Informativa sul sistema di Firma Elettronica Avanzata

(ai sensi del DPCM 22/02/2013 - Art. 57, comma 1)

A integrazione di quanto riportato nell'Atto di informativa già fornito, **Confidi Systema!,** in qualità di Titolare del trattamento, fornisce all'interessato alcune informazioni circa le caratteristiche del servizio di Firma Elettronica Avanzata.

COS'È LA FIRMA ELETTRONICA AVANZATA

La Firma Elettronica Avanzata (o FEA) è un particolare tipo di firma elettronica che soddisfa i seguenti requisiti:

a. è connessa unicamente al firmatario;
b. è idonea a identificare il firmatario;
c. è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
d. è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Utilizzando la firma elettronica avanzata, con le modalità meglio specificate nei paragrafi successivi, **Confidi Systema!** garantisce:

a) *l'identificazione del firmatario;*
b) la connessione univoca della firma al firmatario;
c) *il controllo esclusivo del firmatario sul sistema di generazione della firma;*
d) *l'immodificabilità del documento dopo l'apposizione della firma;*
e) *la possibilità per il firmatario di ottenere evidenza e copia di quanto sottoscritto;*
f) *la connessione unica della firma al documento sottoscritto*

In particolare, Confidi Systema! utilizza due tipologie di firma elettronica avanzata:

- Grafometrica (FG)
- La firma remota con One Time Password (OTP)

FG - La firma grafometrica è una tecnologia che consente l'apposizione di una firma autografa su un documento, attraverso l'uso di dispositivi elettronici - pc, tablet, smartphone - in grado di registrare le caratteristiche comportamentali del firmatario al momento della firma, quali ad esempio il ritmo, la pressione, la velocità, l'inclinazione, l'accelerazione e il movimento (i "dati grafometrici"). Previa identificazione del firmatario, con programmi tali da garantirne la sicurezza e la *privacy,* i dati grafometrici così acquisiti vengono criptati, racchiusi e sigillati elettronicamente all'interno del documento informatico a cui si riferiscono, al solo fine di garantire una connessione univoca tra la firma apposta in forma elettronica sul documento e il suo autore, assicurando così l'integrità e l'immodificabilità del documento sottoscritto.

OTP - La firma remota con OTP inviato via SMS è una tecnologia che consente la sottoscrizione di un documento PDF utilizzando un meccanismo di autenticazione forte del firmatario basato sull'invio di un codice casuale (One Time Password) al suo telefono cellulare personale.

Questa tecnologia consente la realizzazione di processi di firma elettronica avanzata in tutti quei casi in cui il firmatario è fisicamente distante dall'ente che propone la sottoscrizione del documento. Inoltre, al firmatario, è richiesto esclusivamente il possesso di strumenti elettronici standard (indirizzo email, browser web e telefono cellulare in grado di ricevere SMS).

IL PROCESSO DI FIRMA

Tecnicamente, l'apposizione di una firma elettronica avanzata su un documento PDF segue un processo, ripetuto per ogni singola firma, che prevede i seguenti passi operativi

FG

1. Viene calcolato l'hash del documento PDF prima della firma
2. Vengono catturati i dati biometrici
3. Viene elaborata un'immagine contenente lo specimen della firma
4. Lo hash e i dati biometrici vengono inseriti in un'unica struttura dati che viene immediatamente cifrata con un algoritmo di cifratura a chiave pubblica di lunghezza adeguata. Si ottiene così un "Encrypted Signature Data Container" (ESDC). L'ESDC ha il duplice scopo di proteggere il dato grafometrico e di legare indissolubilmente la firma al documento per cui essa è stata apposta.
5. L'ESDC viene incorporato nel documento PDF (in accordo con lo standard ISO 32000)
6. Nella posizione del punto firma, sulla pagina, viene inserita l'immagine con lo specimen della firma per un immediato riscontro in fase di lettura o stampa
7. Il documento PDF così ottenuto (cioè l'originale con incluso l'ESDC) viene firmato in modalità PAdES con un certificato di firma tecnica. Questa firma PAdES ha il solo scopo di garantire la non modificabilità del documento dopo l'apposizione della firma grafometrica. Quest'ultima firma non ha, quindi, valore ai fini della sottoscrizione del documento, ma è funzionale esclusivamente alla sicurezza del processo di firma.
8. Può essere effettuata una marcatura temporale del documento. Lo scopo della marcatura temporale effettuata in questo punto è quello di attestare in modo certo la data e l'ora in cui è stata apposta la firma.

Cos'è l'ESDC?

L'Encrypted Signature Data Container è una struttura dati che lega indissolubilmente il dato biometrico catturato all'impronta (hash) del documento per cui quel dato grafometrico è stato rilevato.

Attraverso la cifratura dell'ESDC, il sistema garantisce che il dato biometrico:

1. Resti riservato
2. Non possa essere utilizzato su un documento diverso da quello per cui è stato registrato

La cifratura dell'ESDC avviene attraverso un sistema di chiavi asimmetriche. La chiave pubblica, di lunghezza adeguata, è utilizzata per la cifratura del dato ed è installata sul sistema di firma. Il possessore della chiave privata è il solo in grado di decifrare il dato.

Per garantire la sicurezza, la coppia di chiavi, pubblica e privata, viene generata da un soggetto "terzo fidato" (tipicamente un Notaio o una Certification Authority). La chiave privata è custodita in modo sicuro dall'ente che l'ha generata il quale che si assume la responsabilità della segretezza della stessa.

OTP

1. Viene inviata una email al firmatario contenente un link per accedere al documento.
2. Tramite qualsiasi browser Internet, l'utente apre il link.
3. Prima di consentire l'accesso al documento, un codice OTP viene inviato via SMS al numero di cellulare del firmatario.
4. Autenticandosi utilizzando l'OTP ricevuto, il firmatario accede al documento attraverso il proprio browser e decide se autorizzare o meno la geolocalizzazione.
5. Il firmatario sottoscrive il documento tramite il browser.
6. Un timbro digitale contenente informazioni di base come nome del firmatario, data e ora della sottoscrizione, viene generato automaticamente e posizionato sulla pagina del documento.
7. Il documento viene sigillato con una firma tecnica PAdES con un certificato di firma tecnica. Questa firma PAdES ha il solo scopo di garantire la non modificabilità del documento dopo l'apposizione della firma. Quest'ultima firma non ha, quindi, valore ai fini della sottoscrizione del documento, ma è funzionale esclusivamente alla sicurezza del processo di firma.
8. Un documento di log dell'intero processo viene generato dal sistema per le verifiche in caso di contenzioso. In esso sono tracciati tutti gli eventi, dal momento del caricamento del documento nel sistema di firma fino alla sua chiusura, con indicazione temporale e, se precedentemente autorizzata, anche geografica.

CARATTERISTICHE DEL PROCESSO DI FIRMA

Utilizzando la firma grafometrica **CONFIDI SYSTEMA!** garantisce:

a) *l'identificazione del firmatario*

Confidi Systema! identifica in modo certo il firmatario richiedendone i documenti d'identità prima dell'apposizione della firma.

b) la connessione univoca della firma al firmatario

FG - Il sistema di firma grafometrica registra le caratteristiche fisiche della firma autografa, che il firmatario appone di suo pugno utilizzando una penna elettronica su un apposito dispositivo, il tablet. Le caratteristiche registrate sono, in relazione al tempo, la posizione della penna sul foglio e la pressione, rilevate con opportuna frequenza e risoluzione.
Questa rappresentazione informatica della firma è in grado di raccogliere informazioni superiori rispetto a quelle raccolte su carta da una firma autografa. L'univocità della connessione della firma al firmatario viene garantita dalla sottoscrizione effettuata davanti all'operatore di Confidi Systema!, previa identificazione del firmatario stesso. Inoltre il sistema offre la possibilità di effettuare opportuna perizia grafica, in modo del tutto equivalente ad una firma apposta su carta.

OTP - Il codice OTP è inviato via SMS al dispositivo cellulare che il firmatario ha dichiarato, in fase di accettazione del servizio, come di sua esclusiva proprietà e controllo.

c) *il controllo esclusivo del firmatario sul sistema di generazione della firma*

FG - Nella fase di apposizione della firma, il sistema è sotto il controllo esclusivo del firmatario. Il tablet mostra il documento completo in modo che il firmatario possa prenderne visione e verificarne personalmente i contenuti utilizzando le normali funzioni di visualizzazione del tablet (scorrimento, zoom, etc…). Durante l'apposizione della firma, il tablet mostra in tempo reale l'andamento del tratto grafico. L'operatore di Confidi Systema! non può in alcun modo interferire con l'operazione di firma fino al suo completamento o sino all'annullamento del processo.

OTP - La firma avviene attraverso un browser Internet controllato dal firmatario e previa autenticazione forte dello stesso tramite SMS inviato a telefono cellulare di sua esclusiva proprietà e controllo.

d) *l'immodificabilità del documento dopo l'apposizione della firma*

FG - Il sistema infatti impiega tecnologie che prevedono l'inclusione delle "impronte informatiche", dette "hash", del documento soggetto a sottoscrizione. Confrontando la corrispondenza dell'hash sigillata all'interno dei dati di firma e opportunamente protetta (come descritto al punto h) con l'impronta ricalcolata è possibile verificare se il documento abbia subito modifiche.

OTP - Questo requisito è garantito dalla firma tecnica PAdES del documento PDF sottoscritto.

e) *la possibilità per il firmatario di ottenere evidenza e copia di quanto sottoscritto*

FG - Prima dell'apposizione della firma il firmatario ha la possibilità di visualizzare il documento e leggerlo nella sua

interezza utilizzando gli strumenti standard disponibili sul tablet (scorrimento, zoom, etc…). A questo scopo sono scelti tablet che abbiano display con caratteristiche tali da consentire la corretta visualizzazione del documento (dimensioni e risoluzione).
Successivamente all'apposizione della firma, il firmatario potrà richiedere a Confidi Systema! di visualizzare il documento sottoscritto per mezzo di strumenti informatici standard in grado di visualizzare file PDF.

OTP - Attraverso l'uso del browser il firmatario è in grado di visualizzare in modo chiaro e consultabile l'intero documento; inoltre il firmatario può accedere al/a una copia del documento firmato.

f) l'individuazione del soggetto che eroga il servizio di firma elettronica avanzata

Il sistema utilizza un certificato per la firma PADES del documento (si veda il punto h per maggiori dettagli). Questo certificato di firma è emesso da una autorità di certificazione attendibile e riporta la dicitura "Confidi Systema!" che identifica in modo certo l'erogatore del servizio e che è verificabile con i comuni software per la visualizzazione di file PDF.

g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati

I documenti prodotti dal sistema sono esclusivamente nel formato standard ISO PDF/A che garantisce l'assenza di qualunque elemento in grado di modificare atti, fatti o dati in essi rappresentati.

h) la connessione unica della firma al documento sottoscritto

FG - I dati della firma grafometrica, che costituiscono il "vettore grafometrico" vengono uniti all'"impronta" informatica del documento da sottoscrivere in un'unica struttura dati che, con opportuna tecnica crittografica, viene cifrata, allo scopo di preservare i dati della firma da ogni possibilità di estrazione o duplicazione, e, infine, inserita all'interno del documento sottoscritto. Per la cifratura viene utilizzata una chiave pubblica a 2048 bit. L'unica chiave crittografica (privata) in grado di decifrare la struttura dati è in esclusivo possesso di un notaio appositamente designato e potrà essere utilizzata unicamente per eventuali perizie, solo su richiesta dall'autorità giudiziaria, per attestare l'autenticità del documento e della sottoscrizione.
Inoltre, per ogni firma eseguita, il sistema appone una firma "tecnica" di tipo PADES per garantire che il documento non abbia subito modifiche in periodi successivi all'apposizione della firma grafometrica. Mentre il "vettore grafometrico" allegato al documento è invisibile, la firma "tecnica" PADES può essere verificata con i software standard per la lettura dei file PDF.

OTP - Attraverso il file di log generato dal sistema di firma si ha una tracciatura dettagliata del processo di firma che consente di individuare in modo certo il momento di apposizione di una determinata firma su quale documento è avvenuta.