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)
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. 3/18

Dispositivo: **SafeNet Luna® PCI-E Cryptographic Module used as an embedded device in Luna® SA**

Sviluppato da: **SafeNet Canada, Inc.**

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 Rita Forsi)

Roma, 12 giugno 2018

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/SFNT/03/2018/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 e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Rapporto di Accertamento

SafeNet Luna® PCI-E Cryptographic Module used as an embedded device in Luna® SA

OCSI/ACC/SFNT/03/2018/RA

Versione 1.0

12 giugno 2018

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	12/06/2018

2 Indice

3 Elenco degli acronimi

AES Advanced Encryption Standard

CC Common Criteria

DL Decreto Legislativo

DPCM Decreto del Presidente del Consiglio dei Ministri

DSA Digital Signature Algorithm

DTBS(R) Data To Be Signed (Representation)

EAL Evaluation Assurance Level

ECDSA Elliptic Curve Digital Signature Algorithm

eIDAS electronic IDentification Authentication and Signature

HSM Hardware Security Module

IT Information Technology

NTL Network Trust Link

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto della Valutazione

PCIe Peripheral Component Interconnect express

PIN Personal Identification Number

PP Profilo di Protezione (Protection Profile)

RSA Rivest, Shamir, Adleman

SCA Signature Creation Application

SCD Signature Creation Data

SFR Security Functional Requirement

TDS Traguardo di Sicurezza (Security Target)

TLS Transport Layer Security

TOE Target Of Evaluation

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 V1.2.1 (2017-05)

[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

[RC] “Certification Report Luna PCI-E Cryptographic Module, Firmware Version 6.10.9”, NSCIB-CC-179205-CR, Version 1, 22 dicembre 2017

[TDS] “LUNA® PCI-E Cryptographic Module Security Target”, CR-3524, Rev. 23, 5 dicembre 2017

[CCUG] “LUNA® PCI-E Cryptographic Module Common Criteria User Guidance”, CR-4119, Rev. 7, 5 dicembre 2017

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 il dispositivo denominato "SafeNet Luna® PCI-E Cryptographic Module, Firmware 6.10.9" utilizzato esclusivamente come modulo crittografico inserito (*embedded*) in un apparato SafeNet Luna® SA.

Il modulo crittografico Luna® PCI-E inserito in un apparato Luna® SA viene complessivamente indicato nel seguito anche come "Luna PCI-E", "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.

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo Luna PCI-E, prodotto dalla società SafeNet Canada, Inc., 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, così come descritto nel relativo Traguardo di Sicurezza [TDS], limitatamente alla configurazione come modulo crittografico inserito in un apparato Luna® SA, 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 sia come dispositivo per la creazione di una firma elettronica qualificata (*qualified electronic signature creation device*), sia come dispositivo per la creazione di un sigillo elettronico qualificato (*qualified electronic seal creation device*).

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

Il dispositivo Luna PCI-E è costituito da un modulo crittografico, o *Hardware Security Module* (HSM), installato all'interno di un apparato denominato Luna® SA che fornisce funzionalità di sicurezza delle comunicazioni tra l'HSM ed altre entità IT esterne autorizzate.

La scheda con connettore standard PCIe, illustrata in Figura 1, è contenuta in un guscio di sicurezza che fornisce evidenza di eventuali tentativi di manomissione. Inoltre, in caso di manomissione il dispositivo garantisce la protezione del materiale crittografico e degli altri dati sensibili memorizzati sulla scheda stessa che vengono resi di fatto inaccessibili all'attaccante.

Il dispositivo certificato (ODV), "LUNA® PCI-E Cryptographic Module", include i seguenti componenti:

- il modulo crittografico Luna® PCI-E;

- la documentazione di guida “LUNA® PCI-E Cryptographic Module Common Criteria User Guidance” [CCUG].

Figura 1 - Modulo crittografico Luna® PCI-E (ODV)

L’ODV fornisce un ambiente logicamente e fisicamente protetto per la gestione e l’utilizzo in sicurezza di materiale crittografico ed altri dati sensibili, che consente di mantenere la confidenzialità e l’integrità di chiavi di sottoscrizione (SCD, ossia dati per la creazione di una firma elettronica o di un sigillo elettronico) e di cifratura. Il materiale crittografico viene generato, memorizzato ed utilizzato esclusivamente all’interno dei confini di sicurezza del dispositivo certificato.

Il dispositivo Luna PCI-E fornisce le seguenti funzionalità crittografiche:

- generazione di chiavi simmetriche e di coppie di chiavi asimmetriche;
- memorizzazione sicura delle chiavi;
- funzionalità di cifratura e decifratura mediante algoritmi crittografici simmetrici e asimmetrici;
- generazione e verifica di firme elettroniche.

Inoltre, il dispositivo fornisce le seguenti funzionalità di sicurezza per la protezione del materiale crittografico e dei servizi di firma:

- autenticazione degli utenti;
- controllo di accesso per le funzioni di amministrazione delle funzioni di sicurezza;
- controllo di accesso per la creazione e distruzione delle chiavi;
- controllo di accesso per l’utilizzo delle chiavi per funzioni crittografiche e di firma;
- *self-test* del dispositivo;
- meccanismi anti-manomissione e di evidenza di tentata manomissione.

Affinché la politica di sicurezza dell'ODV risulti pienamente realizzata, questo deve essere installato in un ambiente protetto che limiti l'accesso fisico al dispositivo al solo personale autorizzato.

In particolare, per poter essere utilizzato come dispositivo per la creazione di una firma elettronica qualificata e/o come dispositivo per la creazione di un sigillo elettronico qualificato, l'ODV deve essere configurato esclusivamente come modulo crittografico inserito in un apparato Luna® SA. La configurazione dell'ODV come modulo crittografico *standalone* non rientra nel presente Accertamento di Conformità.

L'apparato Luna® SA, illustrato in Figura 2, è costituito da un dispositivo hardware montabile su *rack* contenente un modulo crittografico Luna PCI-E.

Figura 2 – Apparato Luna® SA (ODV "embedded")

L'apparato Luna® SA consente agli utenti si interfacciano con l'ODV da remoto di autenticarsi per l'accesso ai servizi crittografici mediante applicazioni client autorizzate. Inoltre, Luna® SA fornisce le seguenti funzionalità di sicurezza:

- instaurazione di un canale di comunicazione sicuro fra il dispositivo e le applicazioni client;
- gestione delle sessioni in caso di configurazioni multi-partizione, in modo da garantire l'accesso al materiale crittografico memorizzato nelle singole partizioni ai soli utenti proprietari autenticati;
- raccolta e gestione dei dati di audit.

Il dispositivo Luna PCI-E supporta i seguenti ruoli per gli utenti autenticati:

- **Security Officer (SO)**: autorizzato ad installare e configurare l'ODV, configurare e gestire le politiche di sicurezza, creare ed eliminare utenti (ruoli Crypto Officer e Crypto User). Per ogni dispositivo può essere configurato un solo utente nel ruolo SO.
- **Crypto Officer (CO)**: autorizzato a creare, utilizzare, distruggere ed eseguire il backup/ripristino del materiale crittografico. Un dispositivo può avere un solo un solo utente nel ruolo CO per partizione.

- **Crypto User (CU)**: autorizzato al solo uso del materiale crittografico (ad esempio, per operazioni di firma, cifratura e decifratura).

Il ruolo CU è opzionale e può esserne assegnato solamente uno per partizione. Un utente autenticato non può assumere contemporaneamente il ruolo di CO e CU.

Gli utenti nei ruoli sopra indicati vengono autenticati, a seconda dei privilegi associati, mediante una combinazione di un *token* crittografico, di un PIN inserito mediante un dispositivo dedicato (*trusted PIN entry device*) e di una password (*challenge secret*) inviata dal client al dispositivo mediante il canale sicuro implementato dall'apparato Luna® SA.

Figura 3 – SafeNet Luna PED II e iKey

I *token* crittografici e il dispositivo per l'inserimento del PIN da utilizzare con l'apparato Luna® SA sono il Luna PED II e le iKey di SafeNet illustrate in Figura 3 (non facenti parte dell'ODV).

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 Configurazioni valutate dell'ODV

Il dispositivo Luna PCI-E include il seguente componente certificato CC, come specificato nel cap. 1.3.1 del Traguardo di Sicurezza [TDS] e nel cap. 2.8 (*Evaluated Configuration*) del rapporto di Certificazione [CR]:

- Luna® PCI-E Cryptographic Module:
    - Firmware Version: 6.10.9.
    - Hardware Version: 808-00015-003

L'ODV può essere fornito come scheda PCIe autonoma (*standalone*) o inserita in un apparato Luna® SA (ODV *embedded*).

Solamente la configurazione del dispositivo come modulo crittografico inserito in un apparato Luna® SA è risultata 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 [PR], a condizione che vengano rispettate le prescrizioni per l'utilizzo del dispositivo indicate nel cap. 8 del presente Rapporto di Accertamento.

Si suggerisce di verificare con il Produttore quali modelli di apparati Luna® SA supportano l'ODV in configurazione certificata.

La configurazione del dispositivo come modulo crittografico *standalone* non è stata oggetto di Accertamento di Conformità.

6.3 Identificazione sintetica dell'accertamento

Richiedente l'accertamento	SafeNet Canada, Inc.
Nome del dispositivo	Luna® PCI-E Cryptographic Module used as an embedded device in Luna® SA
Versione del dispositivo	Firmware version: 6.10.9 Hardware version: 808-00015-003
Traguardo di Sicurezza	"LUNA® PCI-E Cryptographic Module Security Target", CR-3524, Rev. 23, 5 dicembre 2017 [TDS]
Livello di garanzia	EAL4 con aggiunta di ALC_FLR.2 e AVA_VAN.5
Versione dei CC	3.1 Rev.5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della Procedura	9 marzo 2018
Data di rilascio Certificato CC	29 dicembre 2017
Data di rilascio Accertamento	12 giugno 2018

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 scaduto o 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 Luna PCI-E deve essere utilizzato seguendo tutte le prescrizioni contenute nel Traguardo di Sicurezza [TDS], nel Rapporto di Certificazione [RC] e nella documentazione di guida fornita con l'ODV [CCUG].

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 nel cap. 2.2 di [CCUG].

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 Inizializzazione e personalizzazione del dispositivo

Il proprietario di una partizione sul dispositivo (*partition owner*) è il soggetto che detiene il controllo esclusivo delle chiavi di sottoscrizione (SCD) di cui è titolare memorizzate nella partizione stessa, ossia il firmatario o il creatore di un sigillo.

Al momento della creazione della sua partizione da parte del gestore del dispositivo, ossia l'utente amministrativo nel ruolo Security Officer (SO), al firmatario è assegnato il ruolo Crypto Officer (CO) che permette di svolgere sia operazioni di "amministrazione" della partizione, sia operazioni che prevedono l'utilizzo delle chiavi di sottoscrizione.

Il CO effettua il login in locale per mezzo del *token* di autenticazione "Black iKey", unitamente all'inserimento di una password (*challenge secret*) mediante l'interfaccia a linea di comando. Entrambi questi passi sono necessari per poter generare o utilizzare le chiavi di sottoscrizione memorizzate all'interno di una singola partizione.

A sua discrezione, il firmatario può richiedere la creazione del ruolo limitato Crypto User (CU), abilitato al solo utilizzo da remoto delle chiavi crittografiche, senza la possibilità di configurare o amministrare la partizione. In questo caso, il dispositivo genera due *challenge secret* distinti, uno per il ruolo CO, uno per il ruolo CU.

I *challenge secret* iniziali vengono mostrati in chiaro sul display del dispositivo Luna PED II connesso all'apparato Luna® SA.

Per ottenere e mantenere il controllo esclusivo dell'uso delle chiavi di sottoscrizione in caso di accesso al dispositivo da remoto, le procedure di inizializzazione e personalizzazione del dispositivo devono prevedere quanto segue:

- la partizione deve essere creata in presenza del proprietario/firmatario[1];

[1] Se la partizione non è stata creata in presenza del firmatario, il firmatario deve assicurarsi di impostare un nuovo valore per il *challenge secret* prima della generazione delle chiavi nella partizione, al fine di garantire il controllo esclusivo.

- la generazione delle chiavi di sottoscrizione deve essere effettuata esclusivamente all'interno del dispositivo in presenza del proprietario/firmatario[2];
- i *challenge secret* generati durante l'inizializzazione debbono essere rivelati/comunicati al solo utente firmatario; nessun soggetto non autorizzato al loro utilizzo, incluso l'amministratore del dispositivo, deve venirne a conoscenza;
- il gestore del dispositivo deve consegnare il dispositivo di autenticazione "Black iKey" al firmatario immediatamente, alla conclusione della procedura di inizializzazione e personalizzazione.

Ai fini del mantenimento del controllo esclusivo sulle chiavi di sottoscrizione di cui è titolare conservate nel dispositivo, il firmatario sarà tenuto ad assicurare la custodia del dispositivo "Black iKey" e a mantenere la riservatezza dei codici personali (*challenge secret*).

8.2 Protezione della confidenzialità dei dati di autenticazione

Una volta attivata una partizione mediante l'uso in locale della "Black iKey", è possibile per il firmatario o creatore di un sigillo accedere da remoto alle proprie chiavi di sottoscrizione da una postazione client registrata e autorizzata unicamente mediante l'inserimento del *challenge secret*. Tale sistema di autenticazione non può essere considerato un metodo di autenticazione forte.

Si precisa che per "postazioni client" si intendono i computer sui quali è installato e configurato il software client fornito dal produttore e che comunicano con l'apparato Luna® SA mediante connessioni di rete sicure NTL (si veda [CCUG] cap. 2.1.3.3). Le connessioni NTL utilizzano autenticazione reciproca mediante certificati digitali e cifratura TLS per proteggere i dati sensibili in transito tra le postazioni client e le partizioni attive sul dispositivo Luna® PCI-E.

Il canale sicuro di comunicazione tra le postazioni client e il dispositivo, implementato dall'apparato Luna® SA, risulta quindi adeguato a proteggere efficacemente la confidenzialità dei dati in transito dalla SCA al dispositivo, inclusi i dati di autenticazione, e a garantire l'integrità della rappresentazione dei dati da firmare [DTBS(R)], a patto che questi vengano generati ed inviati al dispositivo in modo corretto.

Nel caso in cui la SCA faccia parte di un'architettura *multi-tier* e/o preveda che i firmatari accedano ad essa remotamente, da una postazione diversa dalla "postazione client", l'ambiente operativo in cui il dispositivo certificato è installato dovrà comunque garantire la sicurezza del canale di comunicazione tra la postazione utilizzata fisicamente dal titolare delle chiavi di sottoscrizione e la SCA, in modo tale da proteggere adeguatamente la riservatezza dei dati di autenticazione e l'integrità dei dati da firmare trasmessi al dispositivo per l'operazione di firma o di apposizione di un sigillo elettronico.

[2] Tale condizione è da intendersi soddisfatta anche nel caso in cui il proprietario/firmatario genera le proprie chiavi operando da una postazione dislocata in un luogo diverso da quello in cui il dispositivo è custodito, mediante un applicativo che gli consenta comunque di mantenere il controllo esclusivo sull'operazione. Questo a patto che ciò avvenga previa autenticazione, secondo le modalità descritte nel Traguardo di Sicurezza [TDS], e rispettando altresì i requisiti di sicurezza richiesti per il canale di comunicazione tra la postazione stessa e il dispositivo di firma.

In questo caso, l'architettura del server di firma remota gestito per conto dell'utilizzatore (firmatario o creatore di un sigillo) da un prestatore di servizi fiduciari qualificato ai sensi del Regolamento eIDAS, dovrà altresì prevedere l'implementazione di un sistema di autenticazione forte (ad es., a 2 fattori) a supporto del meccanismo di *challenge/response* implementato dal dispositivo.

8.3 Politica di sicurezza del dispositivo

L'amministratore deve configurare il dispositivo in maniera conforme a quanto dichiarato nel TDS (si veda [TDS] cap. 7.2. - *Capability and Policy Settings*) seguendo scrupolosamente la guida per l'installazione sicura fornita col prodotto certificato (si veda [CCUG] cap. 2.4.3.6 - *CC Compliant Settings*).

Inoltre, per l'utilizzo come dispositivo per la creazione di una firma elettronica qualificata e/o come dispositivo per la creazione di un sigillo elettronico qualificato, debbono essere configurate le seguenti opzioni di sicurezza aggiuntive.

Politica di sicurezza a livello di HSM:

- *Force user PIN change after set/reset*: **On**

Politica di sicurezza a livello di singola partizione:

- *Perform RSA signing without confirmation*: **Off**
- *Minimum pin length (inverted: 255 - min)*: **<= 239** (ossia minimo 16 caratteri, si veda anche la raccomandazione al cap. 9.1)
- *Max failed user logins allowed*: massimo **5**.

8.4 Algoritmi crittografici

Gli algoritmi crittografici utilizzati dalle funzioni di sicurezza (TSF) del dispositivo certificato sono elencati nel Traguardo di Sicurezza (si veda [TDS] cap. 7.3.9 – *Cryptography*), così come nella formulazione dei requisiti funzionali di sicurezza (SFR) della classe FCS: *Cryptographic Support* (si veda [TDS] cap. 6.1.1 - *Cryptographic operation and key management*).

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 con il dispositivo oggetto dell'Accertamento è consentito l'uso solamente dei seguenti algoritmi crittografici:

- **Funzioni di *hash*:**
    - SHA-256, SHA-384 e SHA-512.

- **Metodi di sottoscrizione:**
    - RSA con *padding* RSA-PKCS1v1_5 o RSA-PSS (raccomandato), con lunghezza di chiave non inferiore a 2048 bit.
    - ECDSA (raccomandato), a patto che vengano utilizzate esclusivamente le curve indicate in [ESI-CS], cap. 6.2.2.3 – *Agreed Elliptic Curve Parameters*, Tabella 3.
    - DSA è consentito, ove applicabile, ma non raccomandato in presenza di metodi di sottoscrizione alternativi.

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*).

9 Raccomandazioni

9.1 Scelta del challenge secret

Si premette che il *challenge secret* iniziale, in forma di stringa di 16 caratteri casuali, viene generato dal dispositivo mediante l'uso del proprio generatore random interno, la cui adeguatezza e robustezza è garantita dalla certificazione di sicurezza ottenuta.

A causa della criticità di questo segreto che, unitamente al dispositivo "Black iKey", consente al titolare delle chiavi di sottoscrizione memorizzate nel dispositivo di mantenere il controllo esclusivo del loro utilizzo, è essenziale che le caratteristiche di sicurezza di tale dato di autenticazione siano mantenute inalterate durante l'intero ciclo di vita del dispositivo.

A questo scopo si raccomanda che il firmatario, all'atto della modifica del *challenge secret* iniziale, generi una nuova password sulla base dell'entropia estratta dal modulo crittografico. Questo può essere ottenuto, ad esempio, mediante l'uso dello strumento software CKDemo, fornito con il dispositivo. Scegliendo dal menu l'opzione (62) *Generate Random Number* è possibile estrarre dall'HSM una quantità specifica di dati casuali (numero di byte) che può essere utilizzata per generare un nuovo *challenge secret* con una robustezza equivalente.

In alternativa, può anche essere consentito all'utente di impostare *challenge secret* di propria scelta, a patto che la partizione venga configurata per accettare password di lunghezza non inferiore a 16 caratteri e che venga impostata una password di robustezza equivalente.

9.2 Backup e ripristino di chiavi di sottoscrizione

Il dispositivo certificato realizza una funzionalità di backup e ripristino del materiale crittografico, incluse le chiavi private, memorizzato in una singola partizione. Ogni partizione può essere replicata su un dispositivo denominato "Luna® Backup HSM" mediante l'uso del "Luna® Key Cloning protocol" (si veda [TDS] cap. 1.4.8 - *Backup and Restoration*). Il materiale crittografico contenuto in un dispositivo di backup può essere ripristinato su una partizione creata in un diverso dispositivo, opportunamente inizializzato.

Il trasferimento del materiale crittografico tra i due dispositivi è realizzato dalle funzionalità di sicurezza del dispositivo certificato con un livello di robustezza adeguato a proteggere la confidenzialità e l'integrità delle chiavi di sottoscrizione, compresi tutti i loro attributi.

Per l'utilizzo come dispositivo per la creazione di una firma elettronica qualificata e/o come dispositivo per la creazione di un sigillo elettronico qualificato, è necessario che il backup delle chiavi di sottoscrizione avvenga nel rispetto dei limiti imposti dal requisito 4 dell'Allegato II al Regolamento (UE) n. 910/2014 [eIDAS].

La funzionalità di backup e ripristino del dispositivo accertato, così come descritta nel TDS, appare essere conforme al suddetto requisito per quanto attiene alla replicazione delle chiavi di sottoscrizione, a patto che i prestatori di servizi fiduciari qualificati che

gestiscono le chiavi di sottoscrizione per conto del firmatario e/o del creatore di un sigillo utilizzino questa funzionalità esclusivamente per motivi di ripristino in caso di guasto o di aggiornamento di un dispositivo in uso, limitando al minimo necessario il numero di istanze duplicate dei dati in esso contenuti.

Inoltre, è necessario che i dispositivi di backup siano installati nello stesso ambiente operativo del dispositivo certificato, sottoposti alle stesse misure di sicurezza di tipo fisico e procedurale, così come prescritto dagli obiettivi di sicurezza per l'ambiente operativo descritti nel Traguardo di Sicurezza (si veda in particolare [TDS] cap. 4.2.6 - *OE.Env – Protected operating environment*).