

NOTA INFORMATIVA SULLA FIRMA ELETTRONICA AVANZATA DELLA MODULISTICA E DELEGA DIGITALE

Il documento è predisposto ai sensi dell'articolo 57 comma 1 lettera d, g e comma 3 del DPCM 22.2.2013, riguardante la firma elettronica avanzata.

INFORMAZIONI GENERALI

Le società:

CAAF CGIL Lombardia Srl srl, CAAF CGIL Piemonte e VDA srl, CAAF Nordest srl, CAAF CGIL Puglia srl, CAAF CGIL Campania srl, CAAF CGIL Sardegna srl, CAAF CGIL Calabria srl, CAAF CGIL Sicilia srl, (di seguito Caaf Cgil) hanno introdotto un'innovativa soluzione informatica che consente di firmare i documenti in formato elettronico, eliminando così la stampa della carta. Tale soluzione, di seguito denominata "firma elettronica", si inquadra nel più ampio progetto di dematerializzazione dei processi contabili e gestionali con la progressiva sostituzione della documentazione cartacea a favore della documentazione digitale.

La presente nota informativa, contenente le informazioni relative alle caratteristiche del servizio di Firma Elettronica ed alle tecnologie su cui essa si basa, è pubblicata nella home page sul www.caaf.it/InformativaFEA.pdf, come richiesto dalla normativa DPCM 22 febbraio 2013 che stabilisce che gli obblighi di pubblicazione previsti dall'Art. 57 sono a carico dei soggetti che *erogano* soluzioni di firma elettronica avanzata (FEA), identificati come quelli di cui all'Art. 55, comma 2, lettera a).

Tale informativa, pertanto, risulta sempre disponibile per i propri clienti e gli utenti in generale.

NATURA GIURIDICA DELLA FIRMA ELETTRONICA AVANZATA

Secondo quanto disciplinato dal CAD in materia di Firma Elettronica Avanzata, la sottoscrizione dei documenti avviene mediante l'utilizzo della Firma Elettronica Avanzata grafometrica per la sottoscrizione della modulistica (in formato PDF) e della Firma Elettronica Avanzata OTP per i documenti informatici (in formato XML, ZIP, JSON) entrambe le modalità di Firma Elettronica possiedono i requisiti informatici e giuridici che consentono per legge di qualificarla come "Firma Elettronica Avanzata" secondo:

- Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 (in seguito DPCM)
- Decreto Legislativo 7 marzo 2005, n. 82 e ss.mm
- Regolamento (UE) n. 910/2014 eIDAS (Electronic Identification, Authentication and Trust Services)
- Regolamento (UE) n. 1183/2024 eIDAS2 (Electronic Identification, Authentication and Trust Services)
- L'art. 13 del D.Lgs. 196/2003 (il Codice in materia di protezione dei dati personali)
- GDPR (Regolamento UE 2016/679) applicazione effettiva del 25 maggio 2018
- Provvedimento n.513 prescrittivo in tema di biometria del 12 novembre 2014 Gazzetta Ufficiale n.280 del 2 dicembre 2014

Il processo di Firma Elettronica Avanzata (FEA) è stata ideato e progettato da **Sintel srl**, qualificabile come soggetto che realizza soluzioni di FEA ai sensi dell'Art. 55, comma 2, lettera b) del DPCM 22 febbraio 2013.

Sintel srl ha curato l'integrazione architettuale dell'intero sistema, avvalendosi di partner tecnologici di riferimento: **BlueNext srl** per la componente di firma grafometrica (FEA-G) e **Tinexta Infocert SPA** quale Certification Authority per la componente di firma tramite OTP (FEA-OTP). Tale realizzazione è destinata all'offerta di soluzioni connesse ad attività relative ai Caaf Cgil come, ad esempio, i processi di Delega Digitale verso Agenzia delle Entrate e verso INPS.

Per adempiere ai requisiti previsti dall'Art. 58 del DPCM, il soggetto realizzatore (Sintel srl) risulta in possesso delle certificazioni obbligatorie: **Certificazione ISO/IEC 27001** (relativa al proprio sistema di gestione per la sicurezza delle informazioni) e **Certificazione ISO 9001** (relativa al sistema di qualità).

L'infrastruttura e il processo di firma si avvale di certificati emessi dalle Certification Authority Tinexta-Infocert SpA distinti per funzione:

1. Certificati non qualificati: Sono intestati univocamente al soggetto firmatario (delegante/contribuente) e utilizzati per l'apposizione della **firma CADES sulla Delega Digitale (XML)**, nell'ambito del processo di FEA-OTP.

2. Certificati qualificati: Dove richiesto, per l'attestazione del documento, si ricorre a una **firma Elettronica Qualificata** intestata al Caaf Cgil (che è il soggetto erogatore, Art. 55, comma 2, lettera a)). In particolare, poichè il contribuente utilizza una FEA basata su certificato non qualificato, la comunicazione XML all'Agenzia delle Entrate o all'INPS deve essere finalizzata, secondo i provvedimenti, con FEQ dell'intermediario delegato, che attesta così il conferimento della Delega, ottenendo così una busta crittografica che contiene un'ulteriore busta crittografica secondo il formato CADES. La busta crittografica più esterna è dunque quella prodotta e firmata dall'intermediario delegato Caaf Cgil.

Oltre a ciò vengono utilizzati Certificati Qualificati anche per la crittografia e l'immutabilità delle informazioni biometriche acquisite durante la sottoscrizione grafometrica (rilasciati da e In.Te.S.A. SpA), essenziali per assicurare l'integrità del documento FEA ai sensi dell'Art. 56 del DPCM 22 febbraio 2013.

I DOCUMENTI CHE SI POSSONO FIRMARE CON LA FIRMA ELETTRONICA AVANZATA GRAFOMETRICA

La Firma Elettronica Avanzata Grafometrica (di seguito FEA-G) consente di firmare la maggior parte dei documenti di contrattualistica e documentazione e modulistica afferente prodotti e servizi erogati allo sportello offerti nel tempo. (Formati PAdES)

I DOCUMENTI CHE SI POSSONO FIRMARE CON LA FIRMA ELETTRONICA AVANZATA - OTP

La Firma Elettronica Avanzata OTP (di seguito FEA-OTP) consente di firmare le Deleghe Uniche (INPS e Agenzia Delle Entrate) in Formato Digitale (XML, JSON). (Formati CADES) La stessa tipologia di firma è anche utilizzata per la sottoscrizione di modulistica da remoto (Formati PAdES).

IDENTIFICAZIONE DEL FIRMATARIO

Il Caaf Cgil, in qualità di Soggetto che eroga soluzioni di Firma Elettronica Avanzata (FEA) – Art. 55, comma 2, lettera a), del DPCM 22 febbraio 2013 – ha l'obbligo di garantire **l'identificazione certa del firmatario** (Art. 56,

comma 1, lettera a)). L'identificazione e l'adesione al servizio di FEA avvengono rispettando le prescrizioni di cui all'Art. 57, comma 1, lettera a):

L'identificazione in presenza ("De Visu") è eseguita richiedendo un valido documento di identità, di cui il Caaf Cgil acquisisce copia digitale. L'attivazione del servizio è subordinata alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio FEA da parte dell'utente.

Tale metodo di identificazione soddisfa il requisito di cui all'Art. 26, lettera b) del Regolamento (UE) n. 910/2014 eIDAS così come modificato dal Regolamento (UE) 2024/1183 eIDAS2, che impongono che la firma elettronica avanzata sia idonea a identificare il firmatario.

Ai sensi dell'Art. 57, comma 1, lettera b) del DPCM 22 febbraio 2013, il Caaf Cgil garantisce disponibilità, integrità, leggibilità e autenticità, con conservazione a norma per 20 (venti) anni:

- la copia digitale del documento di riconoscimento.
- la dichiarazione di accettazione delle condizioni del servizio sottoscritto con il contratto FEA
- log di sessione del processo di firma

CONNESSIONE UNIVOCA AL FIRMATARIO

Il Caaf Cgil, in qualità di Soggetto che eroga soluzioni di Firma Elettronica Avanzata (FEA) – Art. 55, comma 2, lettera a), del DPCM 22 febbraio 2013 – ha l'obbligo di garantire la **connessione univoca con il firmatario** (Art. 56, comma 1, lettera b) e lettera h)).

Relativamente all'uso della FEA-G, la soluzione, oltre a rilevare l'immagine della firma, acquisisce anche le caratteristiche dinamiche e biometriche della sottoscrizione autografa che il firmatario traccia direttamente con una penna elettronica sul dispositivo dedicato, ossia il *signature pad* che il Caaf Cgil mette a disposizione a uso esclusivo del firmatario. Le informazioni raccolte includono l'andamento temporale dei movimenti – quindi ritmo, velocità e pressione esercitata – registrati durante l'esecuzione della firma. Tali dati biometrici sono propri e distintivi di ogni individuo.

L'associazione univoca tra firmatario e documento è garantita sia dalla firma resa in presenza dell'operatore del Caaf Cgil, dopo l'identificazione del soggetto, sia dalla rilevazione tramite signature pad di dati comportamentali (biometrici) che possono essere attribuiti in modo esclusivo al firmatario e che vengono legati in modo permanente al documento informatico sottoscritto.

Relativamente all'uso della FEA-OTP, l'associazione univoca tra la firma e il firmatario è garantita tramite la correlazione, all'interno della procedura software, tra l'Utente firmatario - previamente identificato da un operatore Caaf Cgil (vedi sezione "Identificazione del firmatario") - e il processo di firma, che prevede l'invio di un OTP al numero di cellulare certificato e nella disponibilità esclusiva del firmatario. L'OTP, valido una sola volta e per un tempo limitato, consente di confermare che l'operazione di firma sia eseguita dal soggetto correttamente identificato, assicurando la connessione certa tra firmatario e sottoscrizione. L'utilizzo di tale codice, noto unicamente al firmatario, permette di effettuare l'autenticazione necessaria per l'uso del certificato di firma a lui univocamente intestato.

DOPPIA CATENA DI FIRMA

È inoltre da considerare che il processo di sottoscrizione della Delega Digitale prevede una doppia catena di firma che rafforza ulteriormente la connessione univoca al firmatario: la sottoscrizione avviene contestualmente sulla Delega in formato PDF (FEA-G, formato PAdES quale formato di cortesia) e sulla corrispondente Delega Digitale in formato XML (FEA-OTP, formato CAdES). I due documenti sono legati in modo indissolubile tramite l'hash del documento PDF PAdES sottoscritto, il quale viene innestato all'interno dell'XML prima che quest'ultimo venga a sua volta sottoscritto in CAdES. Tale meccanismo garantisce che le due sottoscrizioni costituiscano un unico evento di firma correlato, non separabile, assicurando la piena tracciabilità e unicità della volontà espressa dal firmatario in entrambi i formati.

CONTROLLO ESCLUSIVO DEL FIRMATARIO DEL SISTEMA DI GENERAZIONE DELLA FEA

Il Caaf Cgil, in qualità di Soggetto che eroga soluzioni di Firma Elettronica Avanzata (FEA) – Art. 55, comma 2, lettera a), del DPCM 22 febbraio 2013 – ha l'obbligo di garantire **il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima** (Art. 56, comma 1, lettera c)).

Relativamente all'uso della FEA-G, il display del signature pad mostra al firmatario la modulistica da sottoscrivere, permettendogli di verificare direttamente i propri dati e il contenuto oggetto di firma. Durante la procedura, il sistema assiste l'utente guidandolo passo dopo passo. Nel momento in cui il firmatario traccia la propria firma con la penna elettronica, l'immagine viene visualizzata in tempo reale sul signature pad. Sono inoltre disponibili funzioni dedicate che consentono di confermare la firma oppure di annullarla e ripeterla in caso di errore.

Tutte le comunicazioni tra il signature pad e il sistema di generazione della firma sono trasmesse in forma cifrata. Anche i dati grafometrici raccolti durante la sottoscrizione vengono automaticamente criptati mediante una chiave crittografica non disponibile al Caaf Cgil, ma detenuta esclusivamente dalla Certification Authority (In.Te.S.A. SpA). Ciò garantisce non solo l'immodificabilità dei dati, ma soprattutto la loro riservatezza e la totale impossibilità di accesso alle informazioni biometriche. La decifratura è, infatti, consentita esclusivamente alla CA per finalità probatorie in caso di contenzioso legale e solo previa specifica autorizzazione dell'autorità competente.

Relativamente all'uso della FEA-OTP, il firmatario impiega un proprio dispositivo personale (tipicamente uno smartphone), di cui ha piena ed esclusiva disponibilità, per consultare e verificare integralmente i documenti da sottoscrivere o già sottoscritti. La firma viene effettuata mediante l'inserimento dell'OTP ricevuto sul dispositivo personale: l'invio di questo codice al sistema di firma autentica il firmatario e autorizza l'uso esclusivo del certificato di firma a lui intestato.

IMMODIFICABILITA' DEI DOCUMENTI SOTTOSCRITTI

Il Caaf Cgil, in qualità di Soggetto che eroga soluzioni di Firma Elettronica Avanzata (FEA) – Art. 55, comma 2, lettera a), del DPCM 22 febbraio 2013 – ha l'obbligo di garantire che **il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;** (Art. 56, comma 1, lettera d)).

Le soluzioni di FEA utilizzate nei processi di sottoscrizione relativi alle pratiche in convenzione con il Caaf Cgil si basano sulle modalità FEA-G e FEA-OTP, che prevedono rispettivamente l'apposizione di firme nei formati PAdES e CAdES. L'immodificabilità dei documenti firmati è garantita dagli standard stessi, come segue:

Formato PAdES (PDF Advanced Electronic Signatures): Specifico per i documenti PDF, la modulistica mantiene l'estensione .pdf e può essere aperta e verificata con comuni visualizzatori PDF. La firma è integrata direttamente nel documento, che diventa immodificabile senza invalidare la sottoscrizione. La validità e l'integrità sono assicurate dalla crittografia applicata alla firma, che sigilla digitalmente il contenuto del PDF.

Formato CAdES (CMS Advanced Electronic Signatures): Applicabile a file di qualsiasi estensione o tipologia, genera un contenitore con estensione .p7m, che include sia il file originale sia la firma digitale. La firma rende il documento immodificabile: qualsiasi alterazione ne invalida la validità. Per la visualizzazione e la verifica dei documenti firmati in formato CAdES è necessario utilizzare software dedicati, disponibili sul sito AGID al seguente link: <https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/software-verifica>

Il file originale non viene alterato nel suo formato nativo, ma risulta "incapsulato" all'interno della busta digitale firmata.

POSSIBILITÀ PER IL FIRMATARIO DI OTTENERE EVIDENZA DI QUANTO SOTTOSCRITTO

Il Caaf Cgil, in qualità di Soggetto che eroga soluzioni di Firma Elettronica Avanzata (FEA) – Art. 55, comma 2, lettera a), del DPCM 22 febbraio 2013 – ha l'obbligo di **garantire la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto**; (Art. 56, comma 1, lettera e)).

Nel caso di utilizzo della FEA-G nella quale l'apposizione della firma avviene tramite *signature pad* - il sistema consente al firmatario di visualizzare in tempo reale sul display del dispositivo la clausola o il documento oggetto di sottoscrizione, verificandone direttamente contenuto, dati riportati e correttezza prima dell'apposizione della firma. Su richiesta, il firmatario, può inoltre richiedere copia di cortesia rispetto a tutto il fascicolo firmato e sottoscritto, oppure (al fine di mantenere un processo elettronico e di totale dematerializzazione obiettivo promosso dai Caaf Cgil), il Caaf rende disponibili tali documenti anche attraverso l'APP DigitaCGIL, che, gratuitamente, consente la consultazione, il download e l'archiviazione personale delle copie firmate e di tutta la modulistica, conservata a norma per il contribuente senza costi aggiuntivi. In questo modo il firmatario può recuperare in ogni momento l'evidenza completa delle proprie sottoscrizioni, assicurando la piena conformità agli obblighi normativi previsti nonché all'impegno verso la digitalizzazione per ridurre l'impatto ambientale.

Nel caso di sottoscrizione delle Deleghe tramite FEA-OTP, il processo resta invariato: l'apposizione della firma avviene sulla corrispondente Delega Digitale in formato XML (CAdES), che al suo interno contiene l'hash del documento firmato in PAdES, garantendo così l'unicità dell'evento all'interno della procedura informatica di sottoscrizione e abbinamento dei due formati ottenuti. La possibilità per il firmatario di leggere e verificare quanto sottoscritto rimane assicurata secondo le modalità descritte in precedenza.

INDIVIDUAZIONE DEL SOGGETTO EROGATORE DELLA SOLUZIONE FEA

Nel modulo di adesione al servizio di FEA viene espressamente indicato, con tutti i suoi dati identificativi, chi è il soggetto che eroga la soluzione di FEA ai sensi dell'art 55, comma 2, lett. a), del DPCM, e così garantendo l'obbligo rispetto all' Art. 56, comma 1, lettera f)).

L'utilizzo della FEA avviene solo dopo che il firmatario abbia accettato, con apposito contratto, di utilizzare questo sistema di firma e tutte le modalità descritte. Il firmatario ha il diritto di chiedere, contestualmente o successivamente al momento della firma e gratuitamente, una copia stampata della sopracitata dichiarazione di accettazione da lui firmata. Il contratto viene comunque reso a disposizione del firmatario con suo accesso esclusivo all'APP DIGITACGIL.

ASSENZA NELL'OGGETTO DELLA SOTTOSCRIZIONE DI QUALUNQUE ELEMENTO IDONEO A MODIFICARNE GLI ATTI, I FATTI E I DATI IN ESSO RAPPRESENTATI

Al momento della sottoscrizione, il contenuto del documento viene sottoposto a crittografia e la firma elettronica apposta, sigillando il documento in maniera univoca. Questa operazione lega indissolubilmente il contenuto al firmatario e al documento stesso, garantendo l'immutabilità dei dati, degli atti e di tutto ciò che il documento rappresenta. Per ogni documento viene calcolato un hash crittografico, ovvero una "impronta digitale" univoca dei contenuti. L'hash è incluso nella firma elettronica e serve come riferimento per verificare l'integrità del documento in qualsiasi momento successivo.

Qualsiasi modifica, alterazione o manomissione dei contenuti genera una variazione nell'hash calcolato. Durante la verifica della firma elettronica (sia esso PAdES che CAdES), un hash non corrispondente segnala immediatamente che il documento è stato alterato, invalidando così la sottoscrizione e garantendo la certezza dell'integrità originaria del contenuto.

In questo modo, il sistema assicura garanzia di integrità e che nessun elemento può modificarne il valore dell'atto, dei fatti e dei dati in esso rappresentati, in pieno rispetto dell'obbligo di cui Art. 56, comma 1, lettera g) del DCPM).

REVOCA DELL'USO DELLA FEA E DELLE RELATIVA MODALITA' SOTTOSCRITTE

In qualsiasi momento il firmatario può revocare il consenso all'utilizzo della FEA mediante richiesta scritta. In questo caso le firme dovranno essere acquisite su supporto cartaceo, tradizionale con firme autografe. Per motivi tecnici, di sicurezza o di forza maggiore si può in qualsiasi momento sospendere o interrompere la possibilità per il firmatario di utilizzare la FEA, e procedere con i metodi tradizionali di firma.

CERTIFICAZIONE ISO/IEC 27001 E ISO 9001 DEL PRODUTTORE DELLA TECNOLOGIA FEA

Sintel Srl è la società che progetta, sviluppa e integra la soluzione di Firma Elettronica Avanzata all'interno dei gestionali software dei CAAF CGIL, qualificabile come soggetto che realizza soluzioni di FEA ai sensi dell'Art. 55, comma 2, lettera b) del DPCM 22 febbraio 2013. La soluzione è realizzata avvalendosi delle tecnologie e dei servizi offerti da partner tecnologici e Certification Authority qualificate e autorizzate.

Sintel Srl è in possesso della certificazione di conformità **ISO/IEC 27001:2022** e **ISO 9001** del proprio sistema di gestione per la sicurezza delle informazioni, con ambito *"design, development, installation and maintenance of informatic systems and applications"*. È inoltre soggetto essenziale ai sensi della Direttiva **NIS2**, disponendo di tutte le misure di compliance richieste per garantire riservatezza, integrità e disponibilità dei servizi erogati.

Le certificazioni sono consultabili al seguente indirizzo: <https://www.sintel.net/pagina-certificazioni/>

INFORMAZIONI RIGUARDANTI LA POLIZZA ASSICURATIVA

I soggetti Erogatori dichiarano e garantiscono di aver stipulato una polizza assicurativa per la responsabilità civile, rilasciata da una compagnia autorizzata a operare nel settore dei rischi industriali, con un massimale non inferiore a cinquecentomila euro (500.000€). Tale polizza ha lo scopo di tutelare gli Utenti (firmatari della FEA) e i terzi da eventuali danni derivanti da soluzioni tecniche inadeguate adottate per l'erogazione del servizio di FEA, in conformità a quanto previsto dall'art. 57, comma 2, del DPCM 22 febbraio 2013.

L'INFORMATIVA AI SENSI DELLE NORME IN MATERIA DI PRIVACY

A integrazione dell'informativa fornita al momento del conferimento del mandato, si informa circa le modalità di trattamento dei suoi dati connessi all'utilizzo della FEA.

Al momento dell'utilizzo della FEA-G verrà richiesto di apporre alcune firme su un apposito dispositivo in grado di acquisire, oltre all'immagine della sottoscrizione, anche una serie di informazioni relative alle caratteristiche comportamentali a contenuto biometrico. I dati grafometrici verranno criptati e racchiusi elettronicamente all'interno del documento informatico cui si riferiscono, al solo fine di garantire una connessione univoca tra la firma apposta in forma elettronica sul documento ed il suo autore, assicurando così l'integrità e l'immodificabilità del documento sottoscritto.

In nessun caso saranno acquisite informazioni relative allo stato di salute degli interessati, ed i dati grafometrici non saranno accessibili "in chiaro" né al titolare né a qualsiasi altro soggetto responsabile o incaricato del trattamento, se non su espressa richiesta dell'Autorità Giudiziaria per finalità probatorie. Le chiavi private di accesso ai dati grafometrici saranno conservate da uno o più soggetti terzi appositamente nominati Responsabili che ne permetteranno l'utilizzo esclusivamente nei casi previsti dalla legge e su richiesta delle Autorità competenti.

Il conferimento dei dati per tale finalità (utilizzo firma grafometrica) ed il mancato consenso comporterà l'impossibilità di utilizzare la firma grafometrica. Il mancato rilascio dei dati o del consenso da parte del firmatario non comporta pregiudizio alcuno rispetto la finalità principale di esecuzione dei servizi. La sottoscrizione dei documenti relativi ai servizi forniti continuerà quindi ad essere effettuata su supporto cartaceo. Nessuno dei dati grafometrici sopra menzionati sarà oggetto di diffusione.

Al firmatario competono i diritti di cui all'art. 7 del Codice Privacy, tra i quali quello di ottenere l'accesso, la cancellazione, l'aggiornamento, la rettifica e l'integrazione dei dati, nonché di opporsi, per motivi legittimi, al trattamento degli stessi. Le richieste possono essere presentate per iscritto. In ogni momento il firmatario può revocare il consenso all'utilizzo della firma grafometrica mediante richiesta scritta inviata a mezzo PEC a icaaf@legalmail.it o a un qualsiasi sportello del Caaf Cgil.

L'eventuale revoca del consenso al trattamento dei dati necessari per l'utilizzo della firma grafometrica determinerà la disattivazione del servizio stesso, ma non l'eliminazione dei documenti precedentemente sottoscritti.

I dati grafometrici raccolti, cifrati e incorporati all'interno del documento informatico, saranno conservati, nei limiti delle finalità indicate, per il periodo di tempo stabilito dalle disposizioni legislative vigenti per la conservazione dell'atto o del documento cui la firma si riferisce, fatta salva l'esigenza di una loro ulteriore conservazione in ragione di eventuali contestazioni in sede giudiziaria.

Seguendo l'ulteriore integrazione del **Provvedimento del Garante Privacy n.513 del 12 novembre 2014** che stabilisce specifici adempimenti in materia di sottoscrizione dei documenti informatici tramite firma grafometrica. In particolare, la soluzione adottata di **FEA-G** garantisce:

- **Cancellazione dei dati biometrici grezzi e dei campioni biometrici** immediatamente dopo la sottoscrizione del documento;
- **Trasmissione sicura dei dati biometrici** tra i sistemi di acquisizione hardware, le postazioni informatiche e i server, tramite canali protetti con tecniche crittografiche;
- **Protezione dei sistemi informatici** contro malware, con l'adozione di firewall e funzionalità di *remote wiping* disponibili in caso di smarrimento o sottrazione dei dispositivi;
- **Conservazione dei dati biometrici e grafometrici** esclusivamente all'interno dei documenti informatici in forma cifrata mediante crittografia a chiave pubblica.

DESCRIZIONE DEI DISPOSITIVI DI FIRMA

IL DISPOSITIVO DI ACQUISIZIONE DELLA FIRMA FEA-G

Il componente hardware di acquisizione della firma è un dispositivo progettato per rilevare e registrare con precisione le caratteristiche biometriche specifiche del firmatario, quali posizione, tempo, velocità, pressione e accelerazione.

Si tratta di un tablet dedicato, esterno e collegato esclusivamente al PC, privo di sistema operativo. Il dispositivo è dotato di un display e di una penna apposita, tramite i quali il firmatario può:

- visualizzare e scorrere il documento informatico;
- apporre la firma;
- cancellare la firma per ripeterla;
- annullare l'operazione di sottoscrizione del documento.

Il tablet utilizza una tecnologia basata sulla risonanza elettromagnetica per rilevare i dati biometrici forniti dalla penna. Per motivi di sicurezza, il dispositivo non è collegato alla rete e può essere accessibile solo dall'applicazione gestionale dedicata. Le informazioni trattate non possono essere violate e tutti i canali di comunicazione sono completamente crittografati.

Grazie alle caratteristiche del tablet e alle modalità di utilizzo, il tratto grafico della firma viene visualizzato in tempo reale sul display, offrendo al firmatario un'esperienza equivalente alla firma autografa e consentendo un gesto di sottoscrizione del tutto naturale.

IL DISPOSITIVO DI ACQUISIZIONE DELLA FIRMA FEA-OTP

Nel caso della Firma Elettronica Avanzata tramite OTP, il firmatario utilizza un dispositivo personale, tipicamente uno smartphone, di cui ha piena ed esclusiva disponibilità. Prima di poter procedere alla firma, il numero di telefono associato al dispositivo viene certificato, verificando che il numero sia di suo possesso esclusivo utilizzo.

Il dispositivo consente al firmatario di visualizzare integralmente i documenti da sottoscrivere e di ricevere l'OTP necessario per completare la procedura di firma. L'inserimento dell'OTP nel work flow di firma autentica il firmatario e autorizza l'uso esclusivo del certificato digitale a lui intestato.

La comunicazione tra il dispositivo personale e il processo di firma avviene esclusivamente tramite canali criptati, garantendo la sicurezza dei dati trasmessi. In questo modo, il firmatario può verificare e confermare personalmente i documenti, assicurando l'unicità e la validità della sottoscrizione digitale, in piena conformità agli standard di sicurezza previsti per la FEA.

IL SISTEMA INFORMATICO

Il sistema di firma grafometrica garantisce la totale protezione dei dati biometrici o personali acquisiti durante ogni singola firma, in modo da rendere riconducibile univocamente la firma apposta sul dispositivo al firmatario (processo di document binding). Il trasferimento dei dati particolari biometrici dal tablet di firma al software di gestione del documento avviene in modalità protetta, utilizzando un algoritmo AES a chiave simmetrica scambiata attraverso l'algoritmo a doppia chiave DIFFIE-HELLMAN.

I dati particolari biometrici acquisiti dal tablet, dopo ogni firma, vengono associati in modo univoco e indissolubile all'hash del documento pdf sottoscritto, quindi cifrati con algoritmo RSA 2048 bit tramite la chiave pubblica di un certificato digitale. Ogni singola firma genera un pacchetto cifrato (dati biometrici + hash del documento), che viene inserito all'interno del documento pdf insieme alla generazione di una firma PadES. Ogni firma PadES viene effettuata con la cifratura dell'hash del documento (realizzato con algoritmo SHA256) mediante l'utilizzo della chiave privata di un ulteriore certificato digitale.

Questo processo garantisce che i dati biometrici non vengano in nessun modo memorizzati in chiaro sul tablet e sull'applicazione di firma e che ogni firma grafometrica non possa in alcun modo essere associata ad altri documenti. Il documento informatico così ottenuto soddisfa i requisiti normativi legati all'autoconsistenza, immodificabilità e leggibilità nel tempo dello stesso.