Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)
Organismo designato, ai sensi del comma 4 dell'articolo 3 della Direttiva 1999/93/CE sulla firma elettronica, e notificato, ai sensi del punto b) del comma 1 dell'articolo 11 della Direttiva stessa, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo di firma ai requisiti di sicurezza espressi nell'Allegato III alla suddetta direttiva.

Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche ai Requisiti di Sicurezza Previsti dall'Allegato III della Direttiva 1999/93/CE

Attestato di Conformità n. 1/16

Dispositivo: nShield HSM Family v11.72.02

Sviluppato da: Thales e-Security

Il dispositivo per la creazione di firme elettroniche indicato in questo attestato è risultato conforme ai requisiti di sicurezza previsti dall'Allegato III della Direttiva 1999/93/CE

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 6 aprile 2016

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 30 dicembre 2010, n. 235.
La validità del presente Attestato di Conformità è soggetta alle condizioni e alle ipotesi esplicitate nel Rapporto di Accertamento (OCSI/ACC/THLS/02/2011/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

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 Elettroniche ai Requisiti di Sicurezza Previsti dall'Allegato III della Direttiva 1999/93/CE

Rapporto di Accertamento

Thales nShield HSM Family v11.72.02

OCSI/ACC/THLS/02/2011/RA

Versione 1.0

6 aprile 2016

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	06/04/2016

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

HSM Hardware Security Module

HW Hardware

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)

SCA Signature Creation Application

SCD Signature Creation Data

SSCD Secure Signature-Creation Device

SVD Signature Verification Data

SW Software

TDS Traguardo di Sicurezza (Security Target)

4 Riferimenti

[CAD] Decreto legislativo 7 marzo 2005, n. 82, G.U. n. 112 del 16 maggio 2005, Suppl. Ordinario n. 93, recante "Codice dell'amministrazione digitale", modificato ed integrato dal decreto legislativo 30 dicembre 2010, n. 235, G.U. n. 6 del 10 gennaio 2010, Suppl. Ordinario n. 8.

[CD] "Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council", Official Journal L 175, July 15, 2003.

[DEL] **"**Deliberazione CNIPA n. 45 del 21 maggio 2009, modificata dalla Determinazione DigitPA n. 69 del 28 luglio 2010", G.U. n. 191 del 17 agosto 2010.

[DIR] "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 19 on a Community framework for electronic signatures", Official Journal L 13, 19 gennaio 2000.

[DPCM] DPCM del 10 febbraio 2010, G.U. n. 98 del 28 aprile 2010, recante "Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza".

[DS] "Documento di Supporto alla Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche ai Requisiti di Sicurezza Previsti dall'Allegato III della Direttiva 1999/93/CE", OCSI/ACC/02/2010/DDS, versione 1.0, 2 novembre 2010.

[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.

[PR] "Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche ai Requisiti di Sicurezza Previsti dall'Allegato III della Direttiva 1999/93/CE", OCSI/ACC/01/2010/PROC, versione 1.0, 2 novembre 2010.

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

[RT] **"**Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali", DPCM del 22 febbraio 2013, G.U. n. 117 del 21 maggio 2013.

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

5 Ambito dell'Accertamento di Conformità

L'OCSI (Organismo di Certificazione della Sicurezza Informatica) è l'organismo designato, ai sensi del comma 4 dell'articolo 3 della Direttiva 1999/93/CE sulla firma elettronica [DIR] (nel seguito indicata come Direttiva), e notificato, ai sensi del punto b) del comma 1 dell'articolo 11 della Direttiva stessa, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo di firma ai requisiti di sicurezza espressi nell'Allegato III alla suddetta direttiva.

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 30 dicembre 2010, n. 235.

L'oggetto dell'Accertamento di Conformità è il dispositivo (o, più precisamente, famiglia di dispositivi) denominato "nShield HSM Family v11.72.02", prodotto dalla società Thales e-Security (nel seguito indicato come nShield, nShield Family o "dispositivo oggetto dell'Accertamento" o semplicemente "dispositivo").

Al dispositivo si applica, alla data di avvio della procedura di Accertamento (vedi cap. 6.2), il DPCM 10 febbraio 2010, recante "Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza" [DPCM].

Inoltre, per l'Accertamento di Conformità del dispositivo non è applicabile la Decisione Europea 2003/511/CE [CD] relativa al soddisfacimento dei requisiti di sicurezza dell'Allegato III della Direttiva Europea 1999/93/CE [DIR].

Si noti che, ai sensi dell'Art. 50, comma 1 del Regolamento (UE) n. 910/2014 [EIDAS], la Direttiva 1999/93/CE si intende abrogata a decorrere dal 1° luglio 2016.

Ciò nonostante, le Disposizioni transitorie di cui all'Art. 51, comma 1 di [EIDAS], stabiliscono che "I dispositivi per la creazione di una firma sicura la cui conformità sia stata determinata a norma dell'articolo 3, paragrafo 4, della direttiva 1999/93/CE sono considerati dispositivi per la creazione di una firma elettronica qualificata a norma del presente regolamento."

Pertanto, l'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento continuerà a conservare piena validità ed efficacia anche successivamente alla data del 1° luglio 2016, fatto salvo il rispetto delle condizioni e delle ipotesi espresse nel cap. 7. del presente Rapporto di Accertamento.

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo denominato “nShield HSM Family v11.72.02”, prodotto dalla società Thales e-Security, 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 l'apposizione di firme elettroniche qualificate (automatiche e remote).

L'Accertamento è stato condotto dall’OCSI in accordo a quanto indicato nei documenti di riferimento “Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche ai Requisiti di Sicurezza Previsti dall’Allegato III della Direttiva 1999/93/CE”, OCSI/ACC/01/2010/PROC, versione 1.0, 2 novembre 2010 [PR] (nel seguito indicata come Procedura) e “Documento di Supporto alla Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche ai Requisiti di Sicurezza Previsti dall’Allegato III della Direttiva 1999/93/CE”, OCSI/ACC/02/2010/DDS, versione 1.0, 2 novembre 2010 [DS] (nel seguito indicato come Documento di Supporto).

In particolare, poiché all'avvio della Procedura di Accertamento non era ancora disponibile il Certificato Common Criteria né risultava avviato il relativo processo di Certificazione, è stata applicata la Procedura in Modalità 2. Pertanto, in una prima fase, l'OCSI ha esaminato il Traguardo di Sicurezza del dispositivo, emettendo il Pronunciamento positivo sulla sua adeguatezza in data 11 maggio 2012.

Successivamente, in data 8 giugno 2012, veniva avviato presso lo stesso OCSI il Processo di valutazione e certificazione CC: le attività di valutazione da parte dell'LVS si sono concluse con esito positivo il 30 gennaio 2016, mentre il Rapporto di Certificazione e il relativo Certificato CC sono stati rilasciati dall’OCSI il 10 marzo 2016.

Il dispositivo oggetto dell'Accertamento, così come descritto nel relativo Traguardo di Sicurezza [TDS], è risultato quindi conforme ai requisiti di sicurezza espressi nell’Allegato III alla Direttiva, nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura, ovvero ai requisiti prescritti dalla normativa vigente per i dispositivi sicuri per l'apposizione di firme elettroniche qualificate (automatiche e remote).

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 Identificazione sintetica dell'accertamento

Richiedente l'accertamento	Thales e-Security
Nome del dispositivo	nShield HSM Family
Versione del dispositivo	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
Versione dei CC	3.1 Rev. 3
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della Procedura	26 ottobre 2011
Data di inizio della valutazione	8 giugno 2012
Data di fine della valutazione	30 gennaio 2016
Data di rilascio Certificato CC	10 marzo 2016
Data di rilascio Accertamento	6 aprile 2016

6.3 Descrizione del dispositivo accertato

Il dispositivo “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.

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 seguenti dispositivi della nShield Family possono essere utilizzati come “Dispositivi sicuri di firma elettronica (*Secure Signature-Creation Device*, SSCD)”:

- nShield Solo F3 PCIe 500e
- nShield Solo F3 PCIe 500+
- nShield Solo F3 PCIe 6000e
- nShield Solo F3 PCIe 6000+
- nShield Connect 500

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

Il dispositivo si presenta in due varianti principali: in forma di scheda PCIe, denominata nShield Solo F3, o come 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. Nel caso dell'apparato nShield Connect, il lettore di smart card è inserito all'interno del suo involucro.

I dati relativi al "Security World", ossia 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 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;
- 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 (*Signature-Creation Application*) e quindi, una volta decifrati, vengono mantenuti in chiaro nella scheda PCIe durante il loro utilizzo.

Nel caso di utilizzo del dispositivo nella variante nShield Connect, la connessione tra il PC client e il dispositivo stesso è implementata da un protocollo proprietario chiamato ‘impath’, che protegge la riservatezza e l'integrità dei dati.

Il canale sicuro tra la SCA mediante la quale opera il firmatario e il dispositivo SSCD deve invece essere realizzato nell’ambiente operativo del dispositivo certificato (ODV).

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].

6.3.1 Configurazione valutata dell’ODV

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

Modello	Numero di serie	Versioni dei componenti software
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

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

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 di firma elettronica qualificata provvedere alle misure correttive necessarie.

8 Condizioni di utilizzo del dispositivo accertato

Il dispositivo nShield Family 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 alla vigente normativa italiana in materia di firma elettronica, si raccomanda di porre particolare attenzione agli aspetti di seguito descritti.

8.1 Algoritmi crittografici

Per quanto riguarda le funzioni di *hash*, la generazione di coppie di chiavi crittografiche e i metodi di sottoscrizione, fare riferimento a quanto indicato nella Deliberazione CNIPA n. 45/2009, modificata dalla Determinazione DigitPA n. 69/2010 [DEL].

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 chiavi private al di fuori del dispositivo di firma, le "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali" [RT], all'art. 8, comma 3, prescrivono che tale operazione può essere effettuata "esclusivamente per motivi di ripristino in caso di guasto o di aggiornamento del dispositivo in uso, purché protette con algoritmi crittografici ritenuti adeguati ai fini della certificazione e purché le operazioni di esportazione e importazione delle chiavi siano effettuate mediante funzionalità di sicurezza certificate implementate dai dispositivi sicuri di firma".

L'infrastruttura del "Security World" realizzato mediante i dispositivi della famiglia nShield, 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 della normativa vigente a patto che tale *backup* venga conservato nello stesso ambiente operativo dell'ODV e sottoposto quindi alle stesse misure di sicurezza fisiche e procedurali.