordo a quanto indicato nella "Procedura di Accertamento di Conformità di un dispositivo per la creazione di firme e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014", OCSI/ACC/01/2016/PROC, versione 1.0, 21 dicembre 2016 [PR] (nel seguito indicata come Procedura).

L'oggetto dell'Accertamento di Conformità è la famiglia di dispositivi denominata nShield Connect, prodotta dalla società nCipher Security Limited, comprendente i seguenti modelli: nShield Connect 500+, nShield Connect 1500+, nShield Connect 6000+.

I modelli di apparati nShield Connect sopra elencati vengono complessivamente indicati nel seguito anche come "nShield Connect", "dispositivo oggetto dell'Accertamento" o semplicemente "dispositivo".

Il dispositivo oggetto dell'Accertamento è un **Dispositivo di Tipo 2**, così come definito nel cap. 6, punto A.ii, della Procedura.

Il Traguardo di Sicurezza [TDS] del dispositivo non dichiara conformità ad alcuno dei *Protection Profile* (PP) indicati nell'Allegato alla Decisione di esecuzione (UE) 2016/650 della Commissione, del 25 aprile 2016 [DE], che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30 del Regolamento (UE) n. 910/2014.

Si noti che il dispositivo oggetto dell'Accertamento è una versione aggiornata del dispositivo nShield Connect (v11.72.02), già accertato dall'OCSI (Attestato di Conformità n. 1/18 del 5 febbraio 2018 [RA]).

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, i cui risultati sono riportati nel Rapporto di Certificazione [RC].

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

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo nShield Connect, prodotto dalla società nCipher Security Limited, ed è finalizzato a fornire indicazioni ai potenziali acquirenti ed utilizzatori di tale dispositivo circa la sua conformità ai requisiti prescritti dalla normativa vigente per i dispositivi sicuri per la creazione di una firma elettronica e di un sigillo elettronico qualificati.

Il dispositivo oggetto dell'Accertamento comprende i seguenti modelli della famiglia nShield Connect:

- nShield Connect 500+
- nShield Connect 1500+
- nShield Connect 6000+

Il dispositivo, così come descritto nel relativo Traguardo di Sicurezza [TDS] e limitatamente ai modelli sopra elencati, è risultato conforme ai requisiti di sicurezza espressi nell'Allegato II al Regolamento (UE) n. 910/2014, nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura per i Dispositivi di Tipo 2 (cap. 7, punto B) e può quindi essere utilizzato come dispositivo per la creazione di firme e sigilli elettronici qualificati.

Il presente Rapporto di Accertamento deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto e al relativo Rapporto di Certificazione [RC].

La validità dell'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento è soggetta alle condizioni e alle ipotesi esplicitate nel presente Rapporto di Accertamento (vedi cap. 7), che ne costituisce parte integrante e sostanziale.

Il rilascio dell'Attestato di Conformità da parte dell'OCSI non rappresenta alcun tipo di sostegno o promozione all'uso del dispositivo accertato da parte di questo Organismo.

6.2 Descrizione del dispositivo accertato

Gli apparati della famiglia nShield Connect sono 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.

La famiglia di HSM nShield Connect 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 seguenti modelli della famiglia nShield Connect possono essere utilizzati come dispositivi per la creazione di una firma elettronica qualificata (*qualified electronic signature creation device*) e/o come dispositivi per la creazione di un sigillo elettronico qualificato (*qualified electronic seal creation device*):

- nShield Connect 500+
- nShield Connect 1500+
- nShield Connect 6000+

Un dispositivo nShield Connect è costituito da un apparato hardware montabile su *rack* (una unità da 19'') contenente una scheda PCIe nShield Solo F3.

Figura 1 – Una unità nShield Connect

Nello scenario d'uso in cui il firmatario si connette al dispositivo da una postazione d'utente remota, sia il dispositivo, sia il PC client 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 la componente dell'*hardserver* presente nel PC client e la componente dell'*hardserver* presente nel dispositivo nShield Connect è implementata da un protocollo proprietario chiamato 'impath', che protegge la riservatezza e l'integrità dei dati.

La SCA (*Signature-Creation Application*), che non fa parte del dispositivo certificato (ODV), gira sul PC client e comunica col software *hardserver* attraverso specifiche librerie client, parte dell'ODV. Il canale sicuro tra la SCA e l'ODV deve essere realizzato nell'ambiente operativo del dispositivo. Le funzionalità dell'*hardserver* possono altresì essere invocate direttamente tramite le *utility* client fornite con l'ODV.

I dispositivi nShield Connect utilizzano un'infrastruttura HW/SW per la gestione sicura del ciclo di vita delle chiavi denominata "Security World".

I dati relativi al "Security World", che contiene, tra le altre cose, gli SCD (*Signature Creation Data*, ovvero le chiavi private per generare la firma elettronica), 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 loro sicurezza in quanto tali dati vengono memorizzati esclusivamente in forma cifrata, protetti da chiavi di cifratura presenti nella scheda PCIe, ed il loro contenuto in chiaro è accessibile solo all'interno del dispositivo stesso.

In generale, il "Security World" è costituito da:

- uno o più dispositivi nShield Connect;
- 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 del dispositivo;
- un *repository* contenente gli SCD cifrati 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 un "Security World" esistono solo due ruoli (tipologie di utenti):

- Amministratore: colui che possiede il set di smart card ACS, con relativa *passphrase*.
- Firmatario (*Signatory*): colui che possiede i set di smart card OCS o la *Softcard* con relativa *passphrase*.

Durante le operazioni di firma, gli SCD vengono prelevati in forma cifrata dal "Security World", passati alla scheda PCIe da parte della SCA e quindi, una volta decifrati, vengono mantenuti in chiaro nella scheda PCIe durante il loro utilizzo.

Le funzioni di sicurezza implementate dall'ODV sono:

- Identificazione e autenticazione
- Creazione dei set di smart card e protezione degli SCD
- Generazione delle chiavi
- Distruzione delle chiavi
- Operazioni crittografiche
- Integrità dei dati
- Protezione fisica
- Self-test

- Sicurezza delle comunicazioni tra componenti dell'ODV
- Gestione delle sessioni

Per maggiori informazioni sulle caratteristiche dell'ODV e sulla sua politica di sicurezza si faccia riferimento al Traguardo di Sicurezza [TDS] e al Rapporto di Certificazione [RC].

6.2.1 Configurazione certificata del dispositivo

In Tabella 1 sono elencati i modelli dei dispositivi appartenenti alla famiglia nShield Connect, 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 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 Connect

Per ulteriori dettagli si rimanda al Rapporto di Certificazione [RC], Appendice B.

Tutti i modelli nShield Connect elencati in Tabella 1 sono risultati conformi ai requisiti di sicurezza espressi nell'Allegato II al Regolamento (UE) n. 910/2014, nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura [PR], a condizione che vengano rispettate le prescrizioni per l'utilizzo del dispositivo indicate nel cap. 8 del presente Rapporto di Accertamento.

6.3 Identificazione sintetica dell'accertamento

Richiedente l'accertamento	nCipher Security Limited
Nome del dispositivo	nShield Connect 500+, nShield Connect 1500+, nShield Connect 6000+
Versione del dispositivo	v11.72.03[1]
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
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della Procedura	22 ottobre 2019
Data di rilascio Certificato CC	17 settembre 2019
Data di rilascio Accertamento	28 novembre 2019

[1] Questo numero di versione si riferisce all'intero ODV "nShield HSM family v11.72.03" che comprende anche i modelli nShield Solo F3 che non sono stati oggetto di Accertamento di Conformità.

7 Condizioni di validità dell'Attestato di Conformità

L'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento deve essere ritenuto valido ed efficace unicamente sotto le seguenti ipotesi:

i. la certificazione di sicurezza ottenuta ([RC]) è in corso di validità, ovvero il Certificato non è stato revocato;

ii. il dispositivo reale è conforme a quello certificato e descritto nel TDS;

iii. l'ambiente di utilizzo reale del dispositivo è conforme a quello descritto nel TDS;

iv. sono rispettate tutte le condizioni aggiuntive di utilizzo del dispositivo riportate nel cap. 8 del presente Rapporto di Accertamento.

La violazione dell'ipotesi (i) comporta la perdita di validità dell'Attestato di Conformità.

La violazione di una o più delle ipotesi (ii), (iii) e (iv) ha come conseguenza la perdita di efficacia dell'Attestato di Conformità, che mantiene comunque la sua validità.

Eventuali situazioni che comportano la perdita di validità del presente Attestato di Conformità, siano esse rilevate direttamente dall'Organismo di Certificazione emettitore (OCSI) o portate a conoscenza di quest'ultimo da soggetti esterni, saranno rese note ai soggetti interessati attraverso i canali di informazione ufficiali dell'Organismo stesso.

Nel caso si verifichino situazioni che comportano la perdita di efficacia del presente Attestato, sarà cura dell'ente preposto alla vigilanza sui prestatori di servizi fiduciari qualificati provvedere alle misure correttive necessarie.

8 Condizioni di utilizzo del dispositivo accertato

Il dispositivo nShield Connect deve essere utilizzato seguendo tutte le prescrizioni contenute nel Traguardo di Sicurezza [TDS] e nel Rapporto di Certificazione [RC].

In particolare, la consegna, l'installazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo devono avvenire in accordo agli obiettivi di sicurezza indicati in [TDS] e seguendo le indicazioni riportate anche in [RC], Appendice A.

Inoltre, per quanto riguarda l'uso del dispositivo in conformità ai requisiti di sicurezza espressi nell'Allegato II al Regolamento (UE) n. 910/2014 [eIDAS], nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura [PR], si raccomanda di porre particolare attenzione agli aspetti di seguito descritti.

8.1 Algoritmi crittografici

Gli algoritmi crittografici utilizzati dalle funzioni di sicurezza (TSF) del dispositivo certificato sono elencati nel Traguardo di Sicurezza nella formulazione dei requisiti funzionali di sicurezza (SFR) della classe FCS - *Cryptographic Support* (si veda [TDS] cap. 6.2.1).

Per quanto riguarda la generazione di coppie di chiavi crittografiche e i metodi di sottoscrizione, debbono essere utilizzati esclusivamente algoritmi crittografici, lunghezze di chiavi, funzioni *hash*, protocolli e parametri conformi alla specifica ETSI TS 119 312 [ESI-CS].

In particolare, per la generazione e la verifica di firme e/o sigilli elettronici qualificati è consentito l'uso solamente dei seguenti algoritmi crittografici, tra quelli messi a disposizione dal dispositivo oggetto dell'Accertamento:

- **Funzioni di *hash*:** SHA-256, SHA-384, SHA-512.
- **Metodi di sottoscrizione:**
  - RSASSA-PSS (raccomandato) o RSASSA-PKCS-v1_5 (*legacy*), con lunghezza di chiave non inferiore a 2048 bit.
  - EC-DSA (raccomandato) con lunghezza di chiave non inferiore a 256bit, a patto che vengano utilizzate esclusivamente le curve indicate in [ESI-CS], cap. 6.2.2.3 (*EC based DSA algorithms*), Tabella 3 (*Agreed Elliptic Curve Parameters*).

In generale, per i parametri di sicurezza relativi ai metodi di sottoscrizione va tenuto conto di quanto indicato in [ESI-CS], cap. 8.4 (*Recommended key sizes versus time*).

8.2 Posizione di memorizzazione delle chiavi di sottoscrizione

Il *repository* principale dei dati del "Security World", in cui sono memorizzate in maniera persistente le coppie SCD/SVD in forma cifrata, deve essere posizionato nello stesso ambiente operativo dell'ODV o in un ambiente sicuro sottoposto a misure di sicurezza fisiche e procedurali equivalenti.

8.3 Backup e ripristino delle chiavi di sottoscrizione

Quanto alla possibilità di esportare i dati per la creazione di una firma elettronica o di un sigillo elettronico al di fuori del dispositivo, il requisito 4 dell'Allegato II al Regolamento (UE) n. 910/2014 [eIDAS], stabilisce che i prestatori di servizi fiduciari qualificati che gestiscono i dispositivi per conto dell'utilizzatore possono duplicare tali dati solo a fini di *backup*, purché rispettino i seguenti requisiti: "la sicurezza degli insiemi di dati duplicati deve essere dello stesso livello della sicurezza degli insiemi di dati originali" e "il numero di insiemi di dati duplicati non eccede il minimo necessario per garantire la continuità del servizio".

L'infrastruttura del "Security World" realizzato mediante i dispositivi della famiglia nShield Connect, consente di eseguire il *backup* semplicemente copiando i dati dal *repository* principale in una posizione di memorizzazione separata. Poiché i dati del "Security World", che comprendono anche le informazioni necessarie per associare gli SCD con il corrispondente utente Firmatario, sono memorizzati esclusivamente in forma cifrata mediante le funzioni di sicurezza del dispositivo certificato, il *backup* delle chiavi di sottoscrizione effettuato secondo questa modalità risulta conforme alle prescrizioni del Regolamento eIDAS a patto che tale *backup* venga conservato nello stesso ambiente operativo dell'ODV e sottoposto quindi alle stesse misure di sicurezza fisiche e procedurali.