



i Processi di Firma Elettronica Avanzata



Riferimenti normativi	2
Le soluzioni FEA di FirmoSemplice	3
Gli effetti giuridici	6
Conformità alla norma	6
Copertura Assicurativa	6
Le FEA di FirmoSemplice	7
Firma Elettronica Avanzata basata su SPID	7
Il Processo	8
Firma Elettronica Avanzata basata su CIE	10
Il Processo	11
Firma Elettronica Avanzata basata su Self IDp	13
Il Processo di FEA da Remoto con Self IDP	14
Il Processo di FEA in Presenza con Self IDP	16
Il Processo di FEA in Grafometrica con Self IDP	18
Obblighi e Solidità del processo	20

Riferimenti normativi

AgID	Agenzia per l'Italia Digitale: www.agid.gov.it
CAD	"Codice dell'Amministrazione Digitale" Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni.
FEA	"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate". DPCM del 22 febbraio 2013, Art.26 Reg. UE 910/2014 (eIDAS) Decisione di esecuzione (UE) 2015/1506
EIDAS	"Identificazione elettronica e servizi fiduciari per le transazioni elettroniche" Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014,
SPID	"Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)". DPCM del 24 ottobre 2014
CIE	"Carta di Identità Elettronica (CIE)" Decreto Ministero, Interno 23/12/2015 , G.U. 30/12/2015 e successive modificazioni
QTSP	Qualified Trust Service Providers accreditato da eIDAS
Soggetto Erogatore FEA	"coloro che mettono a disposizione il servizio di firma elettronica avanzata a soggetti terzi per motivi istituzionali, societari o commerciali" DPCM del 22 febbraio 2013, Art.55 comma 2 lettera a:
Soggetto realizzatore di soluzione FEA	"colore che realizzano soluzioni di firma elettronica avanzata a favore dei soggetti erogatori DPCM del 22 febbraio 2013, Art.55 comma 2 lettera b

Le soluzioni FEA di FirmoSemplice

La società 01Sistemi srl ha inglobato recentemente le sue startup innovative, fra cui FirmaSPID Srl, fondata nel 2018, sviluppatasi investendo nella realizzazione sistemi di firma elettronica, sfruttando le tecnologie già note ed aggiungendo ad esse anche le caratteristiche messe a disposizione dagli strumenti innovativi come: il sistema pubblico di identità digitale o SPID e la Carta d'Identità Elettronica o CIE e sviluppando con essi processi di firma elettronica avanzata da remoto.

Partendo dall'esperienza di una piattaforma di firma elettronica avanzata (FEA) basata su SPID (Sistema Pubblico di Identità Digitale), progetto già operativo e funzionante sin dai primi mesi di attività, ha poi realizzato poi un HUB evoluto di firma elettronica avanzata denominato FirmoSemplice, che integra due nuove soluzioni basate sull'utilizzo di sistemi di Identità Digitali Pubbliche come SPID e CIE, con una soluzione basata su un'identità digitale privata.

Di pari passo alla realizzazione della piattaforma FirmoSemplice, la società 01Sistemi srl, attraverso la sua capogruppo Maggioli SpA, offre anche il servizio di aggregazione, per soggetti pubblici e privati, a SPID e a CIE

FirmoSemplice consente dunque a qualsiasi soggetto erogatore (impresa, organizzazione), senza l'esigenza di dotarsi di complesse infrastrutture informatiche e senza l'esigenza di ottenere particolari accreditamenti ed autorizzazioni, di proporre alla propria utenza/clientela differenti processi di firma elettronica avanzata basati sulle credenziali già in possesso dell'utenza (identity Provider gestiti da terze parti qualificate SPID/CIE) o su quelle che egli stesso gli ha rilasciato dopo aver espletato un adeguato processo di identificazione (identity Provider proprio)

Il cittadino/utente potrà quindi firmare in presenza o da remoto da remoto tramite diverse soluzioni tecnologiche che traggono la loro originalità dalla fase iniziale di identificazione certa del soggetto firmatario. Nella piattaforma FirmoSemplice l'identificazione del soggetto può avvenire in tre diverse modalità , non esclusive.

La prima modalità di identificazione e le successive autenticazioni possono avvenire attraverso l'identità digitale pubblica del Cittadino:

- **SPID:** utilizzando il sistema di accesso a più fattori (2FA) del Livello 2 di SPID
 - **Entra con SPID - Livello 2:**
Autenticazione con **username**, **password** e un **codice temporaneo OTP** (One-Time Password). L'OTP può essere ricevuto via SMS o generato tramite un'app dedicata (fornita dal gestore SPID).

- **CIE:** la Carta d'Identità Elettronica (CIE) offre diverse modalità di autenticazione, sinteticamente:
 - **Credenziali CIE (livello 1 e 2):**
 - **Entra con CIE - Livello 2:**
Autenticazione con username e password, più un codice temporaneo OTP (One-Time Password) ricevuto via SMS o tramite notifica push sull'app CieID, oppure tramite scansione di un QR code con l'app CieID.
 - **Entra con CIE - Livello 3:**
È necessario uno smartphone dotato di tecnologia NFC e l'app CieID installata. L'autenticazione avviene avvicinando la CIE allo smartphone e inserendo il PIN. In alternativa, da computer è possibile utilizzare un lettore di smart card contactless per la lettura della CIE e il relativo PIN.
 - **Entra con CIE - modalità "desktop + smartphone" livello 2 e 3:**
dove l'autenticazione inizia da computer e si completa tramite l'app CieID sullo smartphone (scansione QR code o lettura NFC).

Alla modalità di identificazione espletate ricorrendo alle identità digitali pubbliche (SPID e CIE) la piattaforma si può integrare a repository anagrafici (Self Identity Provider), gestiti, popolati e mantenuti in maniera conforme a questo previsto da Art.57 del DPCM del Febbraio 2013, dal soggetto erogatore Art.55, comma 2 tipo A. Che quindi si assume la responsabilità di identificare correttamente il soggetto, di acquisire copia del documento di identità in corso di validità.

- **Self IDP:** utilizzando il sistema di accesso a più fattori (2FA) del Livello 2
 - **Entra con Self ID - Livello 2:**
Autenticazione con **username**, **password** e un **codice temporaneo OTP** (One-Time Password). L'OTP può essere ricevuto via SMS o generato tramite un'app dedicata (fornita dal gestore SPID).

Indipendentemente da come sarà fatta la fase di identificazione e successiva autenticazione (SPID, CIE, Self IDP) la fase di somministrare dell'informativa sulle caratteristiche del processo FEA e la sottoscrizione del documento di accettazione saranno puntualmente verificate e gestite automaticamente da FirmoSemplice, in modo che nessun soggetto possa accingersi a sottoscrivere un documento senza che abbiamo prima sottoscritto il documento di accettazione.

Gli effetti giuridici

La piattaforma FEA FirmoSemplice, consente, come previsto dalle norme, di sottoscrivere i documenti inerenti i rapporti giuridici intercorrenti tra il sottoscrittore ed il soggetto che eroga la soluzione di firma elettronica avanzata ed ha l'efficacia prevista dall'articolo 2702 del Codice Civile.

La FEA può essere validamente utilizzata per la sottoscrizione di tutti gli atti/documenti esclusi quelli previsti nei punti da 1 a 12 dell'art. 1350 del Codice Civile, richiamato da art. 21 comma 2bis del CAD.

Conformità alla norma

Tutte le soluzioni incluse nella piattaforma FirmoSemplice sono state implementate in maniera da essere conformi ai requisiti previsti dal Regolamento Europeo eIDAS (Art.26 Reg. UE 910/2014 eIDAS, Decisione di esecuzione UE 2015/1506) e dalla normativa Italiana in materia (DPCM del 22 febbraio 2013,). L'utilizzo del Sistema Pubblico di Identità Digitale SPID risponde alla normativa nazionale (DPCM del 24 ottobre 2014) , ad a quanto previsto nella convenzione riservata ai Service Provider Privati di SPID. L'utilizzo della Carta d'Identità Elettronica risponde alla normativa nazionale (Decreto Ministero, Interno 23/12/2015) ed a quanto previsto nel Manuale operativo per gli erogatori di Servizi.

Copertura Assicurativa

E' obbligo del "soggetto erogatore" di soluzioni di firma elettronica avanzata (Art.55, comma 2 lettera a del dpcm febbraio 2013), stipulare, come richiesto dalla norma (Art.57, comma 2 del dpcm febbraio 2013), una polizza assicurativa per la responsabilità civile, a tutela di eventuali danni cagionati, da inadeguate soluzione tecniche, ai titolari della firma ed a eventuali terzi.

Con la piattaforma FirmoSemplice, la società 01Sistemi srl si configura come "soggetto realizzatore" di soluzioni di firma elettronica avanzata (Art.55, comma 2 lettera b del dpcm febbraio 2013)

Le FEA di FirmoSemplice

Come già esplicitato la piattaforma FirmoSemplice mette a disposizione dei soggetti erogatori che l'adottano diversi tipologie di FEA, che si differenziano in particolare per le modalità di identificazione e riconoscimento del soggetto firmatario. Di seguito saranno descritti i processi di firma elettronica avanzata per ognuna delle tipologie disponibili.

Firma Elettronica Avanzata basata su SPID

SPID, il Sistema Pubblico di Identità Digitale, che come noto è il sistema nazionale pubblico di identificazione e autenticazione del cittadino, idoneo ad identificarlo informaticamente in maniera certa (secondo uno di tre possibili livelli di sicurezza) al fine di consentire l'accesso ai servizi online offerti dalla pubblica amministrazione e dai privati.

L'identità digitale SPID viene rilasciata al Cittadino che ne fa richiesta attraverso un rigoroso processo di identificazione espletato dagli Identity Provider. Tale processo è regolato da procedure stabilite dall'Agid (Agenzia per il Digitale) che prevedono sia il caso del rilascio "de visu", sia il caso del rilascio a distanza con video identificazione o dietro presentazione di un'altra valida credenziale informatica.

L'identity provider ha quindi la piena ed esclusiva responsabilità di garantire l'identità del soggetto a cui viene rilasciato SPID, la corretta gestione dei suoi dati sotto il profilo Privacy, l'assoluta sicurezza nelle autenticazioni/login che il cittadino andrà a fare utilizzando la sua identità digitale SPID e il vero e proprio fornitore di servizi non ha responsabilità sotto il profilo dell'identificazione.

Le credenziali SPID sono utilizzabili dal cittadino per autenticarsi nei servizi online delle Pubbliche Amministrazioni e la Legge impone alla Pubblica Amministrazione di convertire i sistemi di autenticazione dei propri servizi per accettare SPID (e la Carta di Identità Elettronica di cui si parlerà tra poco), dismettendo progressivamente altri sistemi in uso. Alcuni servizi della P.A. già oggi accettano solo accessi tramite SPID.

In Italia ha quindi pieno valore la firma elettronica avanzata di nuovo tipo, pienamente conforme alle specifiche del Regolamento EIDAS, basata - come si diceva - sull'uso dell'identità elettronica SPID, che conferisce alla firma sicurezza ancora maggiore ed esonera il soggetto che la usa dal caricarsi della responsabilità dell'autenticazione.

Questo strumento garantisce dunque:

- Identificazione del firmatario *garantita da SPID ad esclusiva responsabilità degli Identity Provider terzi al servizio, anche sotto l'aspetto Privacy*. Connessione univoca del firmatario alla firma ed al documento sottoscritto

- Controllo esclusivo del firmatario del sistema di generazione
- Le caratteristiche di qualità, sicurezza, integrità ed immutabilità del documento sono verificabili in qualsiasi momento ed in maniera del tutto autonoma da chiunque sia in possesso del documento informatico firmato
- Il processo verifica obbligatoriamente l'effettiva presa visione del documento da firmare
- La Totale indipendenza logistica: il firmatario può firmare i documenti quando vuole e ovunque si trovi, senza alcuna necessità di recarsi presso un ufficio. Gli è sufficiente essere connesso con un qualsiasi smartphone o pc
- La Totale Indipendenza da specifici dispositivi hardware: non servono tavolette grafometriche, smart card,...
- l'assenza di costi aggiuntivi, a quelli del servizio, per il cittadino firmatario, che ha diritto ad avere SPID gratuitamente.

LA FEA basata su riconoscimento SPID è quindi una vera e propria piattaforma abilitante che permette al cittadino di partecipare attivamente al processo di digitalizzazione del paese semplicemente utilizzando la propria Identità Digitale.

Il Processo

Il processo di attivazione, una tantum, della FEA con SPID prevede le seguenti macrofasi

- L'identità dell'utente è garantita da SPID, che è attiva solo se identity Provider ha effettuato la corretta identificazione del soggetto e solo se è in possesso di un suo documento di identità in corso di validità ai fini dell'identificazione. Al primo Login effettuato con SPID, che garantisce la corretta identificazione dell'utente, a questo verrà presentata, sotto forma di documento informatico, l'Informativa sulle caratteristiche, i termini e le condizioni che regolano il servizio di FEA oltre agli aspetti di tutela dei dati personali. L'utente, dopo averla letta per accettazione, potrà firmare il documento con la stessa soluzione che solo in questo primo utilizzo avrà validità di firma elettronica semplice.
- i documenti acquisiti dovranno essere conservati a norma per la durata di 20 anni.
La piattaforma prevede la possibilità, opzionale, di dare al documento di accettazione una validità a lungo termine (LTV) apponendo una Marca temporale contestualmente all'apposizione del Sigillo Digitale Qualificato (QSEAL).

Eseguito il processo di attivazione, la soluzione di FEA con SPID potrà quindi espletare a pieno le sua potenzialità, che per il firmatario si risolvono con un processo semplice ed intuitivo:

01Sistemi s.r.l.

Via Malpasso, 37

52037 Sansepolcro (AR)

Partita Iva: 01935250504

pec: amministrazione@pec.01sistemi.net

18 Aprile 2025

pag. 8

- Il Firmatario riceve (SMS, Email e opzionalmente App) la notifica in cui viene avvisato che gli è stato sottoposto un documento da Firmare.
- L'utente fa Login con SPID Livello 2 nella web application dove potrà visionare il documento.
- Solo dopo che l'utente ha scorso, quindi auspicabilmente letto e compreso tutto il documento, potrà decidere per ogni punto firma se firmare o meno.
- L'utente potrà esprimere la sua volontà su ogni singolo "punto firma", posizionandosi su di esso ed attivando il bottone "Firma". Le informazioni relative all'identificazione iniziale del firmatario stesso (asserzione saml2 da IDP), l'impronta del documento originale ed altri metadati, verranno inclusi in modalità Pades nel documento firmato attraverso l'apposizione di un Sigillo Digitale Qualificato emesso da una QTSP .
- Una volta espressa la volontà per ogni punto firma, all'utente viene mostrato un riepilogo dei singoli punti firma e richiesta una ulteriore autenticazione verso l'IdP, la cui asserzione di risposta conterrà l'impronta del documento e i dati identificativi del firmatario. Tali metadati vengono inclusi nel documento originale e il risultato firmato con il Sigillo Qualificato.
- Il documento firmato aperto con un qualsiasi lettore PDF potrà quindi essere verificato nella sua integrità e immutabilità e nella correttezza e coerenza del processo di firma, anche attraverso strumenti terzi
 - CA: l'integrità e l'immutabilità è garantita dalla catena di Sigilli Digitali Qualificati, rilasciati da un QTSP, apposti nel documento a seguito di ogni singola espressione di volontà (punto firma) ed a conclusione della sessione di ogni firmatario
 - IDP: l'identità del firmatario e l'originalità del documento iniziale sono invece garantiti dalle asserzioni avvenute fra Service Provider e Identity Provider SPID, che includono anche i loro certificati. Tali metadati oltre che inclusi nel documento devono per norma essere conservati per almeno 2 anni dall'IDP come previsto dalla normativa vigente.
- l'utente riceverà a questo punto una notifica sempre via SMS, Email e opzionalmente APP, con il riepilogo dell'operazione di firma appena effettuata, con la possibilità di visualizzare, verificare e scaricare il documento firmato.

Da notare che il processo di firma basato sul riconoscimento con SPID, sia processo, sia nelle tecnologie, è del tutto simile a quello implementato anche da INPS:

<https://www.agendadigitale.eu/cittadinanza-digitale/inps-firma-elettronica-avanzata-fea-con-spid-cosi-semplifichiamo-lape/>

Firma Elettronica Avanzata basata su CIE

CIE è la nuova Carta d'identità elettronica, un documento di identità rilasciato dai Comuni italiani su richiesta dei cittadini che ne certifica l'identità fisica e digitale. È considerata una piattaforma abilitante ai sensi del Piano Triennale per l'informatica nella Pubblica Amministrazione. Nello specifico, per il tramite della CIE 3.0 e del PIN che ciascun cittadino riceve, metà alla richiesta, metà con la carta, è possibile accedere ai servizi erogati in rete dalle PP.AA. con i massimi livelli di sicurezza.

Il microchip contactless integrato nel documento rende la CIE uno strumento unico e sicuro per la verifica dell'identità del titolare e per l'accesso ai servizi online di pubbliche amministrazioni e imprese. All'interno del microchip sono memorizzati in maniera sicura i dati personali e biometrici del titolare (foto e impronte digitali), nonché le informazioni che ne consentono l'identificazione online. Tali dati, ad eccezione delle impronte digitali, possono essere letti dalla CIE semplicemente con un computer a cui è collegato un lettore di smartcard contactless o con uno smartphone dotato di interfaccia NFC (Near Field Communication).

L'accesso con CIE può essere gestito direttamente oppure, con un processo molto più amichevole, attraverso il servizio CielD Server, gestito dal Ministero degli Interni con modalità tecnologiche del tutto simili a quelle di SPID.

CIE quindi ha tutte le caratteristiche tecnologiche e normative necessarie per essere utilizzata come identità digitale alla base di una soluzione di firma elettronica avanzata.

Questo strumento garantisce dunque:

- Identificazione del firmatario garantita da CIE e quindi dal Ministero dell'Interno.
- Connessione univoca del firmatario alla firma ed al documento sottoscritto
- Controllo esclusivo del sistema di generazione da parte del firmatario
- Le caratteristiche di qualità, sicurezza, integrità ed immodificabilità del documento sono verificabili in qualsiasi momento ed in maniera del tutto autonoma da chiunque sia in possesso del documento informatico firmato
- Il processo verifica obbligatoriamente l'effettiva presa visione del documento da firmare
- La Totale indipendenza logistica: il firmatario può firmare i documenti quando vuole e ovunque si trovi, senza alcuna necessità di recarsi presso un ufficio. Gli è sufficiente utilizzare un qualsiasi smartphone o pc
- La Totale Indipendenza da specifici dispositivi hardware: non servono strumenti aggiuntivi, come tavolette grafometriche o smart card.

- l'assenza di costi aggiuntivi, a quelli del servizio, per ogni cittadino firmatario che ha CIE.

LA FEA con riconoscimento attraverso CIE, è quindi un vera e propria piattaforma abilitante che permette al cittadino di partecipare attivamente al processo di digitalizzazione del paese semplicemente utilizzando la propria Carta di Identità.

Il Processo

Il processo di attivazione, una tantum, della FEA con CIE prevede le seguenti macrofasi

- L'identità dell'utente è garantita da CIE, che ai fini dell'autenticazione non può che essere in corso di validità.
- Al primo Login effettuato con CIE, l'utente, che è quindi correttamente identificato, viene invitato a leggere e sottoscrivere l'Informativa sulle caratteristiche, i termini e le condizioni che regolano il servizio di FEA oltre agli aspetti di tutela dei dati personali. L'utente dopo averla letta, potrà firmare il documento per accettazione con la stessa soluzione, che solo in questo primo utilizzo avrà validità di firma elettronica semplice.
- I documenti acquisiti dovranno essere conservati a norma per la durata di 20 anni.
La piattaforma prevede la possibilità, opzionale, di dare al documento di accettazione una validità a lungo termine (LTV) apponendo una Marca temporale contestualmente all'apposizione del Sigillo Digitale Qualificato (QSEAL).

Eseguito il processo di attivazione, la soluzione di FEA con CIE potrà quindi espletare a pieno le sua potenzialità, che per il firmatario si risolvono con un processo semplice ed intuitivo:

- Il Firmatario riceve la notifica (SMS, Email o App) che gli è stato sottoposto un documento da Firmare.
- L'utente fa Login con CIE nella web application dove potrà visionare il documento.
- Solo dopo che l'utente ha scorso, quindi auspicabilmente letto e compreso tutto il documento, potrà decidere se firmare o meno ogni punto firma.
- L'utente potrà esprimere la sua volontà su ogni singolo "punto firma", posizionandosi su di esso ed attivando il bottone "Firma". Le informazioni relative all'identificazione iniziale del firmatario stesso, l'impronta del documento originale ed altri metadati, verranno inclusi in modalità Pades nel documento firmato attraverso l'apposizione di un Sigillo Digitale Qualificato
- Una volta espressa la volontà per ogni punto firma, all'utente viene mostrato un riepilogo dei singoli punti firma e richiesta una ulteriore autenticazione con CIE (NFC+PIN) la cui asserzione di

risposta conterrà l'impronta del documento e i dati identificativi del firmatario. Tali metadati vengono inclusi nel documento originale e il risultato firmato con il Sigillo Qualificato.

- Il documento firmato aperto con un qualsiasi lettore PDF potrà quindi essere verificato nella sua integrità e immutabilità e nella correttezza e coerenza del processo di firma, anche attraverso soggetti terzi
 - CA: L'integrità e l'immutabilità è garantita dalla catena di Sigilli Digitali Qualificati, rilasciati da un QTSP, apposti nel documento a seguito di ogni singola espressione di volontà (punto firma) ed a conclusione della sessione di ogni firmatario
 - CielD: l'identità del firmatario e l'originalità del documento iniziale sono invece garantiti dalle asserzioni avvenute CielD Server, che includono anche i certificati di cui è verificabile l'autenticità negli elenchi pubblici dei Certificatori previsto dal regolamento eIDAS.
- l'utente riceverà a questo punto una notifica sempre via SMS, Email e opzionalmente APP, con il riepilogo dell'operazione di firma appena effettuata, con la possibilità di rivedere, verificare e scaricare il documento firmato.

Firma Elettronica Avanzata basata su Self IDp

Oltre agli Identity Provider pubblici come SPID e CIE esiste anche la possibilità che il soggetto erogatore del servizio voglia o debba utilizzare un proprio Identity Provider, che ha popolato facendosi carico direttamente della fase di identificazione e della responsabilità che deriva dalla gestione dei dati personale dei suoi potenziali clienti/utenti.

Ovviamente questa soluzione per i soggetti erogatori è più onerosa in termini di responsabilità, ma è certamente di più rapida attuazione rispetto alle altre, perché non prevede alcuna interazione con la pubblica amministrazione.

Per garantire la massima solidità alla soluzione di Firma basata su di un Self IDP si è deciso di adottare lo stesso processo di Firma delle modalità basata su di SPID.

L'integrazione dei Self Identity Provider dei soggetti erogatori, si prevede obbligatoriamente di dotare lo stesso Identity Provider di una interfaccia SAML2, in modo che possa dialogare con il processo di firma elettronica avanzata così come fanno i Gestori di Identità SPID. Per implementare una login di livello 2, la firma con SPID prevede l'invio di un OTP al numero di cellulari o una email ai contatti dichiarati al momento dell'identificazione.

Quindi è dimostrato che il processo di firma elettronica avanzata basato sul riconoscimento attraverso un Self IDP è lo stesso dei processi basati sul riconoscimento con SPID, la differenza sostanziale è determinata dal fatto che in questo caso l'identificazione iniziale non è garantita da un soggetto qualificato e terzo, ma è garantita dal soggetto erogatore (Art.55, comma 2 lettera A, DPCM Febbraio 2013) che se ne assume la piena responsabilità.

Questo strumento garantisce dunque:

- Identificazione del firmatario garantita dall'Identity Provider del soggetto erogatore (Self IDP) che si assume quindi l'esclusiva responsabilità rispetto alla corretta identificazione e rispetto alla corretta gestione dei dati.
- Connessione univoca del firmatario alla firma ed al documento sottoscritto
- Controllo esclusivo del firmatario del sistema di generazione
- Le caratteristiche di qualità, sicurezza, integrità ed immodificabilità del documento sono verificabili in qualsiasi momento ed in maniera del tutto autonoma da chiunque sia in possesso del documento informatico firmato
- Il processo verifica obbligatoriamente l'effettiva presa visione del documento da firmare
- La totale indipendenza logistica: il firmatario può firmare i documenti quando vuole e ovunque si trovi, senza alcuna necessità di recarsi presso un ufficio. Gli è sufficiente essere connesso con un

qualsiasi smartphone o pc

- La Totale Indipendenza da specifici dispositivi hardware: non servono tavolette grafometriche, smart card,...
- l'assenza di costi aggiuntivi, a quelli del servizio, per il cittadino firmatario, che ha CIE.

LA FEA basata sul riconoscimento con Self IDP, è quindi una piattaforma che permette anche ai cittadini che non hanno né SPID né CIE di usufruire di comunque dei servizi online offerti da ogni soggetto erogatore.

Il Processo di FEA da Remoto con Self IDP

Il processo di attivazione, una tantum, della FEA con Self IDP prevede le seguenti macrofasi

- Nella fase di identificazione il soggetto erogatore provvederà ad acquisire una copia del documento di identità in corso di validità. In ogni caso il processo di Firma si avvierà solo per i firmatari di cui il soggetto erogatore ha effettuato correttamente il processo di identificazione.
- Al primo Login effettuato con OTP, che garantisce la corretta identificazione dell'utente, a questo verrà presentata, sotto forma di documento informatico, l'Informativa sulle caratteristiche, i termini e le condizioni che regolano il servizio di FEA oltre agli aspetti di tutela dei dati personali. L'utente dopo averla letta, per accettazione potrà firmare il documento con la stessa soluzione che solo in questo primo utilizzo avrà validità di firma elettronica semplice.
- i documenti acquisiti dovranno essere conservati a norma per la durata di 20 anni
La piattaforma prevede la possibilità, opzionale, di dare al documento di accettazione una validità a lungo termine (LTV) apponendo una Marca temporale contestualmente all'apposizione del Sigillo Digitale Qualificato (QSEAL).

Eseguito il processo di attivazione, la soluzione di FEA con OTP potrà quindi espletare a pieno le sua potenzialità, che per il firmatario si risolvono con un processo semplice ed intuitivo:

- Il Firmatario riceve la notifica (SMS, Email o App) che gli è stato sottoposto un documento da Firmare.
- L'utente fa login, inserendo correttamente le sue credenziali e subito dopo inserendo l'OTP che gli è arrivato via SMS o Email, completata l'autenticazione nella web application e potrà visionare il documento.
- Solo dopo che l'utente ha scorso, quindi auspicabilmente letto e compreso tutto il documento, potrà decidere per ogni punto firma se firmare o meno.

- L'utente potrà esprimere la sua volontà su ogni singolo "punto firma", posizionandosi su di esso ed attivando il bottone "Firma". Le informazioni relative all'identificazione iniziale del firmatario stesso, l'impronta del documento originale ed altri metadati, verranno inclusi in modalità Pades nel documento firmato attraverso l'apposizione di un Sigillo Digitale Qualificato
- Una volta espressa la volontà per ogni punto firma, all'utente viene mostrato un riepilogo dei singoli punti firma e richiesta una ulteriore autenticazione, di livello 2 con OTP, la cui asserzione di risposta conterrà l'impronta del documento e i dati identificativi del firmatario. Tali metadati vengono inclusi nel documento originale e il risultato firmato con il Sigillo Qualificato.
- Il documento firmato aperto con un qualsiasi lettore PDF potrà quindi essere verificato nella sua integrità e immodificabilità e nella correttezza e coerenza del processo di firma, anche attraverso soggetti terzi
 - CA: l'integrità e l'immodificabilità è garantita dalla catena di Sigilli Digitali Qualificati, rilasciati da un QTSP, apposti nel documento a seguito di ogni singola espressione di volontà (punto firma) ed a conclusione della sessione di ogni firmatario
 - Blockchain: ad ulteriore garanzia di tutto il processo, possono essere registrate in una catena blockchain le informazioni necessarie per garantire la correttezza del processo di firma (opzionale)
- l'utente riceverà a questo punto una notifica sempre via SMS, Email e opzionalmente APP, con il riepilogo dell'operazione di firma appena effettuata, con la possibilità di rivedere, verificare e scaricare il documento firmato.

Il Processo di FEA in Presenza con Self IDP

Il processo può essere declinato anche con qualche piccola variante in modo che questa possa consentire al firmatario di espletare il processo di FEA anche in presenza e non solo da Remoto.

Il processo di attivazione, una tantum, della FEA in Presenza con Self IDP prevede le seguenti macrofasi

- Nella fase di identificazione il soggetto erogatore provvederà ad acquisire una copia del documento di identità in corso di validità. In ogni caso il processo di Firma si avvierà solo per i firmatari di cui il soggetto erogatore ha effettuato correttamente il processo di identificazione.
- Al primo Login effettuato con OTP, che garantisce la corretta identificazione dell'utente, a questo verrà presentata, sotto forma di documento informatico, l'Informativa sulle caratteristiche, i termini e le condizioni che regolano il servizio di FEA oltre agli aspetti di tutela dei dati personali. L'utente dopo averla letta, per accettazione potrà firmare il documento con la stessa soluzione che solo in questo primo utilizzo avrà validità di firma elettronica semplice.
- i documenti acquisiti dovranno essere conservati a norma per la durata di 20 anni
La piattaforma prevede la possibilità, opzionale, di dare al documento di accettazione una validità a lungo termine (LTV) apponendo una Marca temporale contestualmente all'apposizione del Sigillo Digitale Qualificato (QSEAL).

Eseguito il processo di attivazione, la soluzione di FEA in Presenza con OTP potrà quindi espletare a pieno le sua potenzialità, che per il firmatario si risolvono con un processo semplice ed intuitivo:

- L'operatore fa Login sulla piattaforma Gestione attraverso una autenticazione a due fattori (2FA).
- Nel gestione espleta le pratiche e genera i documenti da sottoporre alla sottoscrizione del Firmatario
- L'operatore, attraverso un processo di Single Sign On passa alla piattaforma FirmoSemplice, impersonificando il Firmatario.
- L'Operatore ha la responsabilità di far visionare, leggere e comprendere il contenuto del documento al Firmatario,
- L'Operatore ha la responsabilità di raccogliere fedelmente la volontà del Firmatario rispetto alla sottoscrizione di ogni singolo punto firma, anche attraverso una specifica funzionalità, FirmoSemplice, registra le informazioni utili a dimostrare l'attività di raccolta della volontà.

- L'operatore conclusa la disamina dei singoli punti firma, procede attivando l'Invio di un OTP al firmatario.
- FermoSemplice provvederà verificare se il Firmatario ha già effettuato l'operazione di validazione e securizzazione del suo numero di cellulare e/o indirizzo email. Diversamente ingaggerà automaticamente il firmatario nel processo di verifica e securizzazione del suo numero di cellulare e/o indirizzo email.
- Verificata che il firmatario è in possesso di un numero di cellulare o di un indirizzo email verificato e securizzato, FermoSemplice provvederà ad inviare l'OTP, che non sarà in alcun modo intercettabile dal software gestionale e men che meno dall'operatore.
- Il Firmatario riceve (SMS, Email o App) una notifica che gli indica quale documento e quali punti firma sta sottoscrivendo, l'OTP per confermare la sua volontà di Firmare.
- Il Firmatario per sottoscrivere il documento e i suoi punti firma, comunica l'OTP ricevuto all'operatore, che lo digita in una apposita pagina/funzione di verifica proposta da FermoSemplice. Il sistema prima di tutto verifica automaticamente che l'OTP comunicato dal firmatario sia quello Corretto, e sia ancora valido temporalmente.
- Al buon esito della verifica dell'OTP. i metadati raccolti da FermoSemplice durante il processo di Firma, e utili a identificare il Documento, il Firmatario, le sue volontà di sottoscrizione e l'operatore, vengono inclusi nel documento originale e il risultato viene firmato con il Sigillo Qualificato.
- Il documento firmato aperto con un qualsiasi lettore PDF potrà quindi essere verificato nella sua integrità e immutabilità e nella correttezza e coerenza del processo di firma, anche attraverso soggetti terzi
 - CA: l'integrità e l'immutabilità è garantita dalla catena di Sigilli Digitali Qualificati, rilasciati da un QTSP, apposti nel documento a seguito di ogni singola espressione di volontà (punto firma) ed a conclusione della sessione di ogni firmatario
 - Blockchain: ad ulteriore garanzia di tutto il processo, possono essere registrate in una catena blockchain le informazioni necessarie per garantire la correttezza del processo di firma (opzionale)
- l'utente riceverà a questo punto una notifica sempre via SMS, Email e opzionalmente APP, con il riepilogo dell'operazione di firma appena effettuata, con la possibilità di rivedere, verificare e scaricare il documento firmato.

Il Processo di FEA in Grafometrica con Self IDP

L'adozione di Self Identity Provider, è propedeutica anche all'espletamento di processi di Firma elettronica Avanzata in modalità Grafometrica.

FirmoSemplice offre quindi anche una soluzione di Firma Elettronica Avanzata di tipo Grafometrico.

Nella fattispecie in FirmoSemplice si sono adottate Tavolette Grafiche Wacom, leader indiscusso di mercato, sdk Wacom, e software di gestione del processo di Firma realizzato da ARUBA.

Il processo di attivazione, una tantum, della FEA con Self IDP prevede le seguenti macrofasi

- Nella fase di identificazione il soggetto erogatore provvederà ad acquisire una copia del documento di identità in corso di validità. In ogni caso il processo di Firma si avvierà solo per i firmatari di cui il soggetto erogatore ha effettuato correttamente il processo di identificazione.
- A seguito della corretta identificazione dell'utente, a questo verrà presentata, sotto forma di documento informatico, l'Informativa sulle caratteristiche, i termini e le condizioni che regolano il servizio di FEA oltre agli aspetti di tutela dei dati personali. L'utente dopo averla letta, per accettazione potrà firmare il documento con la stessa soluzione che, solo in questo primo utilizzo avrà validità, di firma elettronica semplice.
- I documenti acquisiti dovranno essere conservati a norma per la durata di 20 anni

Eseguito il processo di attivazione, la soluzione di FEA Grafometrica potrà quindi espletare a pieno le sua potenzialità, che per il firmatario si risolvono con un processo semplice ed intuitivo:

- Il software permette l'avvio del processo di firma grafometrica solo dopo avere automaticamente verificato la disponibilità del documento di identità in corso di validità, e la corrispondenza del documento con il soggetto fisicamente presente in ufficio
- **Utilizzo del dispositivo di firma (Tavoletta Wacom)**
Il documento da firmare viene visualizzato su un **tablet grafometrico** certificato. Il firmatario appone la firma usando una penna elettronica.
- **Acquisizione dei dati biometrici:** Il sistema registra le caratteristiche biometriche univoche del gesto grafico. Questi dati non sono separabili dal documento firmato e sono crittografati e integrati nel PDF.
- Una volta firmato, il documento viene, in un modalità sicura viene trasmesso al software applicativo che ha avviato il processo di firma e per essere gestito nelle modalità opportune che possono prevedere, l'archiviazione documentale, la conservazione digitale ecc ecc.

- Il documento firmato aperto con un qualsiasi lettore PDF potrà quindi essere verificato nella sua integrità e immutabilità e nella correttezza e coerenza del processo di firma, anche attraverso soggetti terzi.
 - CA: l'integrità e l'immutabilità è garantita dalla catena di Sigilli Digitali Qualificati, rilasciati da un QTSP, apposti nel documento a seguito di ogni singola espressione di volontà (punto firma) ed a conclusione della sessione di ogni firmatario
- l'utente potrà ricevere una notifica sempre via SMS, Email e opzionalmente APP, con il riepilogo dell'operazione di firma appena effettuata, con la possibilità di rivedere, verificare e scaricare il documento firmato.

Obblighi e Solidità del processo

Tutte le tipologie di FEA (basate su SPID, CIE, Self IDP) di FirmoSemplice sono conformi al regolamento europeo eIDAS e alla normativa italiana in materia di FEA. Quello che cambia è il livello di solidità del processo, che raggiunge i suoi massimi livelli con SPID e CIE, cioè le due soluzioni dove l'identificazione dei firmatari è a carico di soggetti pubblici qualificati.

Nella Firma basata sul Self IDP è previsto che in fase di identificazione, soggetto erogatore, che è direttamente responsabile, debba necessariamente assicurarsi che si proceda alla scrupolosa ed attenta associazione univoca del soggetto identificato, con un suo documento di identità in corso di validità, con il suo numero di cellulare ed il suo indirizzo email. L'acquisizione del documento di identità è obbligatoria per dimostrare l'avvenuta identificazione da parte del soggetto erogatore. Il numero di cellulare e l'indirizzo email sono molto importanti perché saranno utilizzate per inviare al firmatario le notifiche relative ai documenti che sono da sottoscrivere e soprattutto saranno i soli ed esclusivi contatti a cui sarà inviato l'OTP per effettuare l'autenticazione di Livello 2 nei casi di FEA non Grafometrica: in questo modo il Firmatario ad ogni login dimostra di conoscere le credenziali che gli sono state assegnate al momento dell'identificazione e di avere il controllo sui canali di comunicazione dichiarati sempre al momento dell'identificazione.

Per tutte le FEA in caso di assenza di un documento in corso di validità e, nel caso delle FEA non Grafometriche, di almeno un canale di contatto valido, fra numero di cellulare e indirizzo email, non sarà possibile avviare il processo di firma elettronica avanzata. Questo processo rigoroso rende adeguatamente solida anche la firma basata sul Self IDP.

Gli stessi controlli sono attivi anche in quando si effettua il riconoscimento con SPID e CIE, ma è ovvio che in questi due casi sono superati dal semplice fatto di utilizzare SPID e CIE, che garantiscono il massimo della sicurezza. L'Identità digitale SPID infatti può essere utilizzata solo in presenza di un documento di identità in corso di validità. Nel momento in cui il documento di identità scade, l'IdP impedisce il buon esito della Login. Mentre utilizzando CIE è ovvio che ad ogni Login il sistema è in grado di verificare la validità del documento di identità stesso.

Come già descritto nel dettaglio di ogni processo di FEA offerta da FirmoSemplice, al primo accesso all'utente verrà presentato il documento che lo informa dei termini, delle condizioni e delle eventuali limitazioni relative all'utilizzo del servizio FEA. L'attivazione del servizio di FEA è

subordinato all'accettazione delle condizioni del servizio. Il documento di accettazione firmato dall'utente è poi, obbligatoriamente, il primo documento che la piattaforma FirmoSemplice trasferisce al soggetto erogatore. Eventuali altri documenti potranno essere acquisiti dal soggetto erogatore solo successivamente alla presa in carico del documento di accettazione.

Acquisiti il documento di Identità ed il documento di accettazione sarà poi cura e responsabilità del soggetto erogatore provvedere all'invio di tali documenti al sistema di conservazione, dove dovranno rimanere disponibili per la durata di anni 20, garantendo integrità, leggibilità e autenticità.

L'utente potrà gratuitamente e liberamente richiedere copia del documento di accettazione e dei documenti da lui firmati. Tali richieste potranno avvenire attraverso delle specifiche funzionalità rese note dal soggetto erogatore attraverso la pubblicazione nel suo sito. Di solito il soggetto erogatore, preferisce condividere documenti con i propri clienti/utenti utilizzando strumenti propri come sistema documentale, intranet, App che rientrano in una strategia di collaborazione e fidelizzazione più ampia della firma. Per questo la piattaforma FirmoSemplice, salvo specifiche richieste, non conserva copia dei documenti che hanno concluso il loro iter di firma.

Le eventuali richieste di revoca dal servizio di FEA sono invece gestite da una specifica funzione di FirmoSemplice, che permette all'utente di procedere liberamente ed in piena autonomia.

Inoltre sarà sempre responsabilità del soggetto erogatore quella di pubblicare nel proprio sito le caratteristiche del processo e le caratteristiche tecnologiche dei processi di FEA che FirmoSemplice mette a disposizione e di cui fornisce adeguata documentazione.