FIRMA ELETTRONICA AVANZATA

Documento delle caratteristiche del sistema di Firma Elettronica Avanzata ai sensi dell'art. 57 DPCM 22 febbraio 2013

1. Premessa

La Firma Elettronica Avanzata (di seguito "FEA"), come definita nel D. Lgs 82/2005 e successive modifiche (Codice dell'Amministrazione Digitale, di seguito "CAD"), è un insieme di dati in formato elettronico connessi ad un documento informatico che consentono l'identificazione del firmatario e garantiscono la connessione univoca al firmatario; essi sono creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, in modo tale da consentire di rilevare se i dati cui la firma si riferisce siano stati successivamente modificati. Un documento sottoscritto con FEA, in conformità alle previsioni di legge e alle regole tecniche di cui al DPCM 22 febbraio 2013, ha la medesima efficacia probatoria della scrittura privata cartacea sottoscritta con firma tradizionale.
Il servizio di Firma Elettronica Avanzata proposto da Italiaonline S.p.A. (di seguito "Servizio") consente di dematerializzare i contratti intercorrenti tra il Cliente e Italiaonline S.p.A. (di seguito "Italiaonline") relativi a tutti i servizi pubblicitari offerti da quest'ultima, mediante sottoscrizione dei contratti stessi in forma elettronica.
Il Servizio consiste nell'apposizione della firma del Cliente (anche per il tramite del Sottoscrittore in sua rappresentanza, se il Cliente è una società o ente) su un video dispositivo portatile (di seguito "Tablet") mediante apposita penna elettronica, da cui è possibile, tramite l'utilizzo di una specifica tecnologia, la rilevazione dinamica di tratti calligrafici e dell'immagine della firma stessa, in modo tale da connettere in maniera univoca la firma al firmatario.

2. Descrizione del processo FEA

Il processo di FEA si articola nelle seguenti fasi principali e si sviluppa nel rispetto delle regole tecniche previste dal CAD e dal D.P.C.M. 22 febbraio 2013, secondo quanto descritto nel successivo art. 4.

- Il Cliente (previamente identificato) visualizza sul Tablet il contratto da sottoscrivere e ne può verificare integralmente il contenuto, anche tramite funzionalità di "zoom" che consentono di ingrandire le sezione di interesse;
- Il Cliente appone la firma grafometrica sul Tablet mediante apposita penna elettronica;
- Tramite specifica soluzione tecnica di seguito descritta i dati biometrici connessi alla sottoscrizione e l'immagine della firma vengono immediatamente cifrati e sigillati in maniera univoca al documento che diviene immodificabile;
- Il documento informatico viene archiviato secondo le norme previste per la conservazione sostitutiva;
- Il Cliente riceve via posta elettronica all'indirizzo sopra indicato copia del documento sottoscritto con FEA. Tale copia contiene solo l'immagine della firma e non anche i dati biometrici della stessa.

I dati biometrici, cifrati e sigillati elettronicamente all'interno del documento informatico cui si riferiscono, sono raccolti in modo da escludere qualsiasi possibilità di risalire a eventuali informazioni inerenti lo stato di salute dei firmatari.

3. Caratteristiche tecniche e descrizione del Servizio

La soluzione di FEA adottata da Italiaonline, in conformità al CAD e al DPCM 22/02/2013, garantisce:

- **L'identificazione del firmatario del documento**: prima della sottoscrizione del documento il Cliente viene riconosciuto tramite idoneo documento d'identità, acquisito in copia in allegato alle presenti condizioni di Servizio e conservato a norma di legge.
- **La connessione univoca della firma al firmatario**: tale connessione è garantita dal fatto che il firmatario appone di suo pugno la firma sul Tablet, mediante utilizzo di apposita penna elettronica. Il sistema applicativo rileva i dati biometrici della firma insieme all'impronta informatica del contenuto del PDF del documento, composta da una stringa di caratteri generata da apposito algoritmo a tutela dell'integrità dei dati (di seguito "Hash"); e ciò in modo che sia sempre tecnicamente possibile eseguire una perizia calligrafica in maniera equivalente ad una firma autografa apposta su carta.
- **Il controllo esclusivo del firmatario del sistema di generazione della firma**: durante la fase di firma il sistema è sotto il controllo esclusivo del firmatario. Quest'ultimo ha completa disponibilità del Tablet e può visualizzare nella sua interezza il documento da sottoscrivere, con facoltà di scorrere il testo e ingrandire i dati inseriti o le sezioni di maggiore interesse. Al momento della sottoscrizione, la penna mostra in tempo reale il segno grafico apposto dal Cliente sul Tablet. In ogni momento, fino al termine della fase di firma, è facoltà del Cliente cancellare e correggere eventuali errori.
  La tecnologia utilizzata e le misure di sicurezza adottate, come di seguito descritte, garantiscono che i dati biometrici rilevati, opportunamente cifrati, siano univocamente connessi al firmatario. I parametri biometrici inseriti del documento non saranno registrati in nessun altro luogo se non all'interno del documento stesso.
- **Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma.**
  L'inalterabilità, immodificabilità e integrità del documento firmato sono garantiti tramite un sistema basato su una coppia di chiavi asimmetriche (una pubblica e una privata). In particolare, al termine dell'acquisizione della firma, il documento viene immediatamente sigillato – unitamente ai dati biometrici cifrati mediante utilizzo di diversa e apposita coppia di chiavi asimmetriche descritte al successivo par. 4.8 - tramite apposizione di firma digitale di Italiaonline e marca temporale. Il certificato digitale di Italiaonline è rilasciato da una Certification Authority accreditata presso gli enti competenti che assicura il rispetto dei requisiti di sicurezza. La chiave privata del certificato di firma digitale è custodita da Italiaonline nel proprio sistema sicuro "Hardware Security Module" (di seguito "HSM") (da cui non è esportabile), che garantisce l'opportuna protezione. Si precisa che l'HSM è un criptoprocessore utilizzato per la gestione delle firme e chiavi digitali.
  La soluzione tecnologica adottata consente di verificare che il documento non sia stato alterato mediante confronto tra l'impronta ricalcolata e quella sigillata all'interno del documento firmato. Tale confronto può essere operato mediante: a) ricalcolo dell'Hash del pdf sigillato con dati biometrici; b) decifratura dell'Hash originariamente calcolato tramite chiave pubblica del certificato di firma digitale (memorizzata all'interno del documento insieme all'Hash stesso); c) confronto dei valori dei due Hash per il controllo di integrità.
  In caso di occasionale mancanza di connettività, il sistema garantisce in ogni caso l'integrità del documento mediante idonee misure tecniche e di sicurezza.
- **La possibilità per il firmatario di ottenere evidenza di quanto sottoscritto.**

Il Cliente riceve via posta elettronica all'indirizzo sopra indicato copia del documento sottoscritto con FEA. Tale copia contiene solo l'immagine della firma e non anche i dati biometrici della stessa. In ogni momento, inoltre, il Cliente può richiedere a Italiaonline copia dei documenti sottoscritti mediante FEA telefonando al Servizio Clienti di Italiaonline, telefonando al seguente numero verde 800/011411, inviando una mail al seguente indirizzo: info@Italiaonline.it o inviando un fax al seguente numero verde: 800/011412.

- **Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati**
  I documenti firmati con FEA sono prodotti in formati che garantiscono l'assenza, nell'oggetto della sottoscrizione, di qualunque elemento che possa modificare gli atti, fatti o dati in essi rappresentati. In particolare, Italiaonline utilizza il formato ISO PDF/A.

- **La connessione univoca della firma al documento sottoscritto**
  I dati biometrici della firma vengono inseriti nel documento e ad esso uniti indissolubilmente mediante un'impronta informatica protetta e cifrata con una seconda coppia di chiavi asimmetriche specificamente dedicate a tale cifratura. I dati biometrici di ogni firma sono infatti cifrati insieme all'hash del PDF originale e sigillati tramite certificato digitale. Tale certificato digitale utilizzato per garantire la cifratura dei dati biometrici è rilasciato da una Certification Authority accreditata presso gli enti competenti. La chiave privata in grado di estrarre le informazioni è in possesso esclusivo di un soggetto terzo fiduciario (di seguito, per brevità, "S.T.") appositamente designato da Italiaonline che offre idonee garanzie di indipendenza e sicurezza ed è necessaria per poter eseguire le opportune perizie calligrafiche.
  La tecnologia utilizzata consente in ogni caso di connettere univocamente i dati biometrici del firmatario al documento da questi sottoscritto, in modo che la firma non possa essere in alcun modo associata ad altro documento, né riutilizzata.
  In ogni caso, la decifrazione dei dati biometrici e il relativo accesso "in chiaro" sono consentiti esclusivamente nei casi previsti dalla legge, su richiesta delle Autorità competenti (ad esempio, in caso di contenzioso legate al disconoscimento della firma).I dati biometrici quindi, come detto, non hanno residenza nel Tablet ma, una volta incorporati nel documento, vengono cancellati e non risultano conseguentemente visualizzabili se non tramite la collaborazione tra Italiaonline, titolare della chiave pubblica contenuta nel certificato digitale e del suddetto soggetto terzo, detentore della chiave privata.
  In ogni caso, si precisa che i dati biometrici non sono conservati, neanche per periodi limitati, sui Tablet utilizzati per la raccolta, venendo, come sopra descritto, memorizzati in forma cifrata all'interno dei documenti informatici sottoscritti, tramite i suddetti sistemi di crittografia.
  In caso di occasionale mancanza di connettività, viene temporaneamente utilizzata una chiave simmetrica di cifratura che in ogni caso non è visibile in chiaro in modo da garantire che l'integrità e la riservatezza del documento siano sempre tutelate.

4. Descrizione delle caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare alla normativa

Italiaonline utilizza le seguenti tecnologie al fine di proteggere la raccolta e la conservazione dei dati biometrici e garantire l'inalterabilità e univocità del documento sottoscritto con FEA:

- La cifratura dei dati è permessa utilizzando la chiave pubblica di un certificato digitale rilasciato a Italiaonline da una Certification Authority accreditata presso gli enti competenti.
- I dati biometrici sono cifrati utilizzando doppia modalità di cifratura RSA, SHA-1, SHA-2. Il documento che contiene i dati biometrici è inoltre firmato digitalmente per garantirne l'inalterabilità e la veridicità.
- La chiave privata che consente la decifrazione dei dati biometrici è inoltre detenuta da S.T. appositamente designato da Italiaonline

5. Misure di sicurezza adottate da Italiaonline

Al fine di proteggere i dati biometrici indicati nelle presenti condizioni, Italiaonline ha adottato le seguenti misure di sicurezza, anche tenuto conto delle previsioni dell'Autorità Garante della protezione dei dati personali in materia:

- Tutte le trasmissioni di dati biometrici avvengono esclusivamente tramite canali di comunicazione sicuri con l'utilizzo di tecniche crittografiche
- Sono state adottate idonee misure volte a ridurre i rischi di installazione abusiva di software o di modificazione della configurazione dei dispositivi in dotazione agli agenti, nonché ogni accorgimento utile a contrastare l'azione di eventuali agenti malevoli (malware);
- È previsto un sistema di gestione dei dispositivi impiegati nei trattamenti grafometrici basato su certificati digitali e policy di sicurezza che disciplinano, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro. In particolare, sono disponibili funzionalità di cancellazione remota dei dati dal Tablet (c.d. "Remote Wiping"), applicabili nei casi di smarrimento o sottrazione dei dispositivi a garanzia e tutela della sicurezza;
- Sono inoltre stati adottati tutti gli accorgimenti tecnici necessari a garantire la sicurezza perimetrale della rete aziendale (es. firewall) e contro i tentativi di accesso abusivo ai dati.

6. Conservazione sostitutiva dei documenti

Al termine dell'operazione di firma, il documento firmato con FEA e contenente i parametri biometrici cifrati è inviato tramite un canale sicuro alla conservazione sostitutiva, effettuata a norma di legge tramite S.T. appositamente incaricato e abilitato allo svolgimento di tale attività nel rispetto delle previsioni del CAD e della normativa di settore.

7. Copertura assicurativa

In conformità alla normativa vigente, Italiaonline si è dotata di una copertura assicurativa per la responsabilità civile connessa al servizio di FEA rilasciata da primaria compagnia di assicurazioni abilitata ad esercitare nel campo dei rischi industriali per un ammontare non inferiore ai massimali previsti dalla legge.

8. CONTROLLI: obiettivo e ambito di applicazione

Italiaonline si è dotata di una procedura interna di controllo periodico conformemente alla vigente normativa in materia.