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. 1/19

Dispositivo: J-SIGN v1.8.9

Sviluppato da: STMicroelectronics, S.r.l.

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)
Rita Forsi

Roma, 21 gennaio 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/STM/08/2018/RA) ad esso allegato, che ne costituisce parte integrante e sostanziale.

Questa pagina è lasciata intenzionalmente vuota

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

J-SIGN v1.8.9

OCSI/ACC/STM/08/2018/RA

Versione 1.0

21 gennaio 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	21/01/2019

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CGA	Certificate Generation Application
CIE	Carta di Identità Elettronica
CNS	Carta Nazionale dei Servizi
DL	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
DTBS(R)	Data To Be Signed (Representation)
EAL	Evaluation Assurance Level
EC-DSA	Elliptic Curve - Digital Signature Algorithm
eIDAS	electronic IDentification Authentication and Signature
EN	European Norm
I/O	Input/Output
ISO	International Organization for Standardization
IT	Information Technology
JCS	Java Card System
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PIN	Personal Identification Number
PP	Profilo di Protezione (Protection Profile)
RAD	Reference Authentication Data
RSA	Rivest, Shamir, Adleman
SCA	Signature Creation Application
SCD	Signature Creation Data
SFR	Security Functional Requirement
SVD	Signature Verification Data

TDS	Traguardo di Sicurezza (Security Target)
TOE	Target Of Evaluation
TSF	TOE Security Functions
VAD	Verification Authentication Data

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 V1.2.2 (2018-09)

[PP1] “Protection profiles for secure signature creation device - Part 2: Device with key generation”, EN 419211-2:2013

[PP2] “Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application”, EN 419211-4:2013

[PP3] “Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application”, EN 419211-5:2013

[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] “J-SIGN version 1.8.9”, Rapport de certification ANSSI-CC-2019/05, 11 gennaio 2019

[TDS] “J-Sign EIDAS Security Target - Public Version”, J-SIGN_EIDAS_Security_Target_Lite Rev. A, STMicroelectronics, 26 luglio 2018

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 "J-SIGN v1.8.9" sviluppato dalla società STMicroelectronics (nel seguito indicato anche come "dispositivo oggetto dell'Accertamento" o semplicemente "dispositivo").

Si tratta di un'applicazione software su *smart card* che implementa un dispositivo sicuro per la creazione di una firma elettronica o di un sigillo elettronico.

Il dispositivo oggetto dell'Accertamento è un **Dispositivo di Tipo 1**, così come definito nel cap. 6, punto A.i, della Procedura.

Il Traguardo di Sicurezza [TDS] del dispositivo dichiara conformità ai Protection Profile (PP) [PP1], [PP2] e [PP3] (EN 419211-2/4/5).

Questi PP sono stati indicati come norme di riferimento 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 ai sensi 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 J-SIGN v1.8.9, prodotto dalla società STMicroelectronics, 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 1 (cap. 7, punto A) 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 J-SIGN v1.8.9 è un'applicazione software multifunzione su *smart card* che implementa un dispositivo sicuro per la creazione di una firma elettronica o di un sigillo elettronico, con funzionalità di generazione delle chiavi. Il dispositivo fornisce inoltre le funzionalità di CIE e CNS.

Il dispositivo certificato (ODV) è un prodotto composito costituito da un'applicazione software (*applet*) su piattaforma Java Card J-SAFE JCS, il tutto integrato su microcontrollore STMicroelectronics SB23YR80B comprensivo di libreria crittografica, anch'esso certificato.

Il dispositivo J-SIGN v1.8.9 fornisce le seguenti funzionalità crittografiche e di sicurezza, derivate dai PP di riferimento [PP1], [PP2] e [PP3]:

- generazione e gestione sicura di coppie di chiavi crittografiche di sottoscrizione (SCD/SVD);
- protezione della chiave privata (SCD);
- esportazione sicura della chiave pubblica (SVD) verso un'applicazione fidata CGA;

- importazione sicura dei dati da firmare (DTBS) o della loro rappresentazione [DTBS(R)] da un'applicazione fidata SCA;

- creazione sicura di firme e sigilli elettronici.

La piattaforma Java Card fornisce servizi ottimizzati per la gestione dell'integrità di dati sensibili specifici dell'applicazione, funzionalità di gestione della memoria, funzioni di I/O conformi a standard ISO, servizi di transazione di dati atomici, implementazione sicura di funzioni crittografiche e altre funzionalità proprietarie.

L'ODV viene personalizzato in modo sicuro da un amministratore fidato e competente. Una volta personalizzato, l'ODV è pronto per:

- essere utilizzato in modo sicuro per la firma sotto il controllo esclusivo di un utente specifico (firmatario);

- essere gestito in modo sicuro da un amministratore autorizzato.

L'amministratore può generare e memorizzare nell'ODV i dati di riferimento per l'autenticazione del firmatario (RAD), che possono essere modificati o sbloccati dall'utente firmatario.

Il firmatario deve essere autenticato, ad es. tramite inserimento di un PIN, prima di poter accedere alla funzionalità di firma. Le credenziali del firmatario (VAD), i dati da firmare (DTBS) o la loro rappresentazione [DTBS(R)] vengono trasferiti da un'applicazione fidata SCA all'ODV esclusivamente mediante un canale sicuro che ne preserva confidenzialità e integrità.

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 Configurazione valutata dell'ODV

Il dispositivo certificato include l'applicazione "J-SIGN" versione 1.8.9 istanziata sulla piattaforma Java Card "J-SAFE", il tutto integrato su microcontrollore STMicroelectronics SB23YR80B certificato, comprensivo di libreria crittografica "Neslib v3.1".

La seguente documentazione di guida per l'utente e per l'amministratore è inclusa nell'ODV:

- J-SIGN-EIDAS Operational User Guidance, Rev.F, 29 giugno 2018
- J-SIGN-EIDAS Preparative Procedures, Rev.E, 12.luglio.2018

Maggiori dettagli sono inclusi nel cap. 6 (*TOE Description*) del Traguardo di Sicurezza [TDS] e nel cap. 1.2.6 (*Configuration évaluée*) del rapporto di Certificazione [CR].

Il dispositivo J-SIGN v1.8.9 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	STMicroelectronics, S.r.l.
Nome del dispositivo	J-SIGN
Versione del dispositivo	1.8.9
Traguardo di Sicurezza	"J-Sign EIDAS Security Target - Public Version", J-SIGN_EIDAS_Security_Target_Lite Rev. A, STMicroelectronics, 26 luglio 2018 [TDS]
Livello di garanzia	EAL4 con aggiunta di ALC_DVS.2 e AVA_VAN.5
Versione dei CC	3.1 Rev. 5
Conformità a PP	EN 419211-2:2013 [PP1] EN 419211-4:2013 [PP2] EN 419211-5:2013 [PP3]
Data di inizio della Procedura	21 dicembre 2018
Data di rilascio Certificato CC	11 gennaio 2019
Data di rilascio Accertamento	21 gennaio 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 J-SIGN v1.8.9 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.

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].

Il dispositivo deve essere configurato seguendo scrupolosamente la documentazione di guida inclusa con l'ODV.

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 Algoritmi crittografici

Gli algoritmi crittografici utilizzati dalle funzioni di sicurezza (TSF) del dispositivo certificato sono elencati nel Traguardo di Sicurezza (si veda [TDS] cap. 5.3 - *TOE Overview* e cap. 12.1.3 - *Key Management and Cryptography*), così come nella formulazione dei requisiti funzionali di sicurezza (SFR) della classe FCS: *Cryptographic Support* (si veda [TDS] cap. 11.2).

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-512.
- **Metodi di sottoscrizione:**
    - RSA-PSS (raccomandato) o RSA-PKCSv1_5, con lunghezza di chiave non inferiore a 2048 bit.
    - EC-DSA (raccomandato) con lunghezza di chiave non inferiore a 256 bit, a patto che vengano utilizzate esclusivamente le curve indicate in [ESI-CS], cap. 6.2.2.3 (*EC based DSA algorithms*), Tabella 3 (*Agreed Elliptic Curve Parameters*).

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*).