

SERVIZIO DI FIRMA ELETTRONICA AVANZATA EROGATO DA E-WORK SPA

INFORMATIVA - CONDIZIONI RELATIVE ALL'USO DELLA FIRMA ELETTRONICA AVANZATA - CARATTERISTICHE TECNICHE DEL SISTEMA

Informazioni Generali

e-work spa ha scelto di introdurre e di proporre, in via facoltativa, ai suoi clienti e lavoratori l'utilizzo di una tecnologia digitale innovativa per migliorare l'efficienza nella sottoscrizione di tutti i documenti che richiedono una o più firme autografe, evitando così la stampa dei documenti da firmare.

La sottoscrizione dei documenti avviene mediante l'utilizzo di firma elettronica avanzata, ovvero una modalità di firma che possiede i requisiti giuridici ed informatici come da normativa che regola questa materia è contenuta sia nel Decreto Legislativo n. 82/2005 (Codice dell'Amministrazione Digitale) che nel DPCM del 22 Febbraio 2013 pubblicato in Gazzetta Ufficiale il 21 Maggio 2013.

In particolare la procedura di firma elettronica avanzata proposta rispecchia gli articoli contenuti nell'Articolo V del suddetto DPCM.

I documenti che l'utente deciderà di sottoscrivere con la procedura di firma elettronica avanzata, saranno a tutti gli effetti documenti informatici che:

- sul piano tecnico soddisfano i requisiti di sicurezza definiti dalla normativa vigente;
- sul piano giuridico hanno lo stesso valore dei documenti cartacei sottoscritti con firma autografa.

e-work spa è l'erogatore della soluzione di Firma Elettronica Avanzata (così come da definizione contenuta nel DPCM 22-02-2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali", all'articolo 55, comma 2, lettera a).

Firma elettronica avanzata

Il processo associato al sistema di *firma elettronica avanzata* garantisce:

1. l'identificazione del firmatario;
2. la connessione univoca della firma al firmatario;
3. il controllo esclusivo del firmatario del sistema di generazione della firma;
4. la possibilità di verificare che il documento sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
5. la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
6. l'individuazione dell'intermediario (e-work spa) che realizza la soluzione di *firma elettronica avanzata e che funge da Certification Authority per l'emissione dei Certificati Digitali di firma FEA*;
7. l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
8. la connessione univoca della firma al documento sottoscritto;

Il processo di firma elettronica avanzata implementato da e-work spa prevede due modalità:

- Firma con uso di Certificati Digitali, emessi dalla CA e-work Spa
- Firma Grafometrica

1. Descrizione delle caratteristiche del sistema che garantiscono l'identificazione del firmatario

- FEA Grafometrica – In questo caso e-work spa (di seguito, anche solo, "e-work") identifica preliminarmente il firmatario dei documenti (generalmente il Lavoratore Somministrato ma anche l'Utilizzatore, di seguito Utente) richiedendo il relativo documento d'identità in corso di validità ed assistendo l'Utente in tutte le fasi di visualizzazione e firma dei documenti
- FEA con Certificati Digitali – In questo caso e-work identifica i propri Utenti che saranno

i firmatari mediante la raccolta del documento d'identità o più in generale con le stesse modalità previste oggi per il cartaceo.

2. Descrizione delle caratteristiche del sistema che garantiscono la connessione univoca della firma al firmatario

Prima di procedere con l'apposizione delle proprie firme, il firmatario può consultare interamente il documento informatico, controllandone e validandone i contenuti direttamente a video. Tale documento informatico ripropone le medesime caratteristiche delle precedenti versioni cartacee, ma è di più semplice ed efficace gestione.

- FEA Grafometrica - Il sistema registra le caratteristiche dinamiche della firma autografa che il firmatario appone di suo pugno con penna elettronica sull'apposito dispositivo di firma ("signature PAD"). Le caratteristiche registrate corrispondono alla scansione temporale di posizione, vale a dire il ritmo, la velocità e la pressione della penna, quali quelle acquisite con opportuna risoluzione. L'univocità della connessione viene garantita dalla sottoscrizione effettuata davanti all'operatore di filiale, previa identificazione del firmatario, e alla possibilità di effettuare un'eventuale perizia grafica, in modo del tutto equivalente a quanto previsto per una firma autografa su carta.

Il processo consente di visualizzare, anche a distanza di tempo, la firma apposta sul documento informatico e di confrontarla visivamente con le altre presenti sullo stesso documento o su altri documenti, apposte dallo stesso soggetto, evidenziando oltre alla grafia anche ulteriori informazioni quali la data, l'ora nonché, eventualmente, il luogo di apposizione. L'utente, utilizzando il signature PAD collegato al PC via USB, firma con la penna in dotazione, esattamente come farebbe su carta. Il sistema è in grado di rilevare le caratteristiche comportamentali del firmatario, quali la posizione (coordinate), la velocità, il ritmo e la pressione. Terminata l'operazione, il sistema visualizzerà la firma grafica apposta dall'utente, provvedendo a cifrare i dati biometrici e l'hash del documento, in modo da garantire l'assoluta indissolubilità dei dati rispetto al documento PDF visualizzato e sottoscritto. Non è pertanto consentita l'estrazione dei dati biometrici né la loro associazione ad un altro documento, diverso da quello sottoscritto. Una volta inseriti nel documento PDF, i dati biometrici vengono peraltro distrutti e cancellati sia dalla memoria applicativa che dalla memoria del sistema su cui opera l'applicazione. Durante la sottoscrizione con firma grafometrica, viene generato per ogni firma un nuovo Certificato intestato al firmatario. Tale Certificato permette di effettuare, a tutti gli effetti, una firma PDF del documento, in modo da renderla visibile e verificabile con gli strumenti più diffusi (Client Adobe, ecc.). Il processo di firma prevede la creazione di una busta Cades, tipicamente utilizzata per le firme PDF, all'interno della quale sono inseriti la firma dell'hash del documento originale e, come ulteriori attributi della firma, una sorta di blob cifrato, costituito dall'hash stesso e dai dati biometrici. Tale blob viene a sua volta firmato ed inserito nella busta Cades.

- FEA con Certificati Digitali - Questa modalità è fruibile a seguito di un'autenticazione effettuata sul portale <https://e-job.e-workspa.it/login.php> con UserID e Password gestita direttamente dall'utente. Dopo essersi autenticato l'utente potrà visionare, consultare ricercare e firmare i propri documenti PDF in modalità singola, tramite la piattaforma di visualizzazione sicura Web2Sign oppure in modalità massiva direttamente dall'interfaccia di ricerca documenti. La *firma elettronica avanzata*, da applicare ovviamente ai documenti PDF visualizzati in modalità sicura sempre con l'utilizzo della piattaforma **Web2Sign**. In particolare l'utente potrà apporre firme elettroniche solo sui campi già predisposti alla ricezione della firma elettronica.

L'utente potrà firmare se e solo se dotato di un Certificato Digitale in precedenza rilasciatogli da e-work. Le credenziali per l'uso di detto Certificato sono obbligatoriamente diverse dalle credenziali di accesso al portale e-workspa.it e l'avvio delle attività di firma avviene a seguito dell'immissione di due codici, uno statico o PIN, ricevuto dall'utente in fase di rilascio del Certificato, il secondo dinamico OTP, che può essere ricevuto via SMS, via e-mail o generato tramite un'apposita APP per Mobile Phone, garantendo in questo modo un'autenticazione forte e sicura a 2 fattori.

3.

Descrizione delle caratteristiche del sistema che garantiscono il controllo esclusivo del firmatario sul sistema di generazione della firma

Durante la fase di firma, il sistema è sotto il controllo esclusivo del firmatario. Lo schermo del dispositivo di firma mostra il documento completo, consentendo al firmatario di verificare personalmente i propri dati ed ogni dettaglio contrattuale mediante scorrimento.

- FEA Grafometrica –

Durante l'apposizione della firma grafometrica, lo schermo rappresenta in tempo reale il segno grafico tracciato ed apposite funzioni consentono al firmatario di cancellare in caso di errori. L'operatore non può in alcun modo interferire sino alla conclusione dell'operazione o sino all'annullamento del processo. L'applicazione di firma grafometrica registra i parametri comportamentali del firmatario senza che nessun altro interlocutore – sia esso una persona o un processo – possa agire sul documento, nel momento in cui il firmatario appone la firma il tratto grafico viene visualizzato e direttamente cifrate le informazioni nello spazio dedicato alla firma, le informazioni al termine dell'apposizione della firma vengono immediatamente rimosse dal sistema utilizzato, memoria RAM e fisica; in questo modo non possono essere oggetto di altro utilizzo ma ogni firma successiva sarà costituita da altri nuovi parametri che subiranno comunque il medesimo trattamento. Oltre alla cancellazione immediata di tutte le informazioni grafometriche, i livelli di sicurezza degli strumenti utilizzati ("devices") e il collegamento cifrato permettono di garantire l'assoluta impossibilità di catturare detti dati da altre figure o processi.

- FEA con Certificato Digitale –

Durante l'apposizione della firma, lo schermo visualizza il contenuto del documento PDF. nel caso di firma di un singolo documento.

È possibile selezionare più documenti da firmare e procedere con le operazioni di firma massiva previa la loro visualizzazione o accettazione delle clausole prima di procedere con la firma.

L'Alias del firmatario viene preimpostato applicativamente, l'utente al momento della firma dovrà inserire PIN e OTP e manifestare la propria intenzione di procedere con la firma, tutte queste attività vengono scritte con data e ora, nel log applicativo. La firma che viene effettuata è una firma di tipo PADES esattamente come definite dagli standard europei, similmente alle firme digitali.

4.

Descrizione delle caratteristiche del sistema che garantiscono di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma

Le tecnologie di firma elettronica utilizzate – sia per la firma grafometrica che per le firme con certificato, includono le impronte informatiche (c.d. "hash") del contenuto soggetto a sottoscrizione. Il controllo della corrispondenza tra un'impronta ricalcolata e quella "sigillata" all'interno delle firme permette di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma. Generalmente, al termine delle operazioni di firma, viene effettuata una verifica immediata della firma per validarne la correttezza delle operazioni, inoltre tutti i documenti verranno successivamente portati in conservazione sostitutiva. Questo passaggio è effettuato in automatico e con scadenze secondo le esigenze di e-work che possono essere modificate in qualsiasi momento all'interno del sistema.

5.

La descrizione delle caratteristiche del sistema che garantiscono la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto

All'atto della presentazione del documento per la firma, il firmatario può visualizzare il contenuto in tutte le sue parti, con apposite funzioni di posizionamento e ingrandimento. Le caratteristiche del dispositivo di *firma elettronica avanzata* sono opportunamente scelte per garantire la miglior leggibilità.

Successivamente il firmatario potrà visualizzare il documento elettronico per mezzo di uno strumento informatico standard, di cui avrà piena disponibilità, su supporto duraturo che permetterà la conservazione e la stampa del documento in ogni momento (es. software gratuito PDF Reader). In alternativa potrà richiedere copia ad e-work spa.

6.

Descrizione delle caratteristiche del sistema che garantiscono l'individuazione del soggetto erogatore della soluzione di firma elettronica avanzata.

Il certificato di firma della *firma elettronica avanzata* individua il soggetto erogatore del servizio ed è emesso da un'autorità di certificazione tecnica, riconducibile a e-work spa, con visualizzazione della dicitura "e-work SpA" ("Dettagli certificato").

7.

Descrizione delle caratteristiche del sistema che garantiscono l'assenza nell'oggetto della sottoscrizione di qualunque elemento idoneo a modificarne gli atti, i fatti e i dati in esso rappresentati

I documenti prodotti dal sistema utilizzano esclusivamente formati atti a garantire l'assenza, nell'oggetto della sottoscrizione, di qualunque elemento idoneo a modificare gli atti, i fatti e i dati in essi rappresentati (formato standard ISO PDF/A).

8.

Descrizione delle caratteristiche del sistema che garantiscono la connessione univoca della firma al documento sottoscritto

I dati della firma vengono inseriti nel documento in una struttura, detta "vettore grafometrico", che li unisce indissolubilmente all'impronta informatica del documento sottoscritto. Questa struttura è protetta con opportuna tecnica crittografica, al fine di preservare la firma da ogni possibilità di estrazione o duplicazione. L'unica chiave crittografica in grado di estrarre le informazioni è in esclusivo possesso di pubblico ufficiale (notaio), appositamente designato da e-work e potrà essere usata in sede di perizia per attestare l'autenticità del documento e della sottoscrizione.

Il sistema appone, per ogni firma eseguita, una corrispondente "firma tecnica" in formato standard PADES. A differenza del "vettore grafometrico" queste firme tecniche sono visibili e verificabili con gli strumenti informatici standard per la presentazione e lettura dei documenti (es. PDF Reader).

Per quanto riguarda invece la firma con Certificato, la visualizzazione della firma, cioè la fase di verifica mostra i dati presenti nel certificato che conducono alla persona fisica che ha effettuato l'operazione di firma a seguito di un'autenticazione forte quindi riconducibile esclusivamente al proprietario del Certificato stesso.

9.

Descrizione delle caratteristiche delle tecnologie utilizzate nel servizio di Firma Elettronica Avanzata che consentono di garantire i requisiti previsti ai precedenti punti da 1. a 8.

Il trasferimento dei dati e la loro memorizzazione nel "vettore grafometrico" è protetto con le seguenti tecnologie crittografiche:

- crittografia simmetrica standard AES con chiave a 256 bit segreta e IV condiviso per la protezione dei dati;
Lo scambio delle informazioni biometriche tra i *devices* che le rilevano, siano essi *signature PAD* (Es: Wacom STU-430) e il sistema computer/server sul quale gira l'applicazione Web2Sign viene così garantito:
 - *signature PAD*, i *devices* sono collegati tramite porta USB al computer che mostra il documento da firmare; viene generata ogni volta (per ogni firma che l'utente deve apporre) una differente chiave di sessione AES 256 per cifrare i dati che, tramite cavo USB, transitano dal PAD al computer; una volta ricevuti dal computer, questi dati subiscono una nuova cifratura asimmetrica insieme all'hash del documento, come già sopra descritto,
- RSA 2048 bit con chiave privata detenuta da una terza parte per la cifratura della chiave AES.

La cifratura è di tipo asimmetrico e perciò effettuata utilizzando una coppia di Chiavi/Certificato RSA 2048 rilasciati da una CA iscritta presso AGID. In particolare, per la Cifratura dei dati viene utilizzata la parte pubblica (Certificato), mentre, la decifratura degli stessi, potrà essere effettuata solo avendo diritto di accesso alla corrispondente chiave privata, solitamente custodita in un apparato sicuro a norma, HSM o su di una Smart Card, custodita presso una cassetta di sicurezza dell'Ente stesso, di un Notaio o

di una CA, garantendo così l'accesso esclusivo ad utenti che ne abbiano il diritto (Pubblico Ufficiale/Magistratura) in caso di contenzioso;

- durante la fase di firma grafometrica, viene generato per ogni firma un nuovo Certificato intestato all'utente che appone la propria firma grafometrica, il quale permette di effettuare, a tutti gli effetti, una firma PDF del documento in modo tale che sia visibile e verificabile con tutti gli strumenti di verifica più diffusi (per esempio, Client Adobe); viene dunque creata una PKI/CA apposita per lo scopo sopra descritto.

Il processo di firma avviene con le seguenti modalità:

- viene creata una busta Cades tipicamente utilizzata per le firme PDF,
- all'interno di essa vengono inseriti:
 - i) la firma dell'hash del documento originale e, come ulteriori attributi della firma e ii) una sorta di blob cifrato costituito dall'hash del documento e dai dati biometrici, detto blob viene anch'esso firmato ed inserito nella busta Cades, terminando così l'attività di firma dell'utente grafometrico;
- firma elettronica con Certificato del documento PDF effettuata con firma PADES (Standard e come nel caso della firma digitale).

10.

Descrizione delle modalità attraverso cui gli utenti possono richiedere copia gratuita del modulo di adesione, da questi sottoscritto, al servizio di firma elettronica avanzata.

Gli utenti possono richiedere gratuitamente a e-work una copia cartacea del modulo di adesione al servizio di *firma elettronica avanzata* presentandosi personalmente presso una delle filiali e-work oppure mediante raccomandata A/R corredata di copia del documento valido di riconoscimento. Con analoga modalità possono richiedere, in qualsiasi momento, la revoca della adesione al servizio FEA, tornando quindi ad operare con la tradizionale firma autografa su documentazione cartacea.

11.

Descrizione delle modalità attraverso cui i clienti possono richiedere le informazioni di cui ai precedenti punti da 1. a 8.

Il presente documento, contenente le informazioni relative alle caratteristiche del servizio di *firma elettronica avanzata* ed alle tecnologie su cui questo si basa, è pubblicato in evidenza nella home page del sito internet www.e-workspa.it, risultando in tal modo sempre disponibile per gli utenti ed il pubblico in generale.

Per ogni ulteriore informazione, è comunque possibile rivolgersi direttamente a e-work spa via Cola Montano, 32 - 20159 Milano tel. 02.673381.

12.

Conservazione dei dati

La conservazione a norma è un processo che permette di archiviare in modo sicuro i documenti informatici sottoscritti dall'utente affinché questi restino integri e risultino immodificabili e leggibili nel tempo. A tal proposito E-work spa. utilizza un servizio di conservazione dei documenti informatici secondo le modalità definite dal D. Lgs. n.82/2005 (Codice dell'Amministrazione Digitale). I documenti sottoscritti dall'utente vengono inviati al sistema di conservazione una volta concluso il processo di sottoscrizione, garantendone così l'integrità, la non modificabilità e la validità nel lungo periodo. I documenti vengono memorizzati su idonei supporti informatici che ne permettono la conservazione per la durata definita dalla legge.

13

Informazioni riguardanti la copertura assicurativa.

E-work S.p.A. ha stipulato, in data 18/01/2017 in ottemperanza alle previsioni legislative contenute nel DPCM 22-02-2013, art. 57, comma 2, una polizza assicurativa - rilasciata da primaria assicurazione Zurich Insurance PLC abilitata ad esercitare nel campo dei rischi industriali - per la responsabilità civile da danno a terzi eventualmente derivante dalla fornitura del servizio di FEA.