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. 3/19

Dispositivo: distributed remote Qualified Signature Creation Device (drQSCD) v1.0

Sviluppato da: I4P-Informatikai Kft. (I4P Ltd.)

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, 25 luglio 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/I4P/03/2019/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

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

distributed remote Qualified Signature Creation Device (drQSCD) v1.0

OCSI/ACC/I4P/03/2019/RA

Versione 1.0

25 luglio 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	25/07/2019

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CEN	Comité Européen de Normalisation
CM	Cryptographic Module
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
EN	European Norm
HSM	Hardware Security Module
ISO	International Organization for Standardization
MPC	Multi-Party Computation
MPCA	Multi-Party Cryptographic Appliance
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PP	Profilo di Protezione (Protection Profile)
RSA	Rivest, Shamir, Adleman
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SHA	Secure Hash Algorithm
QSCD	Qualified Signature Creation Device
SFR	Security Functional Requirement
TDS	Traguardo di Sicurezza (Security Target)
TOE	Target Of Evaluation

TOTP	Time-based One-Time Password (algorithm)
TSF	TOE Security Functions
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing

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

[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)

[PP-CM] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, prEN 419 221-5, v015, 29 November 2016

[PP-SAM] “Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing”, prEN 419 241-2, v0.16, 11 May 2018

[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] Rapporto di Certificazione “distributed remote Qualified Signature Creation Device (drQSCD) v1.0”, v1.0, 15 maggio 2019

[TDS] Security Target “distributed remote Qualified Signature Creation Device(drQSCD)”, drQSCD-ST, v1.2, 2 May 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 il dispositivo denominato "distributed remote Qualified Signature Creation Device (drQSCD) v1.0"[1], sviluppato dalla società I4P-Informatikai Kft. (I4P Ltd.) (nel seguito indicato brevemente come drQSCD o anche "dispositivo oggetto dell'Accertamento" o semplicemente "dispositivo").

Il drQSCD è un dispositivo multi-utente e multi-chiave, progettato per essere utilizzato come QSCD per la generazione di firme e sigilli elettronici qualificati in conformità al Regolamento eIDAS n. 910/2014 [eIDAS] e per eseguire ulteriori operazioni crittografiche di supporto.

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

Il dispositivo è composto da un applicativo software con funzionalità di Signature Activation Module (SAM) e da un Modulo Crittografico (CM) inseriti in un unico apparato hardware che ne definisce il confine sicuro. Il dispositivo è certificato in conformità ai due Profili di Protezione (PP) prEN 419 241-2 [PP-SAM] e prEN 419 221-5 [PP-CM].

Si noti che i due PP sopra citati ([PP-SAM] e [PP-CM]) sono attualmente in corso di standardizzazione (CEN) al fine di definire una configurazione di riferimento per la certificazione di sicurezza dei dispositivi per la creazione di firme e sigilli elettronici qualificati in modalità remota.

[1] Questo è il nome che identifica il dispositivo certificato CC (ODV). Il dispositivo è attualmente commercializzato da I4P con il nome TRIDENT HSM.

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo drQSCD v1.0, prodotto dalla società I4P Ltd., 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], 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 drQSCD v1.0 è un dispositivo multi-utente e multi-chiave, progettato per essere utilizzato come QSCD per la generazione di firme elettroniche e sigilli elettronici qualificati in conformità al Regolamento eIDAS n. 910/2014 [eIDAS].

Il dispositivo costituisce un sistema affidabile che supporta la firma lato server (TW4S) e offre servizi di firma elettronica da remoto, garantendo che le chiavi di sottoscrizione del Firmatario vengano utilizzate sotto il suo controllo esclusivo e soltanto per gli scopi previsti.

A seconda della sua configurazione, il dispositivo è costituito da una o tre MPCA (*Multi-Party Cryptographic Appliance*).

Nella configurazione cosiddetta **Multi-party Configuration**, il dispositivo è composto da tre MPCA identiche che operano in modo distribuito come una sola unità logica, mentre nel caso della configurazione denominata **Standalone Configuration**, il dispositivo è costituito da un'unica MPCA.

Una MPCA si presenta sotto forma di apparato con *chassis* metallico, montabile su *rack*, come illustrato in Figura 1.

Figura 1 - Aspetto fisico di una MPCA

Il dispositivo certificato (ODV) è formato da due componenti principali, situati all'interno dell'involucro fisico di una MPCA:

- Il componente **Cryptographic Module (CM)** del drQSCD è un modulo crittografico di uso generico che fornisce il supporto crittografico necessario agli utenti del dispositivo.

- Il componente **Signature Activation Module (SAM)** del drQSCD è un'applicazione locale installata all'interno del perimetro protetto da manomissione del drQSCD che implementa il Signature Activation Protocol (SAP). Il SAM utilizza i Signature Activation Data (SAD) di un firmatario remoto per attivare la chiave di sottoscrizione corrispondente da utilizzare all'interno del modulo crittografico.

I componenti CM e SAM dell'ODV forniscono le seguenti funzionalità.

La **funzionalità CM** include, ma non è limitata a:

- generazione, memorizzazione, utilizzo, backup, ripristino e distruzione di chiavi crittografiche simmetriche e asimmetriche;

- garanzia della sicurezza, in termini di riservatezza e integrità, delle chiavi simmetriche e delle chiavi private asimmetriche;

- generazione di firme elettroniche qualificate e sigilli elettronici qualificati;

- supporto all'uso di password *one-time* TOTP per l'attivazione delle chiavi da parte dei loro titolari.

La **funzionalità SAM** include, ma non è limitata a:

- autenticazione a due fattori del firmatario remoto;

- autorizzazione dell'operazione di firma;

- attivazione della chiave di sottoscrizione nella funzionalità CM interna.

La funzionalità SAM dell'ODV garantisce che il firmatario remoto conservi il controllo esclusivo delle proprie chiavi di sottoscrizione per la generazione di firme elettroniche qualificate, come stabilito dall'Allegato II ad [eIDAS].

In caso di configurazione Multi-party, la **funzionalità MPC** include, ma non è limitata a:

- generazione di coppie di chiavi RSA in modo distribuito;
- creazione di firme elettroniche utilizzando un metodo di firma a più passi;
- autenticazione degli utenti finali in modo distribuito.

Il drQSCD garantisce la coerenza interna tra le diverse MPCA. La gestione delle chiavi di sottoscrizione avviene in maniera distribuita, in conformità a quanto prescritto nel PP prEN 419 221-5 [PP-CM].

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

6.2.1 Configurazione certificata del dispositivo

La configurazione certificata del dispositivo drQSCD v1.0 include i seguenti elementi:

- una o tre MPCA (ODV);
- la documentazione di guida, che fornisce informazioni sulla configurazione certificata e consente di installare e utilizzare correttamente il dispositivo.

Maggiori dettagli sono inclusi nel cap. 1.4 (*TOE Description*) del Traguardo di Sicurezza [TDS] e nel cap. 10 (*Configurazione valutata*) del Rapporto di Certificazione [RC].

Il dispositivo drQSCD v1.0 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 [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	I4P-informatikai Kft. (I4P Ltd.)
Nome del dispositivo	distributed remote Qualified Signature Creation Device (drQSCD)
Versione del dispositivo	1.0
Traguardo di Sicurezza	Security Target “distributed remote Qualified Signature Creation Device(drQSCD)”, v1.2, 2 May 2019 [TDS]
Livello di garanzia	EAL4 con aggiunta di AVA_VAN.5 e ALC_FLR.3
Versione dei CC	3.1 Rev. 4
Conformità a PP	prEN 419 241-2, v0.16, 11 May 2018 [PP-SAM] prEN 419 221-5, v015, 29 November 2016 [PP-CM]
Data di inizio della Procedura	30 aprile 2019
Data di rilascio Certificato CC	15 maggio 2019
Data di rilascio Accertamento	25 luglio 2019

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 drQSCD v1.0 deve essere configurato ed utilizzato seguendo tutte le prescrizioni contenute nel Traguardo di Sicurezza [TDS], nel relativo Rapporto di Certificazione [RC] e nella documentazione di guida per l'amministratore fornita con l'ODV.

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].

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 Limitazioni alla configurazione certificata

La certificazione CC del dispositivo drQSCD comprende per il CM sia il caso d'uso "Local Signing", sia quello "Remote Server Signing", così come descritti nel Protection Profile prEN 419 221-5 [PP-CM].

A questo riguardo si precisa che il presente Attestato di Conformità copre unicamente il caso d'uso "Remoto", illustrato in Figura 2.

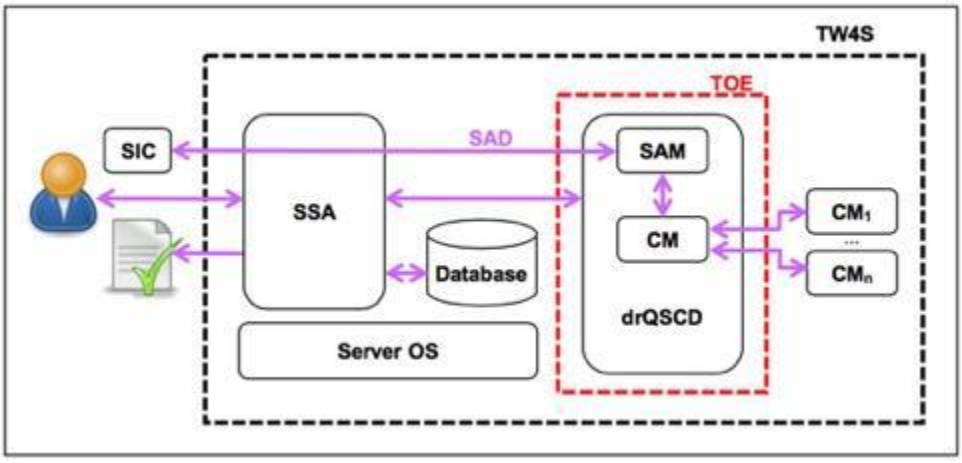

Figura 2 – Il dispositivo drQSCD (TOE) nel caso d'uso "Remoto"

Questa modalità di utilizzo è rivolta ai TSP che soddisfano i requisiti per la creazione di firme o di sigilli elettronici da remoto, come specificato in [eIDAS].

Inoltre, per poter essere utilizzato come QSCD, il dispositivo deve essere opportunamente configurato per utilizzare, assieme al modulo SAM, esclusivamente il componente CM integrato in ogni MPCA.

Solamente i due componenti SAM e CM integrato soddisfano complessivamente i requisiti per i QSCD nel contesto della firma remota, così come descritti nell'Allegato II ad [eIDAS]. L'uso di CM esterni, pur contemplato dalla certificazione, non rientra tra le configurazioni coperte dal presente Attestato di Conformità.

8.2 Algoritmi crittografici

Gli algoritmi crittografici utilizzati dalle funzioni di sicurezza (TSF) del dispositivo certificato sono elencati nel Traguardo di Sicurezza (si veda [TDS] cap. 1.4.2.1 - CM functionality), nella formulazione dei requisiti funzionali di sicurezza (SFR) della classe FCS - *Cryptographic Support* (si veda [TDS] cap. 6.1.2.2).

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 256 bit e con le seguenti curve ellittiche: P-256, P-384, P-512 (si veda [ESI-CS], cap. 6.2.2.3 *EC based DSA algorithms*).

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*).