

SCHEMA ILLUSTRATIVA
CARATTERISTICHE DEL SISTEMA DI FIRMA ELETTRONICA AVANZATA ("FEA")
E SUE CARATTERISTICHE TECNOLOGICHE (ai sensi degli artt. 57, c. 1 lett. e) e f) del D.P.C.M. 22.02.2013)

Il servizio di firma elettronica avanzata (di seguito, il "Servizio di FEA") è attuato da AUTOTORINO S.p.A. (di seguito, "AUTOTORINO") nel rispetto delle vigenti disposizioni in materia. Si riportano di seguito le caratteristiche dello stesso.

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

AUTOTORINO identifica preliminarmente in modo certo il firmatario, richiedendo un documento di riconoscimento in corso di validità di cui viene acquisita unitamente all'apposita modulistica di adesione debitamente compilata. Copia del documento di riconoscimento e del modulo di adesione al servizio sottoscritto dal firmatario sono conservati per 20 anni, in conformità alla vigente normativa.

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

b.1 FEA Grafometrica

La rappresentazione informatica della firma racchiude informazioni superiori alla raccolta della firma autografa su carta. Infatti, oltre ai dati relativi all'immagine grafica il sistema registra anche le caratteristiche dinamiche della firma autografa che il firmatario appone di suo pugno con penna elettronica, su un apposito dispositivo di firma (il "Pad"). Le caratteristiche registrate corrispondono alla scansione temporale di posizione/inclinazione, ritmo, pressione, velocità, accelerazione e movimento, acquisite durante la firma sul Pad. I dati grafometrici sono tipici e specifici di ogni persona. L'univocità della connessione viene quindi garantita: (i) dalla sottoscrizione effettuata previo riconoscimento del firmatario; (ii) dalla acquisizione attraverso il Pad, in sede di apposizione della firma, di dati comportamentali (c.d. "biometrici" o "grafometrici") univocamente riconducibili al firmatario medesimo, immediatamente inglobati nel documento informatico da lui sottoscritto con un legame indissolubile ed esclusivo, protetti tramite crittografia e in alcun modo conservati nel Pad; (iii) dalla possibilità di effettuare opportuna perizia grafica, in modo del tutto equivalente ad una firma autografa su carta.

b.2 FEA non Grafometrica (o FEA in Mobilità)

L'univocità della connessione della firma al firmatario nel caso di FEA non Grafometrica viene garantita (i) dalla sottoscrizione effettuata previo riconoscimento del firmatario nonché (ii) dall'utilizzo da parte di quest'ultimo di un numero di cellulare riferito ad una SIM card di cui dichiara di essere titolare esclusivo o di avere, in quel momento e per tutto l'arco temporale del processo di sottoscrizione, piena ed esclusiva disponibilità. Il firmatario riceve un codice OTP, generato da un ente certificato, mediante SMS inviato al numero di cellulare dichiarato precedentemente e lo digita nella finestra di richiesta entro 90 (NOVANTA) secondi. Allo scadere dei 90 (NOVANTA) secondi, in caso di mancata conferma, il codice OTP ricevuto scade e, per procedere, necessita la richiesta di un nuovo codice OTP. Le informazioni raccolte dal sistema durante la transazione sono inserite all'interno di ogni firma e collegano in maniera univoca quella firma al firmatario.

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

c.1 FEA Grafometrica

Durante la fase di firma, il sistema è nella piena ed esclusiva disponibilità e sotto il controllo esclusivo del firmatario. Lo schermo del Pad mostra il dettaglio della clausola oggetto della firma consentendo al firmatario di verificare personalmente sia i propri dati, sia ogni dettaglio contrattuale. Durante l'apposizione della firma, il sistema guida il firmatario nel processo di firma. Mentre egli appone la sottoscrizione con l'apposita penna elettronica l'immagine della firma appare in tempo reale sul Pad. Apposite funzioni consentono al firmatario di confermare o cancellare la firma in caso di errori. Il processo di sottoscrizione avviene in modo automatico sulla base del programma installato sul Pad utilizzato dal firmatario. Ogni comunicazione tra il Pad e il sistema di generazione della firma è criptata ed anche i dati grafometrici relativi alla firma apposta sul Pad dal firmatario sono automaticamente cifrati. A seguito della loro cifratura ed invio su canale criptato al server (per la gestione delle ulteriori fasi del processo), i dati grafometrici temporaneamente registrati nella memoria del Pad sono eliminati e non sono più recuperabili.

c.2 FEA non Grafometrica (o FEA in Mobilità)

Durante la fase di firma, il sistema è nella piena ed esclusiva disponibilità e sotto il controllo esclusivo del firmatario.

Lo schermo del Pad mostra il dettaglio della clausola oggetto della firma consentendo al firmatario di verificare personalmente sia i propri dati, sia ogni dettaglio contrattuale. Il firmatario procede, quindi, in autonomia alla lettura delle clausole ed alla selezione dei relativi campi di firma sui quali lo stesso è chiamato ad esprimere manualmente (processo di "Point and Click") la propria volontà di sottoscrizione. Conclusa tale fase, il Pad visualizza una schermata recante il riepilogo di tutti i campi per la sottoscrizione da lui selezionati nonché la richiesta di confermare la sua volontà di firmare. Dopo la conferma, il firmatario riceve un codice OTP, generato da un ente certificato, mediante SMS inviato al numero di cellulare dichiarato precedentemente e lo digita nella finestra di richiesta entro 90 (NOVANTA) secondi. Allo scadere dei 90 (NOVANTA) secondi, in caso di mancata conferma, il codice OTP ricevuto scade e, per procedere, necessita la richiesta di un nuovo codice OTP. Le informazioni raccolte dal sistema durante la transazione sono inserite all'interno di ogni firma e collegano in maniera univoca quella firma al firmatario. Le operazioni sopra descritte e l'esito della transazione con la Certification Authority sono quindi inserite in una struttura dati ("blob di firma") e automaticamente criptate.

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

Al termine della sottoscrizione, una volta esaurito il processo di cifratura precedentemente descritto, il documento informatico è firmato digitalmente con il certificato qualificato emesso da una Certification Authority riconosciuta. La tecnologia di firma digitale include l'impronta informatica ("hash") del contenuto soggetto a sottoscrizione. Il controllo della corrispondenza tra un'impronta ricalcolata e quella "sigillata" all'interno delle firme permette di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma. Questo consente di rilevare ogni possibile alterazione o modifica effettuata al predetto documento informatico sottoscritto dal firmatario.

e) Descrizione delle caratteristiche del sistema che garantiscono la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto.

All'atto della presentazione del documento per la sottoscrizione, il firmatario può visualizzare il contenuto in tutte le sue parti, con apposite funzioni di posizionamento. Successivamente, all'esito del processo di firma sopra descritto, il firmatario potrà visualizzare e conservare il documento elettronico da lui sottoscritto (privo del dato biometrico), che verrà inviato alla casella di posta elettronica comunicata all'atto di adesione del servizio ovvero, se richiesto dal Cliente, reso disponibile su supporto cartaceo.

f) Descrizione delle caratteristiche del sistema che garantiscono l'individuazione del soggetto erogatore della soluzione FEA.

Il certificato di firma digitale, utilizzato a chiusura del processo FEA, individua il soggetto erogatore del servizio ed è emesso da un'autorità di certificazione tecnica (Certification Authority TI Trust Technologies S.r.l.). In questo caso ogni documento, dopo la raccolta delle firme grafometriche del Cliente, viene sigillato tramite apposizione della firma digitale di AUTOTORINO rilasciata dalla Certification Authority.

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

I documenti prodotti dal sistema utilizzano esclusivamente formati atti a garantire l'assenza, nell'oggetto della sottoscrizione, di qualunque elemento idoneo a modificare gli atti, i fatti e i dati in essi rappresentati. Ad esempio, attualmente i documenti sono esclusivamente in formato standard ISO PDF/A (non contenente script, macro, campi da riempire od altri elementi che, dopo la generazione, potrebbero alterarne il contenuto).

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

I dati della firma, integrati con informazioni aggiuntive, vengono inseriti nel documento in una struttura, detta "blob di firma", che li unisce indissolubilmente all'impronta informatica del documento sottoscritto. Questa struttura è protetta con opportuna tecnica crittografica, al fine di preservare la firma da ogni possibilità di estrazione o duplicazione. L'unica chiave crittografica in grado di estrarre le informazioni è in esclusivo possesso di un terzo fiduciario appositamente designato da AUTOTORINO, dotato di idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave e potrà essere usata in sede di perizia, espressamente nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria, per attestare l'autenticità del documento e della sottoscrizione. Inoltre, il sistema appone a sigillatura dell'intero documento una "firma digitale" in formato standard PAdES. A differenza del "blob di firma", queste firme tecniche sono visibili e verificabili con gli strumenti informatici standard per la presentazione e lettura dei documenti (es. PDF Reader).

i) Descrizione delle caratteristiche delle tecnologie utilizzate nel servizio di firma elettronica avanzata.

Il trasferimento dei dati e la loro memorizzazione nel "blob di firma" sono protetti con le seguenti tecnologie crittografiche:

- crittografia simmetrica standard AES con chiave a 256 bit segreta per la protezione dei dati;
- RSA 2048 bit con chiave privata detenuta da una terza parte per la cifratura della chiave AES;
- firma tecnica del documento PDF con firma PAdES.

j) Descrizione delle modalità attraverso cui i clienti possono richiedere copia dei moduli, da questi sottoscritti.

I Clienti, salva loro diversa indicazione, riceveranno a mezzo posta elettronica, all'indirizzo dagli stessi fornito, copia della documentazione sottoscritta. Se richiesto, il Cliente potrà ricevere copia cartacea della predetta documentazione.

k) Descrizione delle modalità attraverso cui i clienti possono richiedere di revocare la propria adesione al servizio di posta elettronica.

Il modulo di adesione alla FEA riporta il link al "Modulo di richiesta di revoca del servizio di Firma Elettronica Avanzata" mediante il quale il cliente è libero di revocare il servizio precedentemente sottoscritto.