DocuSign Overview

DocuSign è diventato in pochi anni uno standard globale per gestire le transazioni digitali basate su documenti elettronici (Digital Transaction Management) ed è oggi il sistema al mondo più usabile e più usato con oltre 100.000 aziende clienti e 50 milioni di utenti.
Di facile uso, è comunque una soluzione che garantisce la riservatezza dei dati che vengono crittografati in modalità sicure, al tempo stesso la versatilità e l'aderenza alle normative rendono la soluzione legalmente accettata in tutto il mondo.
Grazie all'utilizzo di infrastrutture leader di mercato, il servizio è in grado di garantire elevatissimi livelli di servizio, con un uptime sempre prossimo al 100%.
DocuSign consente la preparazione, esecuzione e gestione di transazioni elettroniche in ambiente completamente digitale:

1. Gli utenti predispongono le transazioni elettroniche impostando l'ordine in cui le stesse devono essere completate e i ruoli associati ad ogni step.

2. Le transazioni vengono eseguite con livelli di sicurezza enterprise e metodi di autenticazione avanzati per convalidare l'identità dei firmatari. Le firme elettroniche apposte sono considerate giuridicamente vincolanti.

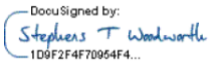
3. completezza di informazioni per reporting dettagliati e prova di conformità.

DocuSign, infatti, implementa un modello di firma elettronica avanzata (remota).
L'OTP (One Time Password) gestito all'interno della soluzione e richiesto al momento della firma poiché consente di autenticare il firmatario in maniera certa.

DocuSign supporta la firma elettronica avanzata (remota) nei seguenti modi:

- **Identificazione univoca del firmatario**

  DocuSign offre un processo sicuro e verificabile di adozione da parte del firmatario della propria firma elettronica. Grazie all'autenticazione dell'e-mail, all'indirizzo IP e a ulteriori metodi di autenticazione, il Servizio DocuSign è in grado di associare in maniera univoca il firmatario alla firma elettronica.



- **Blocco del documento firmato in maniera tale da rilevare eventuali modifiche ai dati**

  Una volta apposta la firma elettronica sui documenti, il Servizio DocuSign appone ai documenti un sigillo di antimanomissione di blocco (utilizzando il metodo hash e la crittografia), utilizzando un certificato digitale globale di firma.

- **Procedure consigliate in caso di controversie**

  In caso di controversie riguardanti un contratto stipulato in maniera elettronica, la semplice conformità alla direttiva UE non è sufficiente. La conformità alla direttiva UE è un passo importante nel processo di selezione di una piattaforma di firma elettronica. Tuttavia, così come i documenti cartacei, i documenti firmati elettronicamente possono essere oggetti di controversie. Il processo di apposizione della firma deve fornire prove sufficienti a conferma della transazione. DocuSign garantisce la raccolta e la conservazione di molti elementi che possono risultare determinanti in caso di controversia per impedire eventuali disconoscimenti di una firma.

Di seguito l'elenco completo degli elementi disponibili a tale scopo:

1. Itinerario di controllo con contrassegno di ora/data di tutte le azioni svolte dal firmatario.

2. Crittografia protetta che consente di leggere e firmare i documenti solo agli utenti designati.

3. Firme univoche create da ciascun utente, accessibili solo dagli utenti corrispondenti e memorizzate online in maniera protetta.

4. Aree di firma (Stick-eTab) richieste, che consentono ai firmatari di apporre le iniziali e la firma su parti specifiche del documento.

- Intenzione di apporre la firma
  Nei documenti cartacei, la collocazione precisa della firma è un criterio importante per stabilire l'intenzione del firmatario. La soluzione DocuSign consente tale trasposizione anche nella forma elettronica.

- Elementi di protezione della firma
  I documenti firmati utilizzando la piattaforma DocuSign presentano una protezione completa e un itinerario di controllo rigoroso delle persone che hanno apposto le firme e dell'ora e la data in cui sono state apposte. In tal caso, parliamo di certificato di completamento: Il certificato di completamento e i documenti firmati in maniera digitale e con sigillo di garanzia sono gli elementi chiave per eseguire e garantire un corretto processo di FEA.

- Ammissibilità in sede probatoria
  Gli Stati membri dell'Unione Europea, tra cui anche l'Italia, prevedono l'ammissibilità in sede probatoria dei record elettronici e delle riproduzioni di questi ultimi. Nel caso della Firma Elettronica Avanzata, l'Art.21 del D.lgs n.85/2005 e ss.mm.ii. detto Codice dell'Amministrazione Digitale (CAD) stabilisce che, in caso di disconoscimento, con l'adozione di tale metodologia di firma risulti fondamentale dimostrare ai tribunali quanto segue:

  - l'identificazione del firmatario e la connessione univoca dello stesso al documento firmato;

  - Tale connessione è creata utilizzando dei mezzi sui quali il firmatario può conservare il controllo esclusivo;

  - consente di rilevare se i dati sono stati modificati successivamente all'apposizione della firma elettronica avanzata.

  Il documento informatico sottoscritto con firma elettronica avanzata che garantiscano i requisiti di cui sopra, ha l'efficacia prevista dall'articolo 2702 del codice civile, il quale stabilisce che: La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta. Pertanto, il documento sottoscritto con firma elettronica avanzata ha valore legale sostanzialmente pari alla firma digitale, purché essa sia stata generata ed apposta nel rispetto delle regole tecniche di cui al decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013, pubblicato sulla Gazzetta Ufficiale n. 117 del 21 maggio 2013.

Elementi di sicurezza nel dataflow

1. Magnolia crea il documento e ne effettua l'upload sulla piattaforma DocuSign (con una connessione sicura TLS). Il sistema calcola automaticamente l'hash SHA-256 del documento oppure ne effettua l'encrypting AES256 utilizzando una delle migliaia di chiavi gestite dal DocuSign Key Manager. La busta digitale che contiene il documento criptato prevede dei metadati in chiaro che possono includere: Firmatario, metodo di autenticazione e storico della firma. Un nuovo record del database viene creato in modo da collegare il documento all'utente, alla chiave di encrypting, l'hash e la dimensione del file.

2. A questo punto, Magnolia inserisce i firmatari previsti per il documento. Tali utenti vengono quindi creati, associando loro i relativi indirizzi e-mail e i diritti per la visione del documento in chiaro. La tabella utente e la tabella di account vengono collegate attraverso una tabella di appartenenza, che determina a quali account gli utenti possono avere accesso.

3. I firmatari ricevono una e-mail che li invita ad accedere al portale Docusign per firmare i documenti (attraverso una connessione sicura TLS).

4. Quando il firmatario clicca sul link contenuto nella mail, l'accesso al documento è garantito attraverso un'autenticazione via e-mail.

5. Il documento è presentato in chiaro solo a dei firmatari prederminati e protetto da una sessione sicura TLS, così come i documenti scaricati.

6. I firmatari devono eseguirà un'azione esplicita per firmare un documento all'interno di una sessione sicura TLS. Nel caso in cui il documento venga scaricato in locale, viene applicata una "firma elettronica della piattaforma", in modo tale che in fase di consultazione sia possibile verificare se il documento sia stato modificato dopo il download. Dal momento che il documento può essere scaricato anche prima che il workflow di firma sia completato, qualsiasi documento (il cui workflow è terminato o no) contiene una firma elettronica della piattaforma. Qualsiasi azione di firma è memorizzata all'interno di un record del database DocuSign, memorizzando l'hash del documento in modo da garantirne l'integrità prima di criptarlo per il salvataggio nello storage della piattaforma.

7. Il processo sopra descritto è reiterato per tutti i firmatari.

8. Quando il workflow di firma del documento è completato da tutti i firmatari viene firmato utilizzando una chiave asimmetrica della piattaforma (sigillo). In questo modo si rende impossibile qualsiasi modifica ulteriore al documento e garantisce che il documento contenente le firma di essere validato dalla chiave pubblica di DocuSign senza necessità di accedere alla versione non criptata del documento.

9. La piattaforma applica una segregazione delle responsabilità, in modo tale che gli amministratori con accesso alle chiavi di encrypting non abbiano accesso anche ai dati criptati

Datacenter

La piattaforma DocuSign eroga il servizio in modalità Software as a Service (SaaS) in regime di Business Continuity attraverso due datacenter ridondati localizzati in Amsterdam (Olanda) e Francoforte (Germania). I dati trattati all'interno del servizio offerto sono dunque memorizzati esclusivamente all'interno del territorio dell'Unione Europea. Tutti i datacenter sono oggetto di certificazione ISO27001.