Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

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'art. 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 di un dispositivo per la creazione di una firma elettronica o di un sigillo elettronico qualificato 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. 1/20

Dispositivo: DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0

Sviluppato da: DocuSign Israel 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)

Firmato digitalmente
da Eva Spina
Data: 2020.09.02
10:12:06 +02'00'

Roma, 2 settembre 2020

Il presente Attestato di Conformità è stato emesso dall'Organismo di certificazione della Sicurezza Informatica (OCSI) ai sensi del comma 5 dell'art. 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/DSA/01/2020/RA) ad esso allegato, che ne costituisce parte integrante e sostanziale.

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

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

DocuSign Signature Appliance
Software Version 9.1.9.10 Hardware Version 8.0

OCSI/ACC/DSA/01/2020/RA

Versione 1.0

2 settembre 2020

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	02/09/2020

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
DL	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
DSA	DocuSign Signature Appliance
EAL	Evaluation Assurance Level
eIDAS	electronic IDentification Authentication and Signature
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OTP	One-time Password
PC	Personal Computer
PDF	Portable Document Format
PP	Profilo di Protezione
QSealCD	Qualified Seal Creation Device
QSigCD	Qualified Signature Creation Device
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
XML	eXtensible Markup Language

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

[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

[RA] “Rapporto di Accertamento DocuSign Signature Appliance v8.4”, OCSI/ACC/DSA/01/2017/RA, versione 1.0, 21 febbraio 2018

[RC] “Rapporto di Certificazione DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0”, OCSI/CERT/IMQ/01/2019/RC, versione 1.0, 22 giugno 2020

[TDS] “Security Target for DocuSign Signature Appliance”, Version 2.18, DocuSign TLV team, 11 July 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 "DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0", sviluppato dalla società DocuSign Israel Ltd. (nel seguito indicato anche come "dispositivo oggetto dell'Accertamento", "*appliance* DocuSign" o "dispositivo DSA").

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.

Si noti che il dispositivo oggetto dell'Accertamento è una versione aggiornata del dispositivo denominato "DocuSign Signature Appliance v8.4", già accertato dall'OCSI (Attestato di Conformità n. 2/18 del 21 febbraio 2018 [RA]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore DocuSign è stato necessario procedere a una ri-certificazione dell'ODV, i cui risultati sono riportati nel Rapporto di Certificazione [RC].

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente dispositivo, per facilità di lettura il presente Rapporto di Accertamento è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo dispositivo "DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0".

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo "DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0", prodotto dalla società DocuSign Israel 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 come dispositivo per la creazione di firme e sigilli elettronici qualificati.

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 "DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0" è un prodotto di firma digitale progettato per essere utilizzato come dispositivo per la creazione di una firma elettronica qualificata (QSigCD) e/o come dispositivo per la creazione di un sigillo elettronico qualificato (QSealCD).

L'*appliance* DocuSign, illustrata in Figura 1, è utilizzata all'interno di un'organizzazione, fisicamente installata in un ambiente operativo sicuro nel data-center dell'organizzazione e connessa alla rete dell'organizzazione stessa.

Un singolo dispositivo DSA può gestire in modo sicuro molti utenti. Ogni account di utente può includere una o più chiavi di firma e altre informazioni, come ad esempio le immagini grafiche dell'utente. Tutti gli account di utente, le chiavi, i certificati e le altre informazioni relative all'utente sono conservate in maniera sicura all'interno dell'*appliance*.

Tre diverse tipologie di utenti sono autorizzate ad operare sul dispositivo: l'utente semplice (Firmatario/Creatore di Sigillo, secondo la configurazione utilizzata) e due diversi profili di utente amministratore: Appliance Administrator (installa l'*appliance* e ne gestisce le funzionalità) e Users Administrator (gestisce gli account degli utenti).

Figura 1 - La DocuSign Signature Appliance (vista frontale)

Nessun utente, incluso l'amministratore dell'*appliance* o qualsiasi altro amministratore, può utilizzare la chiave di un altro utente per l'operazione di firma digitale.

Quando un utente richiede di utilizzare le proprie chiavi per l'operazione di firma digitale, l'utente accede all'*appliance* utilizzando un canale di comunicazione sicuro dedicato realizzato tramite il protocollo TLS. Questo canale sicuro è utilizzato per ogni comunicazione tra il client e l'*appliance* DocuSign.

Nel caso in cui il dispositivo DSA è installato e configurato come dispositivo per la creazione di una firma elettronica qualificata (QSigCD), a ciascun utente viene fornito un dispositivo OTP (*One-time Password*). Ogni dispositivo OTP (OTP-Device) ha un suo identificativo univoco e un suo Profilo del dispositivo OTP univocamente associato. Il dispositivo OTP e il Profilo associato non fanno parte dell'ODV.

L'utente può firmare digitalmente utilizzando la propria chiave di sottoscrizione personale, solamente previa autenticazione a due fattori, basata sulla presentazione di una password statica e una password dinamica che viene visualizzata sul display del dispositivo OTP.

Il dispositivo DSA convalida internamente la password statica. Quando l'ODV è configurato per utilizzare un server RADIUS situato all'interno del suo ambiente operativo, il dispositivo DSA comunica in modo sicuro con il server RADIUS, il quale a sua volta convalida l'OTP inserito dall'utente mediante una chiamata di *callback* al dispositivo. È possibile configurare l'ODV per la convalida dell'OTP senza l'uso di un server RADIUS.

L'utente Firmatario può interagire con l'*appliance* da un PC su cui è installato il software client DSA. Il client DSA consente all'utente finale di integrare la firma digitale prodotta dall'*appliance* DocuSign in un documento in formato PDF, XML o in qualsiasi altro formato supportato. Più utenti possono firmare contemporaneamente da diversi PC. Ogni sessione d'utente è completamente separata dalle altre sessioni d'utente.

Inoltre, è possibile interagire col dispositivo DSA tramite l'interfaccia REST (*Representational State Transfer*), mediante la quale gli utenti Firmatari possono eseguire le stesse operazioni messe a disposizione dal client DSA.

È possibile configurare il dispositivo DSA per permettere all'utente di firmare con la stessa interfaccia diversi documenti o transazioni dopo una sola autenticazione a due fattori, entro un periodo di tempo fissato, configurabile fino ad un massimo di 10 minuti.

Quando il dispositivo è installato come dispositivo per la creazione di un sigillo elettronico qualificato (QSealCD), l'utente corrisponde al "Creatore di Sigillo" ed è autenticato senza fare ricorso all'OTP e al RADIUS Server.

L'*appliance* DocuSign registra in un audit log ciclico tutte le attività amministrative e ogni utilizzo di una qualsiasi chiave di firma di un utente. L'audit log non può essere cancellato e può essere letto da un amministratore autorizzato.

Le funzioni di sicurezza implementate dall'ODV sono:

- Controllo d'accesso
- Identificazione e autenticazione
- Operazioni crittografiche
- Audit di sicurezza
- Comunicazioni sicure e gestione delle sessioni
- Rilevamento delle manomissioni
- Self test
- Funzioni di amministrazione dell'*appliance*

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

Nel Traguardo di Sicurezza dell'*appliance* DocuSign sono elencate quattro diverse possibili configurazioni valutate ([TDS], par. 1.2):

1) PRIMARY-HIGH AVAILABILITY WITH KEY REPLICATION (HA-PRI-REPL-INC-SIGKEY)
2) ALTERNATE-HIGH AVAILABILITY WITH KEY REPLICATION (HA-ALT-REPL-INC-SIGKEY)
3) SEAL-PRIMARY-HIGH AVAILABILITY WITH KEY REPLICATION (SEAL-HA-PRI-REPL-INC-SIGKEY)
4) SEAL-ALTERNATE-HIGH AVAILABILITY WITH KEY REPLICATION (SEAL-HA-ALT-REPL-INC-SIGKEY)

Le configurazioni 1 e 2 fanno riferimento all'installazione come QSigCD, mentre le configurazioni 3 e 4 fanno riferimento all'installazione come QSealCD. Le due coppie di configurazioni (1,2) e (3,4) permettono di utilizzare l'ODV in Alta Disponibilità con replica delle chiavi private del Firmatario: nell'ambiente operativo è installata una sola *appliance* primaria in configurazione 1 o 3 ed una o più *appliance* alternative rispettivamente in configurazione 2 o 4.

Per ulteriori dettagli si rimanda al Traguardo di Sicurezza [TDS], par. 1.3.2.

Tutte e quattro le configurazioni del dispositivo DSA sono risultate conformi 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].

6.3 Identificazione sintetica dell'accertamento

Richiedente l'accertamento	DocuSign Israel Ltd.
Nome del dispositivo	DocuSign Signature Appliance
Versione del dispositivo	Software Version 9.1.9.10 Hardware Version 8.0
Traguardo di Sicurezza	Security Target for DocuSign Signature Appliance, Version 2.18, DocuSign TLV team, 11 July 2019
Livello di garanzia	EAL4 con l'aggiunta di AVA_VAN.5, ALC_FLR.1 e ATE_DPT.2
Versione dei CC	3.1 Rev. 4
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della Procedura	16 luglio 2020
Data di rilascio Certificato CC	22 giugno 2020
Data di rilascio Accertamento	2 settembre 2020

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 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 DSA deve essere utilizzato seguendo tutte le prescrizioni contenute nel Traguardo di Sicurezza [TDS] e nel Rapporto di Certificazione [RC].

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 anche in [RC], Appendice A.