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)

Certificato n. 3/20

(Certification No.)

Prodotto: *(Product)* **DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0**

Sviluppato da: *(Developed by)* **DocuSign**

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+

(AVA_VAN.5, ALC_FLR.1, ATE_DPT.2)

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente da:Eva Spina
Organizzazione:MISE/80230390587
Data:22/06/2020 12:30:25

Roma, 22 giugno 2020

Fino a EAL2 *(Up to EAL2)*

Common Criteria

Fino a EAL4 *(Up to EAL4)*

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

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

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

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	22/06/2020

2 Indice

3 Elenco degli acronimi

CA	Certification Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CD-ROM	Compact Disc - Read-Only Memory
CEA	Certificate Enrollment Application
CEM	Common Evaluation Methodology
CGA	Certificate Generation Application
CSCI	Computer Software Configuration Item
CSP	Certificate Service Provider
DBMS	Database Management System
DLM	Akamai Download Manager
DPCM	Decreto del Presidente del Consiglio dei Ministri
DSA	DocuSign Signature Appliance
DTBS/R	Data To Be Signed/Representation
EAL	Evaluation Assurance Level
HW	Hardware
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OTP	One-Time Password
PDF	Portable Document Format
PC	Personal Computer
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
RFV	Rapporto Finale di Valutazione
RPC	Remote Procedure Call
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCD	Signature Creation Data
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
SVD	Signature (or Seal) Validation Data
SW	Software
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target of Evaluation
TOTP	Time-based One-Time Password
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
TSP	Trust Service Provider
USB	Universal Serial Bus

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Documenti tecnici

[ADM] DocuSign Signature Appliance Administrator Guide V.9.1.9.10, DocuSign, January 2020

[CMS] DSA – ALC – CM Scope, V.2.19, DocuSign, 17/02/2020.

[ETSI1] “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”, ETSI TS 119 312 V1.2.1 (2017-05)

[ETSI2] “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices”, ETSI TS102 176-2 V1.2.1 2005-07

[NIST] NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General (Revision 3), July 2012

[PRE] DocuSign Signature Appliance Preparative Procedures V. 9.1.9.10, DocuSign, January 2020

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

[RFV] “Rapporto Finale di Valutazione dell’ODV DocuSign Signature Appliance”, LVS IMQ/LPS, versione 1.0, 21 febbraio 2020

[TDS] “Security Target for DocuSign Signature Appliance”, Version 2.18, DocuSign TLV team, 11 July 2019

[USR] DSA - AGD Operational User Guidance V. 2.18, DocuSign, 11/07/2019

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su https://www.sogis.eu/.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia fino a EAL4.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA fino a EAL2.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0", sviluppato dalla società DocuSign Israel Ltd., nel seguito del documento anche indicato come "appliance DocuSign", "DocuSign SA" o "DSA".

La valutazione è stata di tipo concomitante, cioè effettuata durante lo sviluppo dell'ODV, ed è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV (DocuSign Signature Appliance v8.4), già certificato dall'OCSI (Certificato n. 2/18 del 21 febbraio 2018 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore DocuSign è stato necessario procedere a una ri-certificazione dell'ODV. L'LVS IMQ/LPS ha potuto riutilizzare parte della documentazione e delle evidenze già fornite nella precedente valutazione.

Si noti che le modifiche effettuate hanno comportato anche la revisione del Traguardo di Sicurezza [TDS]. Gli utenti della precedente versione dell'ODV sono quindi invitati a prendere visione anche del nuovo TDS.

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

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5, ALC_FLR.1 e ATE_DPT.2, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0
Traguardo di Sicurezza	Security Target for DocuSign Signature Appliance, Version 2.18, 11 July 2019 [TDS]
Livello di garanzia	EAL4 con l'aggiunta di AVA_VAN.5, ALC_FLR.1 e ATE_DPT.2
Fornitore	DocuSign Israel Ltd.
Committente	DocuSign Israel Ltd.
LVS	IMQ/LPS
Versione dei CC	3.1 Rev. 4
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	14 maggio 2019
Data di fine della valutazione	21 febbraio 2020

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo capitolo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0" è costituito dall'appliance progettata da DocuSign per essere utilizzata come dispositivo per la creazione di una firma elettronica qualificata (*QSigCD - Qualified Signature Creation Device*) e/o come dispositivo per la creazione di un sigillo elettronico qualificato (QSealCD

- *Qualified Seal Creation Device*). L'appliance DocuSign (Figura 1), 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.

Figura 1 – La DocuSign Signature Appliance (fronte e retro)

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

Le funzionalità a disposizione degli amministratori sono descritte in [TDS], par. 1.4.2.2.4, mentre le funzionalità offerte ad utenti non di tipo amministrativo sono descritte in [TDS], par. 1.4.2.2.1.

Nella Figura 2 sono mostrate le entità esterne con cui interagisce l'ODV quando è installato come dispositivo per la creazione di firme (QSigCD) e la validazione degli OTP (One Time Password) avviene con il supporto di un RADIUS Server[1].

Un firmatario interagisce con l'ODV usando il DSA client per eseguire l'enrollment del/dei certificati e per effettuare operazioni di firma. L'amministratore interagisce con l'ODV per eseguire le varie attività amministrative previste. Le informazioni contenute nel RADIUS Server permettono a DSA di autenticare gli utenti mediante OTP.

Dal punto di vista della sicurezza, ad ogni utente è fornito un dispositivo OTP con un suo Profilo del dispositivo OTP univocamente associato. Quando un utente si autentica utilizzando un dispositivo OTP (OTP-Device), gli viene richiesto di fornire una password statica e una password dinamica (OTP). Il dispositivo OTP e il Profilo associato non fanno parte dell'ODV.

1 Il RADIUS Server è utilizzato dall'ODV configurato come QSigCD quando non è utilizzato il meccanismo di autenticazione TOTP interno (funzionalità introdotta in DSA SW V. 9.1.9.10). Con la nuova funzionalità TOTP interna, l'autenticazione a due fattori per la modalità QSigCD è garantita anche senza l'utilizzo di un server RADIUS esterno.

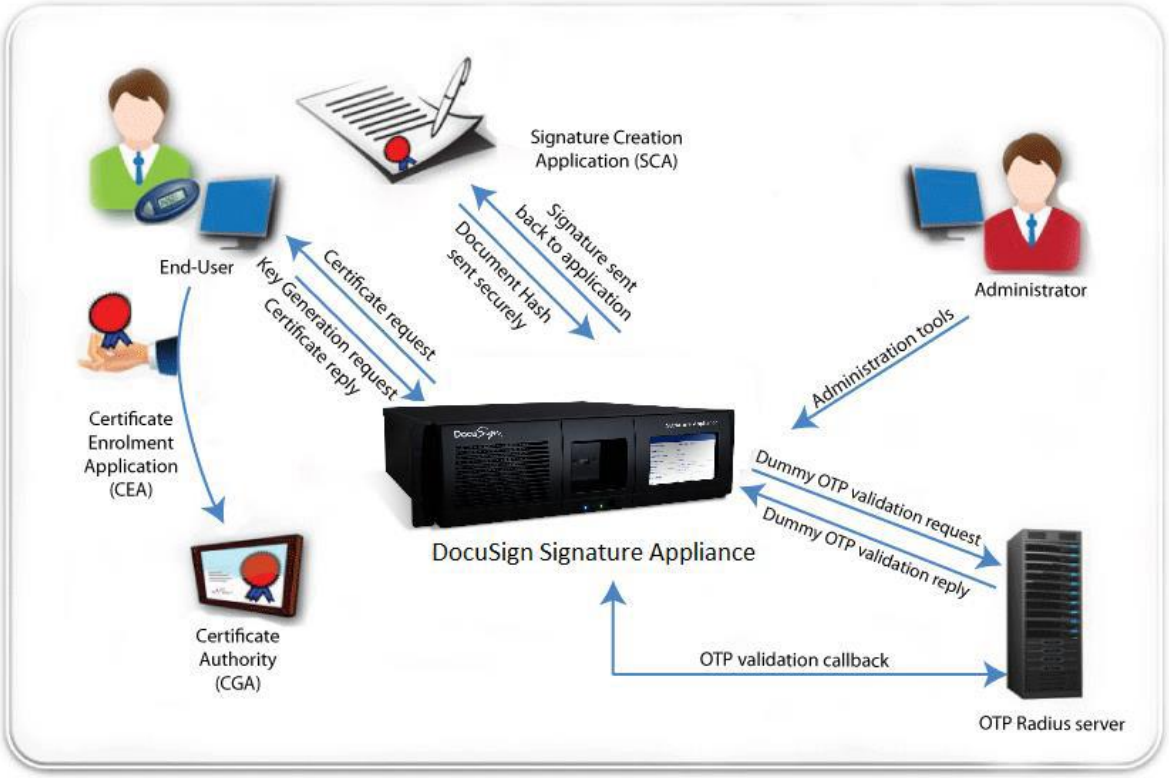

Figura 2 – Entità con cui si interfaccia l'ODV installato come QSigCD (nel caso in cui la validazione degli OTP avviene con il supporto di un RADIUS Server)

Nella Figura 3 sono mostrate le entità esterne con cui interagisce l'ODV nel caso in cui l'ODV è installato come QSigCD ma senza l'ausilio di un RADIUS Server per la validazione degli OTP, o quando l'ODV è installato come QSealCD.

In questo caso il RADIUS Server nell'ambiente operativo è sempre assente e quando l'ODV è installato come QSealCD il firmatario corrisponde al "Creatore di Sigillo" ed è autenticato con la sola password statica, senza il ricorso all'OTP.

Oltre all'OTP-Device (ed il corrispondente OTP-Device Profile) e al RADIUS Server (opzionale), non fanno parte dell'ODV, ma sono da esso richiesti (si veda per maggiori dettagli [TDS], par. 1.3.3): l'applicazione per la creazione della firma (SCA); l'applicazione per la registrazione dei certificati (CEA), l'applicazione per la generazione dei certificati (CGA), il token USB contenente la licenza software, Special Routers (opzionali: permettono di reindirizzare le richieste del client sull'Alternate Appliance in caso di "temporary fatal error" della Primary Appliance e viceversa nel momento in cui la Primary Appliance ritorna ad erogare il servizio) e il PC/Laptop da utilizzare per accedere alla Web Based Console dell'ODV.

Quando un utente desidera firmare digitalmente un documento (o apporvi un sigillo), il DocuSign SA Client 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.

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 (Appliance Administrator).

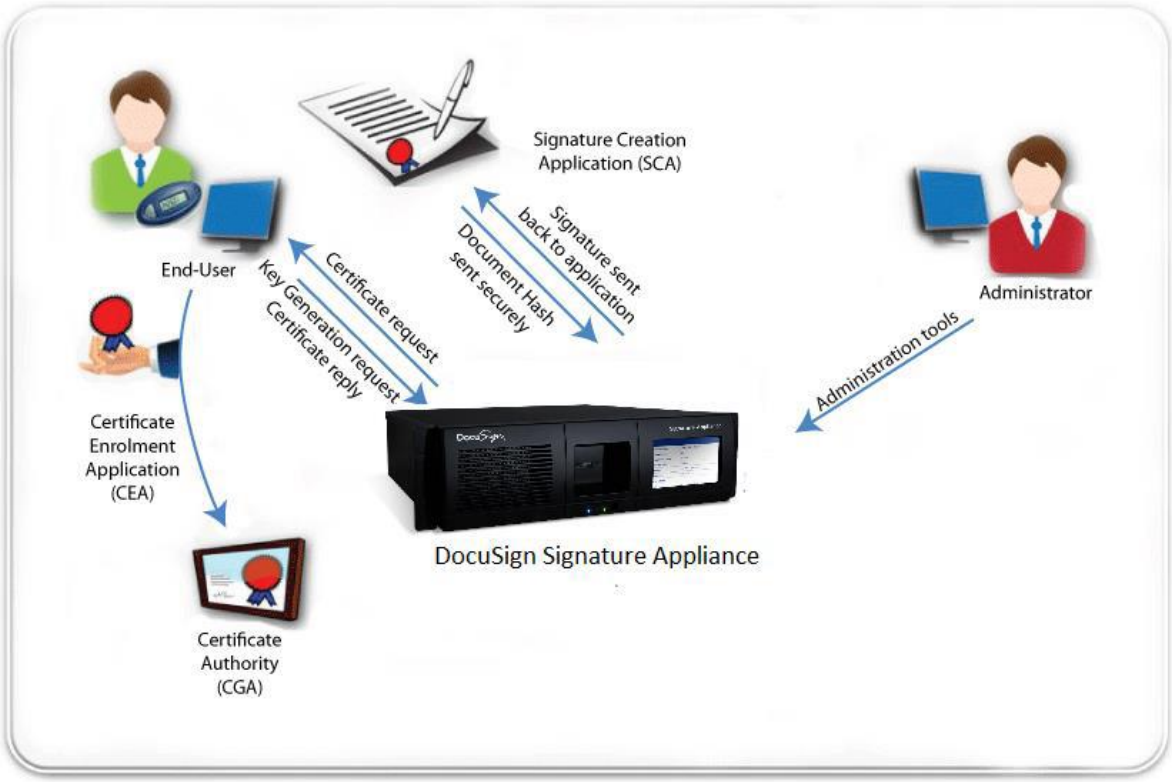

Figura 3 – Entità con cui si interfaccia l'ODV installato come QSealCD o come QSigCD senza l'utilizzo di un RADIUS Server.

7.3.1 Architettura dell'ODV

7.3.1.1 Ambito fisico ed Hardware dell'ODV

La descrizione dell'ambito fisico dell'ODV con l'elenco degli elementi hardware è fornita in [TDS], par. 1.4.2.1.

7.3.1.2 Ambito Logico

La descrizione dell'ambito logico dell'ODV è fornita in [TDS], par. 1.4.2.2.

Il software dell'appliance DocuSign può trovarsi in uno dei seguenti stati:

- *Factory settings:* è lo stato in cui il prodotto arriva dalla fabbrica; il prodotto non è ancora installato e non può essere utilizzato dagli utenti finali;
- *Operational state:* il prodotto è installato e pronto per gestire nuovi account utenti e per eseguire operazioni di firma digitale;
- *Tamper state:* l'appliance è stata manomessa; in questo stato gli utenti finali non possono eseguire operazioni di firma digitale.

Nella Figura 4 è riportato il ciclo di vita dell'ODV. Maggiori dettagli sulla descrizione dei suddetti stati e delle operazioni permesse ad utenti ed amministratori nei diversi stati sono riportati in [TDS], par. 1.4.2.2.6.

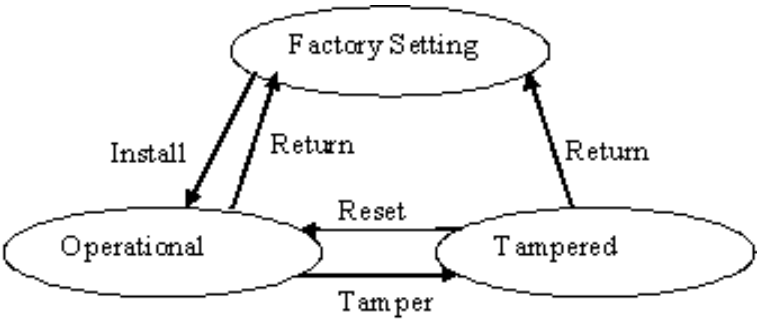

Figura 4 – Ciclo di vita dell'appliance DocuSign

Le seguenti operazioni sono eseguite automaticamente dall'appliance DocuSign nello stato Operational:

- Tamper detection & protection (rilevamento manomissioni e protezione anti manomissione) in caso di apertura del coperchio dell'appliance. La protezione antimanomissione è garantita con l'appliance sia accesa sia spenta.
- Memorizzazione sicura delle chiavi di firma.
- Memorizzazione dei dati applicativi (certificati e immagini delle firme grafiche).

7.3.2 Caratteristiche di Sicurezza dell'ODV

7.3.2.1 Ipotesi

Le ipotesi definite nel Traguardo di Sicurezza [TDS] ed alcuni aspetti delle minacce e delle politiche di sicurezza organizzative non sono coperte direttamente dall'ODV stesso; ciò implica che specifici obiettivi di sicurezza debbano essere soddisfatti dall'ambiente operativo. In particolare, in tale ambito le ipotesi in [TDS], par. 3.3, e di seguito riportate, devono essere verificate:

- **Applicazione CGA affidabile per la generazione di certificati**: la CGA protegge l'autenticità del nome del firmatario e la chiave pubblica (SVD) nel certificato (qualificato) mediante una firma elettronica avanzata del CSP.
- **Applicazione SCA affidabile per la creazione di firme**: il firmatario utilizza solo una SCA affidabile. L'SCA genera e invia la rappresentazione dei dati che il firmatario desidera firmare (DTBS/R) in una forma appropriata per la firma da parte dell'ODV.
- **Configurazione dell'ODV**: le procedure di configurazione dell'ODV: (i) prendono in considerazione le raccomandazioni incluse in [ETSI1] sulla resistenza delle funzioni hash e sulla resistenza delle suite di firma nel tempo, (ii) forniscono una guida chiara all'amministratore dell'appliance al fine di garantire la rigorosa conformità ad [ETSI1] in tutti i casi richiesti, (iii) forniscono una guida chiara all'amministratore dell'appliance, in tutti i casi necessari, al fine di garantire la rigorosa conformità

all'ultima versione aggiornata di [ETSI2] o, in alternativa, al fine di verificare che le condizioni per una conformità estesa a [ETSI2] siano ancora applicabili.

- **Ambiente sicuro**: Si presume che l'ambiente operativo fornisca misure sufficienti per proteggere l'ODV da manomissioni fisiche che consentano accessi non autorizzati alla rete. Inoltre, si presume che l'ambiente operativo fornisca misure sufficienti per proteggere l'ODV dall'uso di strumenti quali tool di analisi delle emissioni elettromagnetiche o tool dedicati alla registrazione del suono che possono tentare di dedurre le informazioni utilizzate dalle unità di elaborazione interne all'ODV.

- **Token USB di backup**: si presume che un amministratore autorizzato sia responsabile di conservare in un luogo sicuro (una cassaforte) entrambi i token USB di backup generati durante l'installazione dell'ODV.

- **File di backup**: si presume che un amministratore autorizzato sia responsabile di conservare il file di backup dell'ODV in un luogo sicuro (una cassaforte).

- **Gestione del profilo del dispositivo OTP e del dispositivo OTP**: si presume che i profili dei dispositivi OTP ed i dispositivi OTP siano gestiti in modo sicuro dalla fase di produzione (ove applicabile) attraverso misure organizzative fino a quando il dispositivo OTP è in utilizzo del Firmatario. Inoltre, nel caso in cui l'ODV sia configurato per utilizzare un server RADIUS OTP esterno, si presume che i profili dei dispositivi OTP siano gestiti correttamente nel server RADIUS OTP, considerando anche lo stato dell'account utente.

  Nota: l'OTP è rilevante se l'ODV è installato come QSigCD.

- **Routing in un ambiente operativo sicuro**: si presume che l'infrastruttura di routing e l'amministrazione del routing vengano eseguite in modo sicuro, in modo che tutte le richieste di servizio vengano inviate correttamente all'ODV primario. In caso di errore irreversibile temporaneo dell'ODV primario, si presume che le richieste siano instradate a un ODV alternativo definito e selezionato fino a quando l'errore irreversibile temporaneo dell'ODV primario viene analizzato e risolto.

- **Utilizzo del dispositivo OTP da parte del firmatario**: si presume che il Firmatario mantenga il proprio dispositivo OTP sotto il suo controllo e in qualsiasi caso rilevi un dispositivo OTP mancante o un dispositivo OTP manomesso, il Firmatario segnali tale fatto all'organizzazione allo scopo di revocare l'account del Firmatario e il dispositivo OTP pertinente.

  Nota: l'OTP è rilevante se l'ODV è installato come QSigCD.

- **Utenti addestrati e affidabili formati e fidati**: si presume che tutti gli utenti dell'ODV siano sufficientemente addestrati per operare sull'ODV in modo sicuro. Si presume inoltre che gli amministratori dell'ODV siano fidati e che siano sufficientemente formati per installare, configurare l'ODV e l'ambiente dell'ODV in modo sicuro. Ciò implica che gli amministratori dell'ODV siano anche responsabili dell'installazione, della configurazione e del funzionamento sicuri del RADIUS Server (ove applicabile).

Nota: nel caso in cui l'ODV sia distribuito come QSigCD, è possibile configurare l'ODV per consentire al Firmatario di applicare la firma di più documenti o transazioni entro un determinato periodo di tempo dopo l'autenticazione a due fattori. In questo caso, gli utenti finali dovrebbero essere consapevoli che non devono lasciare il proprio ambiente di applicazione incustodito, consentendo così ad altri utenti di accedere al proprio ambiente senza fornire la propria password statica e OTP. Quando si lascia l'ambiente di firma è necessario chiudere l'applicazione di firma digitale.

7.3.2.2 Funzioni di sicurezza

Le funzioni di sicurezza implementate dall'ODV sono descritte in dettaglio in [TDS], cap. 7. Di seguito sono riassunti alcuni aspetti ritenuti rilevanti:

- **Controllo d'accesso**: l'ODV autorizza l'accesso degli utenti assegnando i diritti in base al loro ruolo: Firmatario/Creatore di Sigillo, Appliance Administrator e User Administrator.

- **Identificazione e autenticazione**: l'ODV identifica univocamente e autentica gli utenti. Gli amministratori si autenticano con una password statica. Nel caso di installazione dell'ODV come QSigCD, per alcune operazioni, come l'attivazione dell'account e le operazioni di generazione ed uso delle chiavi crittografiche, i Firmatari si autenticano, oltre che con una password statica, anche con una dinamica (OTP). Quando l'ODV è installato come QSealCD gli utenti si autenticano con la sola password statica.

- **Operazioni crittografiche**: l'ODV permette di effettuare operazioni crittografiche, quali generazione chiavi, firma digitale, verifica della firma, oltre che di gestione di chiavi a scopo di protezione dei dati dell'utente.

- **Audit di sicurezza**: l'ODV registra una serie di eventi relativi alla sicurezza; l'ODV permette all'Appliance Administrator di verificare i log registrati.

- **Comunicazioni sicure e gestione delle sessioni**: le comunicazioni tra ODV e RADIUS Server, tra ODV Primary e ODV Alternate e tra ODV e Client avvengono in modo sicuro, garantendo la confidenzialità e l'integrità dei dati trasmessi e la separazione delle sessioni d'utente.

- **Rilevamento delle manomissioni**: l'ODV implementa meccanismi di verifica dell'integrità del software e anti-tampering fisico.

- **Self test**: l'ODV fornisce una suite di test automatici di controllo eseguiti sia all'avvio sia durante la normale operatività, compresa la fase di creazione delle firme.

- **Funzioni di amministrazione dell'appliance**: l'ODV include alcune funzioni di amministrazione dell'appliance fra cui download dei log di audit, configurazione dei parametri di sistema, caricamento della chiave TLS del REST server, gestione dell'appliance primaria ed appliance alternative, caricamento di SW, backup dei dati dell'appliance, spegnimento e riavvio HW/SW dell'ODV.

7.3.3 Configurazioni 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 [TDS], par. 1.3.2.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto viene fornita all'utente finale insieme al prodotto. Questa documentazione contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS]. Devono inoltre essere seguiti gli ulteriori obblighi o note per l'utilizzo sicuro dell'ODV contenuti nel par. 9.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti Funzionali (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS IMQ/LPS.

L'attività di valutazione è terminata in data 21 febbraio 2020 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 17 marzo 2020. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5, ALC_FLR.1 e ATE_DPT.2, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5, ALC_FLR.1 e ATE_DPT.2.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Complete functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo

Classi e componenti di garanzia		Verdetto
Delivery procedures	ALC_DEL.1	Positivo
Identification of security measures	ALC_DVS.1	Positivo
Basic flaw remediation	ALC_FLR.1	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: security enforcing modules	ATE_DPT.2	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing – sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Advanced methodical vulnerability analysis	AVA_VAN.5	Positivo

Tabella 1 – Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 - Dichiarazione di certificazione.

Si raccomanda ai potenziali acquirenti del prodotto "DocuSign Signature Appliance Software Version 9.1.9.10 Hardware Version 8.0" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nel capitolo 3 del Traguardo di Sicurezza [TDS]. Si consiglia ai potenziali acquirenti di verificare la rispondenza ai requisiti identificati e di prestare attenzione alle raccomandazioni contenute in questo Rapporto.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata, le cui modalità di installazione e configurazione sono descritte nelle Procedure di preparazione [PRE] e nella Guida per l'amministratore [ADM] e per l'utente [USR], fornite insieme all'ODV.

Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto nella documentazione citata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'installazione e all'utilizzo sicuro del prodotto.

Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte in [TDS], par. 3.2 e

3.3, in particolare quelle relative al personale ed ai locali all'interno dei quali andrà ad operare l'ODV.

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna

La consegna del dispositivo DocuSign Signature Appliance avviene direttamente presso la sede dell'utente. Al momento della consegna, il prodotto si trova nello stato "Factory Settings", cioè non è stato ancora installato e non è accessibile dagli utenti finali ([TDS], par. 1.4.2.2.6). La sicurezza fisica è assicurata da sigilli metallici, identificati da numeri univoci indicati nella lettera di consegna, che risulterebbero danneggiati in caso di apertura illecita, rendendo così evidente al destinatario se l'involucro è stato manomesso durante il tragitto.

Nella stessa confezione dell'ODV, viene consegnato anche un CD-ROM contenente il client software (DocuSign Signature Appliance client software) e il manuale in formato PDF; i file eseguibili e la documentazione contenuti nel CD-ROM sono firmati digitalmente dal produttore a garanzia dell'integrità del CD-ROM stesso e quindi della sicurezza logica dell'ODV.

Alla ricezione della confezione, il ricevente, in particolare l'Appliance Administrator, deve verificare l'integrità del dispositivo e la correttezza dei dati inclusi nel CD-ROM, seguendo le indicazioni fornite nel documento che descrive le procedure di preparazione [PRE].

9.2 Installazione, inizializzazione ed utilizzo sicuro dell'ODV

L'installazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo in accordo agli obiettivi di sicurezza indicati nel [TDS], devono avvenire seguendo le istruzioni contenute nelle apposite sezioni dei documenti [ADM], [PRE] ed [USR].

In particolare, per rispettare la configurazione valutata, devono necessariamente essere installati sull'ODV tutti gli aggiornamenti di sicurezza rilasciati dal Fornitore, seguendo le indicazioni fornite nel capitolo "Additional Security related updates" della Guida di Amministratore [ADM].

10 Appendice B – Configurazione valutata

Il nome e il numero di versione identificano univocamente l'ODV e i suoi componenti SW, ai quali vanno applicati gli aggiornamenti di sicurezza indicati in Appendice A – Indicazioni per l'uso sicuro del prodotto.

Tale insieme costituisce la configurazione valutata dell'ODV, come riportato nella lista di configurazione, fornita dal Committente ai Valutatori nel documento [CMS], a cui si applicano i risultati della valutazione.

I componenti HW dell'ODV sono riportati in Tabella 2.

Componenti HW	Descrizione
DocuSign Signature Appliance Hardware version 8.0	Intera Appliance HW dell'ODV
USB Token interno con smart card basata sul chip: Atmel AT90SC25672RCT-USB with Athena IDProtect/OS755 Java Card.	Smart card interna, contenuta in un token USB, utilizzato per la generazione di "true random seed"

Tabella 2 – Componenti HW dell'ODV

10.1 Ambiente operativo dell'ODV

Di seguito si riportano gli elementi HW e SW che devono o possono essere presenti nell'ambiente operativo dell'ODV ([TDS], par. 1.3.3):

- OTP-Device e OTP-Device profile (si tratta di token fisici, come ad es. Vasco e Yubico o una applicazione TOTP per smartphone, come ad es. Google Authenticator. Essi sono richiesti solo in caso di utilizzazione dell'ODV come QSCD);
- OTP RADIUS Server (può essere utilizzato nel caso di installazione come QSigCD);
- SCA (Signature Creation Application);
- CEA (Certificate Enrollment Application);
- CGA (Certificate Generation Application);
- Smart Card in formato Token USB per funzioni di backup;
- License USB Token;
- Appliance Administrator PC/Laptop Web Console;
- Special Routers (per permettere una parziale continuità del servizio in caso di indisponibilità temporanea dell'appliance primaria).

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5, ALC_FLR.1 e ATE_DPT.2, tali attività prevedono tre passi successivi:

- valutazione in termini di copertura e livello di approfondimento dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

L'esecuzione dei test funzionali e dei test di intrusione è avvenuta nell'arco temporale dal 4/11/2019 al 06/02/2020 (non continuativi) presso la sede del LVS IMQ.

In concomitanza dell'esecuzione delle prove sono state anche verificate le procedure di rilascio e configurazione e di avvio in esercizio dell'ODV, attività previste da requisiti delle famiglie di garanzia AGD_PRE ed AGD_OPE.

Essendo l'attività di valutazione concomitante con lo sviluppo dell'ODV, durante la valutazione sono state rilasciate nuove versioni dell'ODV per ogni riciclo di test.

11.1 Configurazione per i Test

Per l'esecuzione dei test è stato predisposto un apposito ambiente di test presso la sede dell'LVS con il supporto del Committente/Fornitore, che ha fornito le risorse necessarie e ha messo a disposizione alcune risorse di base, quali:

- un'appliance primaria ed un'appliance alternativa (hardware versione 8.0);
- un RADIUS Server (PC con sistema operativo Windows Server 8).

Inoltre, i seguenti ulteriori strumenti sono stati messi a disposizione dell'LVS da parte del Committente:

- Microsoft CA installata sul sistema operativo Window Server 2008 sul PC su cui è eseguito RADIUS Server;
- certrequestcc.exe Ver. 2017 (tool client per la richiesta di generazione chiavi di diversa lunghezza, creazione del file di richiesta del certificato per la CA, e per importare il certificato in DSA);
- Argenie ver. 5.2.1.0 (tool client per cancellare gli oggetti crittografici come chiavi private e pubbliche di un dato utente, previa identificazione e autenticazione);
- Token OTP Yubico e Vasco.

Inoltre, da parte dell'LVS sono stati utilizzati i seguenti ulteriori strumenti:

- il tool freeware POSTMAN Ver. 5.3.2 (tool utilizzato per l'esecuzione di test sulle interfacce di tipo WS REST);
- Il tool freeware OpenSSL v. 1.1.1c;
- un laptop come Web Based Console (sistema operativo MS Windows 10 Professional a 64 bit);
- uno smartphone dotato di sistema operativo Android (S3 mini Samsung) con installata l'app Google Authenticator, utilizzato come OTP-Device per gli OTP di tipo TOTP.

L'ambiente di test è stato configurato in modo coerente con tutte le possibili configurazioni dell'ODV. In particolare il RADIUS Server è stato utilizzato per i test sull'ODV installato come QSigCD quando non era utilizzato il meccanismo di autenticazione TOTP interno (funzionalità introdotta in DSA SW V. 9.1.9.10).

Invece, per l'effettuazione delle prove sull'ODV installato come QSealCD, nell'ambiente di test non è utilizzato il RADIUS Server, in quanto per tale tipo di dispositivo l'autenticazione di tutti gli utenti è basata su password statica.

Prima dell'esecuzione dei test il software è stato installato e configurato seguendo le istruzioni contenute nei documenti [PRE], [ADM] e [USR], come indicato nel par. 9.2.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Copertura dei test

Il Committente ha prodotto il test plan con un elenco di requisiti da testare e un rapporto di test associato, dall'esame dei quali i Valutatori hanno verificato che:

- sono stati identificati i requisiti che i test devono soddisfare;
- tali requisiti sono stati identificati univocamente con un codice identificativo;
- ogni requisito corrisponde a una TSFI, evidenziata all'interno del titolo del requisito;
- per ogni requisito, sono stati indicati i test progettati per verificare il requisito stesso, cioè la TSFI associata;
- per ogni test, associato a un identificativo numerico, è stata specificata la procedura di test, con tutti i passi previsti, la descrizione degli stessi e i risultati attesi;
- la descrizione del test permette di evincere gli obiettivi del test e le condizioni iniziali dello stesso;
- ad ogni test è stato anche associato lo stato, ovvero se il test è stato eseguito con successo o meno.

11.2.2 Risultati dei test

Per l'esecuzione dei test funzionali proposti dal Fornitore, e per la riesecuzione degli stessi da parte dei Valutatori, sono stati utilizzati i tool messi a disposizione dal Fornitore.

Trattandosi di una ri-certificazione, in una prima fase i Valutatori hanno eseguito una serie di test mirati a verificare, a titolo di non regressione rispetto alla versione già certificata (DocuSign Signature Appliance v8.4), il corretto comportamento delle TSFI, in modo da rilevare in tempi brevi eventuali problemi macroscopici sull'ODV.

I test effettuati hanno evidenziato la necessità di installare un nuovo file di configurazione DLM dell'appliance (DisWPAD.dlm) che nella versione iniziale non era compatibile con la funzionalità di software upload da Web Console.

I test effettuati dai Valutatori hanno dato esito positivo.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI. Il tool freeware POSTMAN ha permesso di effettuare delle chiamate WS/REST configurando liberamente i parametri da inviare all'ODV.

Per ogni test è stata predisposta una scheda apposita; tali schede sono state utilizzate sia come piano dei test dei Valutatori sia come rapporto dei test stessi, opportunamente compilate con i risultati.

Nella progettazione dei test indipendenti, i Valutatori hanno considerato aspetti che nei test del Fornitore erano non presenti o ambigui o eseguiti inizialmente non verificati con esito positivo o inseriti in test più complessi che interessavano più interfacce contemporaneamente ma con un livello di dettaglio non ritenuto adeguato.

I Valutatori, infine, hanno anche progettato ed eseguito alcuni test in modo indipendente da analoghi test del Fornitore, sulla base della sola documentazione di valutazione. I test indipendenti definiti dai Valutatori hanno avuto i seguenti principali obiettivi:

- verificare la correttezza della procedura di installazione dell'appliance DocuSign e preparare i dispositivi DocuSign utilizzati per i test, compresa la funzione di Reset to Factory Settings;
- verificare le operazioni consentite a un utente Firmatario: attivazione, operazioni di firma, inserimento, aggiornamento e cancellazione di firme grafiche, blocco dopo N tentativi di login errati;
- verificare le operazioni consentite a un utente Amministratore: creazione, abilitazione/disabilitazione e sblocco degli utenti, cambio password, imputabilità delle azioni eseguite.

Il completamento dell'attività di test ha richiesto una sospensione di due settimane per il rilascio di una nuova versione dell'ODV per la corretta registrazione degli eventi di Tamper e Tamper Reset nel file di log dell'ODV e delle ambiguità nella documentazione sull'utilizzo delle API REST.

Al termine della sessione finale di test effettuata dai Valutatori, tutti i test hanno dato esito positivo.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali.

I Valutatori hanno innanzitutto verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione, cioè quelle indicate nel [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)

In una prima fase i Valutatori hanno esaminato fonti di informazione pubbliche per la ricerca di potenziali vulnerabilità dell'ODV. Dalla ricerca non sono risultate vulnerabilità potenziali.

Successivamente, è stata effettuata la ricerca di vulnerabilità di rete, utilizzando gli scanner di vulnerabilità Nessus e Burp Suite Pro. Gli scanner non hanno rilevato vulnerabilità potenziali.

I Valutatori hanno effettuato un'analisi differenziale del sorgente fornito dalla versione precedente 8.4 alla nuova 9.1.9.10 per meglio tracciare le modifiche apposte al codice nella nuova versione. I Valutatori mediante il tool responder.py hanno verificato a titolo di non regression test, che il problema (invio in rete di hash NetNTLM) emerso nel corso della valutazione della versione 8.4 dell'ODV, risolto con l'applicazione del software update DisWPAD.dlm, continua a non essere più presente.

I Valutatori hanno effettuato un'analisi manuale parziale del codice sorgente al fine di individuare debolezze nell'implementazione del nuovo meccanismo di TOTP interno e di nuove vulnerabilità nel codice che gestisce le richieste RPC e REST, che si è conclusa senza evidenziare vulnerabilità sfruttabili.

I Valutatori hanno inoltre effettuato l'analisi statica dell'intera codebase tramite il tool Cppcheck per individuare eventuali bug che potrebbero produrre dei memory error o l'utilizzo di funzioni di libreria non sicure, che non ha evidenziato bug significativi per la sicurezza.

Successivamente, i Valutatori hanno esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza e documentazione operativa) al fine di evidenziare eventuali vulnerabilità potenziali dell'ODV.

Da queste analisi, congiuntamente a quella del codice sorgente, i Valutatori hanno effettivamente determinato la presenza di una vulnerabilità potenziale:

- è stata individuata una versione obsoleta della libreria JQuery utilizzata dalla Web Console che presenta vulnerabilità note per quanto di fatto non sfruttabili nell'ambiente operativo dell'ODV in quanto la Web Console è sottoposta a controlli fisici e ispezioni da parte dell'appliance administrator e quindi non offre opportunità di attacco da parte di agenti ostili. È stata emessa una raccomandazione da parte dell'LVS affinché fosse effettuato un aggiornamento della libreria.

I Valutatori non hanno riscontrato la presenza di vulnerabilità potenzialmente sfruttabili da un attaccante con potenziale di attacco High e l'attività di verifica delle vulnerabilità si è pertanto conclusa con esito positivo senza il progetto e l'effettuazione di test di intrusione specifici.

Da segnalare inoltre che è stata emessa una raccomandazione allo Sviluppatore per consigliare di iniziare a offrire un servizio di sanificazione/sostituzione di fabbrica per l'hardware dell'appliance agli utenti finali in caso di manomissioni, essendo quest'ultime difficilmente rilevabili non solo dagli utenti ma anche dagli amministratori dell'ODV.