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. 2/18

Dispositivo: DocuSign Signature Appliance v8.4

Sviluppato da: DocuSign

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)

Roma, 21 febbraio 2018

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/DSA/01/2017/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

DocuSign Signature Appliance v8.4

OCSI/ACC/DSA/01/2017/RA

Versione 1.0

21 febbraio 2018

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	21/02/2018

2 Indice

3 Elenco degli acronimi

CC Common Criteria

DL Decreto Legislativo

DPCM Decreto del Presidente del Consiglio dei Ministri

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

PP Profilo di Protezione (Protection Profile)

RADIUS Remote Authentication Dial-In User Service

REST Representational State Transfer

TDS Traguardo di Sicurezza (Security Target)

TLS Transport Layer Security

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 ARX CoSign v8.2”, OCSI/ACC/ARX/01/2017/RA, versione 1.0, 7 febbraio 2017

[RC] “Rapporto di Certificazione DocuSign Signature Appliance v8.4”, OCSI/CERT/IMQ/07/2017/RC, versione 1.0, 21 febbraio 2018

[TDS] “Security Target for DocuSign Signature Appliance”, Version 2.13, DocuSign, 23 January 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 "DocuSign Signature Appliance v8.4", prodotto dalla società DocuSign (nel seguito indicato come "dispositivo oggetto dell'Accertamento" o semplicemente "dispositivo DocuSign" o "appliance" DocuSign).

Tale dispositivo 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 "CoSign v8.2", già accertato dall'OCSI (Attestato di Conformità n. 1/17 del 7 febbraio 2017 [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 v8.4".

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo denominato “DocuSign Signature Appliance v8.4”, prodotto dalla società DocuSign, 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 v8.4” è costituito dall’appliance progettata da DocuSign per essere utilizzata come dispositivo per la creazione di una firma elettronica qualificata (*qualified electronic signature creation device*) e/o come dispositivo per la creazione di un sigillo elettronico qualificato (*qualified electronic seal creation device*).

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

Una singola appliance può gestire in modo sicuro molti utenti, e per ogni account di utente è possibile generare diverse chiavi di firma e i relativi certificati.

Tre diverse tipologie di utenti sono autorizzate ad operare sull’ODV: 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;
- *Users Administrator*: gestisce gli account degli utenti.

Quando il dispositivo è installato come dispositivo per la creazione di una firma elettronica qualificata, un utente (Firmatario) interagisce usando il DocuSign SA Client o l'interfaccia REST (Representational State Transfer) per eseguire la registrazione dei certificati e per effettuare le operazioni di firma.

Ad ogni utente Firmatario è fornito un dispositivo OTP (One Time Password) con un suo Profilo del dispositivo OTP univocamente associato. Il dispositivo OTP (OTP-Device) e il Profilo associato, così come l'OTP RADIUS Server che gestisce i dispositivi OTP, non fanno parte dell'ODV. Un firmatario si autentica fornendo una password statica e una password dinamica che viene visualizzata sul display del dispositivo OTP. Quando un utente desidera firmare digitalmente un documento, mediante il DocuSign SA Client o l'interfaccia REST (Representational State Transfer), apre una sessione utente protetta 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.

È possibile configurare il dispositivo per permettere all'utente di firmare, mediante il DocuSign SA Client, 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, 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

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

Il Traguardo di Sicurezza del dispositivo DocuSign descrive quattro diverse possibili configurazioni:

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 dispositivo per la creazione di una firma elettronica qualificata, mentre le configurazioni 3 e 4 fanno riferimento all'installazione come dispositivo per la creazione di un sigillo elettronico qualificato.

Per ulteriori dettagli si rimanda a [TDS], par. 1.3.2.

Tutte e quattro le configurazioni del dispositivo DocuSign 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
Nome del dispositivo	DocuSign Signature Appliance
Versione del dispositivo	8.4
Traguardo di Sicurezza	Security Target for DocuSign Signature Appliance, Version 2.13, DocuSign, 23 January 2018
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 rilascio Certificato CC	21 febbraio 2018
Data di inizio della Procedura	25 luglio 2017
Data di rilascio Accertamento	21 febbraio 2018

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 DocuSign 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.