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

Note Interpretative sul Rapporto di Accertamento del dispositivo di firma "Luna® PCI Configured for Use in Luna SA 4.1"

OCSI/ACC/SFNT/01/2011/NI

Versione 1.0

21 maggio 2013

Riferimenti

[RA] Rapporto di Accertamento del dispositivo di firma "Luna® PCI Configured for Use in Luna SA 4.1", OCSI/ACC/SFNT/01/2011/RA, Versione 1.0, 12 dicembre 2012.

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

Scopo del documento

In relazione al Rapporto di Accertamento del dispositivo di firma "Luna® PCI Configured for Use in Luna SA 4.1" [RA], si rendono disponibili alcune note interpretative, volte a chiarire aspetti specifici riguardanti le modalità d'uso dell'apparato in questione.

Il presente documento va consultato unitamente al citato Rapporto di Accertamento, di cui costituisce allegato.

Note Interpretative

Nota 1 – Generazione delle chiavi di sottoscrizione

Nel cap. 7.1 (Inizializzazione e personalizzazione del dispositivo) di [RA], al secondo punto elenco si afferma:

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

L'inciso "sulla partizione appena creata" va considerato rimosso in quanto, per motivi legati alle reali modalità operative e agli strumenti messi a disposizione dal produttore del dispositivo per la generazione delle chiavi di firma, il momento temporale di creazione delle chiavi è necessariamente svincolato da quello di creazione della partizione.

Per quanto riguarda la richiesta che la generazione delle chiavi avvenga in presenza del firmatario, questa è da intendersi soddisfatta anche nel caso in cui il 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 del dispositivo certificato [TDS], e rispettando altresì i requisiti di sicurezza richiesti per il canale di comunicazione tra la postazione stessa e il dispositivo di firma.

Nota 2 – Postazioni client

Con riferimento al cap. 7.3 (Sicurezza delle postazioni client e della SCA) di [RA], si precisa che per “postazioni client” si intendono i computer sui quali è installato e configurato il software “Luna Software”, secondo quanto prescritto dalle Guide per l'Utente e l'Amministratore dell'ODV, fornito dal produttore con il dispositivo certificato (vedere [TDS], cap. 1.2 - ST Overview e cap. 2.11 - Environment).

Ciò premesso, fatto salvo quanto prescritto nel cap. 7.2 (Protezione della confidenzialità dei dati di autenticazione) di [RA], nel caso in cui l'applicazione per la creazione della firma elettronica (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 garantire la riservatezza dei dati di autenticazione e dei dati da firmare trasmessi al dispositivo per l'operazione di firma.

Nota 3 – Sicurezza delle postazioni client

Nel cap. 7.3 (Sicurezza delle postazioni client e della SCA) di [RA], al terzo punto elenco si richiede che:

“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”.

Si precisa che tale prescrizione è da intendersi come raccomandazione.