Ministero dello Sviluppo Economico

Dipartimento per le Comunicazioni

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 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. 1/12

Dispositivo: Luna® PCI Configured for Use in Luna SA 4.1

Sviluppato da: SafeNet, Inc.

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, 12 dicembre 2012

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/SFNT/01/2011/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

Dipartimento per le Comunicazioni

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

Luna® PCI Configured for Use in Luna SA 4.1

OCSI/ACC/SFNT/01/2011/RA

Versione 1.0

12 dicembre 2012

Questa pagina è lasciata intenzionalmente vuota

1 Indice

2 Elenco degli acronimi

API Application Programming Interface

CC Common Criteria

DL Decreto Legislativo

DPCM Decreto della Presidenza del Consiglio dei Ministri

DTBS(R) Data To Be Signed (Representation)

EAL Evaluation Assurance Level

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto della Valutazione

PP Profilo di Protezione (Protection Profile)

SCD Signature Creation Data

SFP Security Function Policy

SFR Security Functional Requirement (Requisito Funzionale di Sicurezza)

SSCD Secure Signature Creation Device

SVD Signature Verification Data

TDS Traguardo di Sicurezza (Security Target)

TSF TOE Security Function

3 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.

[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.

[ETS] “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”, ETSI TS 102 176-1 V2.1.1 (2011-07), Technical Specification

[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] Certification Report, “Luna® PCI Configured for Use in Luna SA 4.1 with Backup”, NSCIB-CC-07-09219-CR, 2 novembre 2009

[TDS] "Luna® PCI Configured for Use In Luna® SA 4.1 With Backup Security Target", CR-2386, revisione 11, 17 settembre 2009.

4 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 di firma denominato "Luna® PCI Configured for Use In Luna® SA 4.1", prodotto dalla società SafeNet, Inc. (nel seguito indicato come "dispositivo oggetto dell'Accertamento" o semplicemente "dispositivo").

Al dispositivo si applica, alla data di avvio della procedura di Accertamento (vedi cap. 5.2), 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].

5 Riepilogo dell'accertamento

5.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo denominato "Luna® PCI Configured for Use In Luna® SA 4.1", prodotto dalla società SafeNet, 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 l'apposizione di firme elettroniche qualificate con procedure automatiche.

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).

Il dispositivo oggetto dell'Accertamento, così come descritto nel relativo Traguardo di Sicurezza [TDS], è risultato 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 con procedure automatiche.

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. 6), 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.

5.2 Identificazione sintetica dell'accertamento

Richiedente l'accertamento	SafeNet, Inc.
Nome del dispositivo	Luna® PCI Configured for Use In Luna® SA 4.1
Identificativo dell'ODV	Luna PCI Hardware Version VBD-03-0100 (part number 900691-000), Firmware Version 4.6.1
Traguardo di Sicurezza	"Luna® PCI Configured for Use In Luna® SA 4.1 With Backup Security Target", CR-2386, revisione 11, 17 settembre 2009
Livello di garanzia	EAL4 con aggiunta di ADV_IMP.2, ALC_FLR.2, AVA_CCA.1, AVA_MSU.3, AVA_VLA.4
Versione dei CC	2.3
Conformità a PP	CWA 14167-2, "Cryptographic Module for CSP Signing Operations with Backup (CMCSOB) Protection Profile", version 0.28, 27 October 2003
Data di inizio della Procedura	11 aprile 2011
Data di fine della Procedura	30 novembre 2012

5.3 Descrizione del dispositivo accertato

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

La scheda PCI è contenuta in un guscio di sicurezza che fornisce resistenza fisica alla

manomissione e garantisce la cancellazione sicura, mediante azzeramento, del materiale crittografico e degli altri dati sensibili memorizzati sulla scheda stessa, nel caso venga rilevato un tentativo di manomissione.

Il dispositivo certificato (ODV) include i seguenti componenti:

- il modulo crittografico Luna® PCI (900691-000 con Firmware Versione 4.6.1);
- un dispositivo Luna® PIN Entry Device (PED) (Firmware Versione 2.0.2) e iKeys;
- libreria di API e driver (versione 4.1),
- Luna SA 4.1 Guidance Documentation (900506-037, Revisione B).

Le funzioni di sicurezza del dispositivo sono realizzate interamente all'interno dei confini fisici del modulo crittografico Luna® PCI. Il dispositivo fornisce funzionalità per la gestione sicura di materiale crittografico, che consentono di mantenere la confidenzialità e l'integrità di chiavi di sottoscrizione (SCD) e di cifratura. Il materiale crittografico è generato, memorizzato ed utilizzato esclusivamente all'interno dei confini di sicurezza del dispositivo certificato.

In particolare, 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 la creazione e distruzione delle chiavi;
- controllo di accesso per le funzioni di amministrazione delle funzioni di sicurezza;
- controllo di accesso per l'utilizzo delle chiavi per funzioni crittografiche e di firma;
- Self-test del dispositivo.

Per maggiori informazioni sulla politica di sicurezza realizzata dall'ODV si faccia riferimento al cap. 2 di [TDS].

6 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 (v. [CR]) 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. 7 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 (OCSI) emettitore 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.

7 Condizioni di utilizzo del dispositivo accertato

7.1 Inizializzazione e personalizzazione del dispositivo

Si premette che il proprietario di una partizione sul dispositivo (*partition owner*) è il soggetto che detiene il controllo esclusivo delle chiavi di sottoscrizione di cui è titolare memorizzate nella partizione stessa, ossia il *firmatario*. 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, effettuando il login da locale per mezzo del dispositivo di autenticazione “Black iKey”, sia operazioni di utilizzo delle chiavi di firma, effettuando il login da una postazione remota utilizzando una password (*challenge secret*). A sua discrezione, il firmatario può richiedere per sé stesso la creazione, in aggiunta, del ruolo limitato *Crypto User* (CU), abilitato al solo utilizzo da remoto delle chiavi crittografiche. 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 (v. ad es. [TDS] cap. 2.5) connesso all'HSM.

Ciò premesso, le procedure di inizializzazione e personalizzazione del dispositivo devono prevedere quanto segue:

- La partizione deve essere creata in presenza del proprietario/firmatario.
- La generazione delle chiavi di sottoscrizione deve essere effettuata esclusivamente all'interno del dispositivo, sulla partizione appena creata, in presenza del proprietario/firmatario.
- 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.

In base alla normativa vigente in materia di firma elettronica, 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*).

7.2 Protezione della confidenzialità dei dati di autenticazione

Si premette che, una volta attivata una partizione mediante l'uso in locale della “Black iKey”, è possibile per il firmatario accedere da remoto alle proprie chiavi di sottoscrizione per l'apposizione di firme elettroniche da una postazione registrata e autorizzata unicamente mediante l'inserimento del *challenge secret*. Tale sistema di autenticazione non può essere considerato un metodo di autenticazione forte.

Risulta quindi di fondamentale importanza che la trasmissione di tale dato, ancorché protetto dal meccanismo di *challenge/response* implementato dal dispositivo, avvenga unicamente attraverso un canale sicuro realizzato nell'ambiente operativo del dispositivo, come prescritto in [TDS], v. cap. 4.2. - *Security Objectives for the IT Environment* - e cap. 5.3.5. - *Trusted path (FTP)*.

Si ritiene che la soluzione di sicurezza realizzata dall'apparato Luna® SA, che costituisce un componente dell'ambiente operativo del dispositivo certificato (v. [TDS] cap. 2 - *TOE Description*), mediante *Network Trust Link Server* (NTLS) sia adeguata a proteggere efficacemente la confidenzialità dei dati in transito dalla SCA al dispositivo in quanto, pur non essendo realizzata dalle TSF dell'ODV, è stata sottoposta a verifiche di correttezza funzionale e test di penetrazione indipendenti nell'ambito del processo di valutazione a cui il dispositivo è stato sottoposto (v. [RC], cap. 2.6.3 - *Independent Penetration Testing*).

Risulta quindi necessario, in sede di sorveglianza, verificare che il dispositivo reale sia stato installato nell'ambiente operativo previsto e configurato correttamente, secondo quanto prescritto dalle Guide per l'Utente e l'Amministratore dell'ODV, parte dell'ODV e fornite dal produttore con il dispositivo certificato.

7.3 Sicurezza delle postazioni client e della SCA

Come già evidenziato nel cap. precedente, il sistema di autenticazione del firmatario attraverso il login mediante *challenge secret* – una volta attivata la propria partizione mediante la “Black iKey” – non può essere considerato un metodo di autenticazione forte.

È necessario quindi che le postazioni client siano installate in un ambiente adeguatamente protetto dal punto di vista fisico ed utilizzate esclusivamente da utenti specificamente autorizzati dall'organizzazione di appartenenza.

Dato che il dispositivo non è in grado di identificare i diversi utenti che potenzialmente accedono ad una singola postazione client per operazioni di firma, è necessario garantire almeno che:

- le postazioni client siano correttamente configurate, registrate ed assegnate alle

partizioni del dispositivo in modo da autorizzare l'accesso agli utenti delle postazioni stesse unicamente alle partizioni contenenti le chiavi di sottoscrizione di cui sono titolari. Tale configurazione deve essere effettuata dall'amministratore del dispositivo (o dalla figura equivalente individuata dall'azienda di appartenenza dell'utente);

- le postazioni siano di tipo fisso (è da escludere l'uso di PC portatili o altri dispositivi di tipo mobile o trasportabile), connesse al dispositivo unicamente attraverso una rete aziendale privata con connessioni di tipo ethernet protette mediante le funzionalità di sicurezza previste per l'ambiente di utilizzo del dispositivo (NTLS);
- la singola postazione sia dedicata esclusivamente alle operazioni di firma e, ove possibile, sia adibita all'uso del solo utente (non amministrativo) titolare delle chiavi memorizzate nella partizione del dispositivo per la quale la postazione è registrata ed autorizzata all'accesso;
- le postazioni siano configurate in modo da richiedere come minimo userid e password dell'utente prima di consentire l'accesso al sistema e agli applicativi e siano dotate di misure di sicurezza standard (personal firewall, antivirus), possibilmente definite all'interno di una politica di sicurezza aziendale, tali da minimizzare i rischi derivanti dalla presenza di software non autorizzati o malevoli e dall'accesso di utenti non autorizzati;
- i sistemi operativi utilizzati sulle postazioni client debbono essere configurati in modo tale da forzare l'utente ad usare password robuste, a cambiarle periodicamente e a non lasciare sessioni di lavoro aperte non custodite;
- le applicazioni per la creazione delle firme elettroniche (SCA) installate sulle postazioni client debbono essere unicamente quelle fornite ad autorizzate dall'amministratore di rete (o dalla figura equivalente individuata dall'azienda di appartenenza dell'utente). Esse debbono avere caratteristiche note di correttezza e affidabilità nel fornire l'interfaccia utente al firmatario per la richiesta dei servizi di firma al dispositivo e nel proteggere l'integrità dei dati da firmare (DTBS) sul sistema host, così come nel garantire che la rappresentazione dei dati da firmare [DTBS(R)] venga generata ed inviata al dispositivo in modo corretto, conformemente ai requisiti per l'ambiente operativo espressi nel TDS. Le SCA debbono inoltre consentire al firmatario di scegliere e visionare i documenti da firmare prima di esprimere la volontà di apporre la firma su di essi, ove prescritto dalla normativa vigente in materia di firma elettronica.
- le SCA devono essere realizzate e configurate in modo da richiedere al firmatario l'inserimento del *challenge secret* ogni volta che si attiva una sessione verso il dispositivo per operazioni di firma, anche di tipo massivo. Il *challenge secret* non deve in alcun modo essere memorizzato in modo permanente sulla postazione client.

7.4 Politica di sicurezza del dispositivo

L'amministratore deve configurare il dispositivo in maniera conforme a quanto dichiarato nel TDS (v. [TDS] cap. 6.2. - *Capability and Policy Settings*), seguendo scrupolosamente la

guida per l'installazione sicura fornita col prodotto certificato.

Inoltre, per un utilizzo del dispositivo come SSCD, debbono essere configurate le seguenti opzioni di sicurezza aggiuntive.

Politica di sicurezza a livello di HSM:

- Allow/disallow forcing change of User authentication data (PIN) after set/reset: **ON**

Politica di sicurezza a livello di singola partizione:

- Allow/disallow High Availability Recovery: **OFF**
- Allow/disallow incrementing of failed login attempt counter on failed challenge response validation: **OFF**
- Allow/disallow RSA signing without confirmation: **OFF**
- Minimum/maximum password length: (max pin) – (min pin) >= **16** (v. anche raccomandazione al cap. 8.1)
- Number of failed Partition User logins allowed before partition is locked out/cleared: massimo **5**.

7.5 Algoritmi crittografici

Il TDS elenca gli algoritmi crittografici utilizzati dalle TSF nel cap. 6.3.12 – *Cryptography*, oltre che nella formulazione dei requisiti funzionali specifici della famiglia FCS (v. [TDS] capp. 5.1.2 e 5.2.1).

Conformemente alla versione corrente dello standard ETSI di riferimento per gli algoritmi crittografici ([ETS]) e alla normativa Italiana vigente in materia di firma elettronica, solamente i seguenti algoritmi e parametri, tra quelli supportati dal dispositivo accertato, possono essere utilizzati.

Funzioni di hash

Per la generazione e la verifica di firme elettroniche deve essere utilizzata unicamente la funzione SHA-256.

Generazione di coppie di chiavi crittografiche

Per la generazione di nuove coppie di chiavi crittografiche deve essere utilizzato unicamente l'algoritmo RSA con lunghezza di chiavi non inferiore a 2048 bit.

Metodi di sottoscrizione

Per la generazione e la verifica di firme elettroniche conformi alla specifica ETSI TS 102 176-1 deve essere utilizzato unicamente il metodo di sottoscrizione *sha256-with-rsa* con

padding conforme alla specifica RFC 3447 (indicato in [TDS] come PKCS #1 V1.5, PKCS #1 PSS).

8 Raccomandazioni

8.1 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 memorizzate nel dispositivo di mantenere l'uso esclusivo delle stesse, è essenziale che le caratteristiche di sicurezza di tale dato di autenticazione siano mantenute inalterate durante l'intero ciclo di vita del dispositivo stesso. Si consideri inoltre che la robustezza delle funzioni di sicurezza dell'ODV dichiarata nel TDS e confermata dalla certificazione CC (*Strength of Function*: SoF-High), viene mantenuta solamente se i segreti generati dall'ODV ed utilizzati dalle TSF hanno le caratteristiche di sicurezza indicate nel TDS stesso (v. [TDS] cap. 6.4. *Strength of Function*).

A questo scopo si raccomanda che il firmatario, all'atto della modifica del *challenge secret* iniziale, utilizzi la funzione di generazione casuale del segreto fornita dal dispositivo certificato, scegliendo l’opzione (2) visualizzata dal comando di <partition changePw> attraverso la Command Line Interface (CLI).

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.

8.2 Backup e ripristino di chiavi di sottoscrizione

Alla data della stesura del presente Rapporto di Accertamento, la bozza delle regole tecniche sulle firme elettroniche, pubblicata sul sito dell'Agenzia per l'Italia Digitale (ex DigitPA) ed in attesa di emanazione da parte dell'organo legislativo competente, prevede (v. art. 8, comma 3) la possibilità di esportare chiavi private al di fuori di un dispositivo sicuro di firma, esclusivamente per motivi di ripristino in caso di guasto o di aggiornamento del dispositivo in uso, purché cifrate con algoritmi ritenuti adeguati ai fini della certificazione e purché le operazioni di esportazione e importazione delle chiavi siano effettuate mediante funzionalità di sicurezza certificate implementate dal dispositivo di firma. Le stesse regole tecniche prevedono, inoltre, che la conservazione delle chiavi esportate debba avvenire nell'ambiente operativo del dispositivo, sottoposta a opportune misure di sicurezza di tipo fisico e procedurale che debbono essere descritte, in forma di obiettivi o ipotesi per l'ambiente, nel relativo Traguardo di Sicurezza.

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 Token” mediante l'uso del “Luna® Key Cloning protocol” (v. [TDS] cap. 6.3.21 - *Backup and Recovery*). Il materiale crittografico contenuto in un Backup Token può essere ripristinato su una partizione creata in un diverso dispositivo, opportunamente inizializzato.

Allo stato attuale, la funzionalità di backup e ripristino del dispositivo accertato, così come descritta nel TDS, appare essere conforme alle disposizioni dell'attuale versione delle regole tecniche sopra citate.

Si raccomanda tuttavia, in sede di sorveglianza, di verificare che la modalità di gestione delle chiavi da parte del dispositivo accertato sia in linea con quanto previsto dalle regole tecniche sulle firme elettroniche al momento in vigore, per quanto attiene alla replicazione delle chiavi di sottoscrizione.

8.3 Limitazione alla configurazione per High Availability

Alla data della stesura del presente Rapporto di Accertamento, la bozza delle regole tecniche sulle firme elettroniche, pubblicata sul sito dell'Agenzia per l'Italia Digitale (ex DigitPA) ed in attesa di emanazione da parte dell'organo legislativo competente, prevede (v. art. 8, comma 4) la possibilità di realizzare una configurazione ad alta affidabilità del dispositivo sicuro di firma a condizione, tra le altre, che solo uno dei dispositivi fisici in questa configurazione sia abilitato ad effettuare le operazioni di firma.

Le funzionalità rese disponibili dal dispositivo certificato per la configurazione in *High Availability* (HA) prevedono che la SCA si interfacci con un dispositivo in HA tramite l’indirizzamento di uno slot virtuale dietro al quale si attestano in modo trasparente all’applicazione due o più slot corrispondenti a HSM reali, sui quali il materiale crittografico viene replicato automaticamente.

Per far sì che il dispositivo certificato ottemperi alle prescrizioni della normativa Italiana è necessario limitare tali funzionalità, realizzando una configurazione alternativa. Tale configurazione alternativa prevede che la HA venga realizzata a livello applicativo richiedendo in modo “esplicito” la *network replication* per la replicazione in maniera sicura delle chiavi private e non sfruttando la visibilità come un unico dispositivo del gruppo di HA (*cluster*). Ciò è possibile richiedendo che l’applicazione indirizzi lo slot reale della partizione, e non quello virtuale associato al gruppo di HA, e pertanto compia operazioni di firma con un solo HSM fisico “primario”. Nel momento in cui tale HSM primario non dovesse rispondere, ad. es a causa di un guasto, è necessario ed è responsabilità dell’applicazione aprire una nuova sessione verso lo slot associato ad un HSM secondario nel gruppo. Le logiche di passaggio dallo slot dell’HSM primario al secondario e viceversa vanno dunque gestite a livello applicativo.

Si raccomanda, in sede di sorveglianza, di verificare che la configurazione in HA del dispositivo accertato, qualora utilizzata, sia in linea con quanto previsto dalle regole tecniche sulle firme elettroniche al momento in vigore, per quanto attiene alle configurazioni ad alta affidabilità dei dispositivi di firma.