helvetia
La tua Assicurazione svizzera

Caratteristiche tecniche del sistema di firma elettronica avanzata ("FEA") e tecnologie utilizzate

art. 56 e 57 comma 1 lett. e) del Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013

Il servizio di firma elettronica avanzata (di seguito anche "servizio" o "FEA") è attuato da Helvetia Compagnia Svizzera d'Assicurazioni SA - Rappresentanza Generale e Direzione per l'Italia nel rispetto delle vigenti disposizioni in materia. Si riportano di seguito le caratteristiche del servizio in oggetto.

a) Caratteristiche del sistema che garantiscono l'identificazione del firmatario.

Helvetia identifica preliminarmente il firmatario richiedendo il relativo documento d'identità e la compilazione del modulo di adesione. I predetti documenti vengono conservati per 20 anni, in conformità alla vigente normativa. L'adesione al servizio FEA è facoltativa.

b) Caratteristiche del sistema che garantiscono la connessione univoca della firma al firmatario.

a1 **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.

a2 **FEA non Grafometrica (o FEA OTP)**

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 avere, in quel momento e per tutto l'arco temporale del processo di sottoscrizione, piena ed esclusiva disponibilità. Il firmatario effettua una chiamata ad un numero verde ed inserisce una One Time Password ("OTP") di firma sulla tastiera del proprio telefono. Le informazioni raccolte dal sistema durante la transazione telefonica sono inserite all'interno di ogni firma e collegano in maniera univoca quella firma al firmatario. Il sistema certifica che il numero dichiarato come proprio dall'utente abbia effettuato una chiamata al numero verde indicato e abbia inserito l'OTP relativo a quella transazione e relativo a quel documento.

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

a1 **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.

a2 **FEA non Grafometrica (o FEA OTP)**

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 nome del firmatario, il suo numero di cellulare, il riepilogo di tutti i campi per la sottoscrizione da lui selezionati nonché la richiesta di confermare quanto indicato. Dopo la conferma, il Pad visualizza un numero telefonico (numero verde con chiamata gratuita) ed una password avente durata temporale limitata (OTP), sotto forma sia di codice numerico sia di quick response code (QR code), che il firmatario dovrà comporre utilizzando il numero di cellulare il quale, sulla base di quanto dichiarato dallo stesso firmatario, si trova nella sua piena ed esclusiva disponibilità. Le operazioni sopra descritte e l'esito del processo di strong authentication e sottoscrizione sono quindi inserite in una struttura dati ("blob di firma") e automaticamente criptate.

d) 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 il documento informatico è firmato digitalmente con 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 documento informatico sottoscritto dal firmatario.

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

All'atto della presentazione del documento per la firma, il firmatario può visualizzare sul video il contenuto in tutte le sue parti, con apposite funzioni di posizionamento. Successivamente il firmatario potrà visualizzare il documento elettronico firmato, comodamente a casa propria essendo quest'ultimo già disponibile nella propria casella di posta elettronica personale che il firmatario ha dichiarato in fase di adesione.

f) 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 sia dell'Intermediario che del Cliente, viene sigillato tramite apposizione della firma digitale di Helvetia rilasciata dalla Certification Authority.

g) 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.

h) Caratteristiche del sistema che garantiscono la connessione univoca della firma al documento sottoscritto.

I dati della firma 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

H-964 01.18

Helvetia Compagnia Svizzera d'Assicurazioni SA
Rappresentanza Generale e Direzione per l'Italia
Imp. Autor. alleser. delle ass. con D. di ric. Del M. Ind., Comm. Ed Artig. del 26/11/1984 pubbl. sul suppl. n.2 G.U.
n. 357 del 31/12/1984 Provv. ISVAP n. 00757 del 19/12/1997 pubbl. su G.U. n. 298 del 23/12/1997

un terzo fiduciario appositamente designato da Helvetia, 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 SIGNATURE 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:

j) Descrizione delle modalità attraverso cui i clienti possono richiedere copia del modulo di adesione, da questi sottoscritto, al servizio di firma elettronica avanzata.

I Clienti, salva loro diversa indicazione, riceveranno attraverso posta elettronica, all'indirizzo dagli stessi fornito, copia della documentazione sottoscritta: Condizioni, Scheda Informativa sulla Privacy, Modulo di adesione e documenti di riconoscimento. Se richiesto, il Cliente potrà ricevere copia cartacea della predetta documentazione tramite posta elettronica all'indirizzo email comunicato in sede di attivazione del Servizio.

- 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.

Per eventuali approfondimenti tecnici si rimanda alla documentazione analitica pubblicata sulla sezione del sito www.helvetia.it dedicata alla FEA.

Helvetia Compagnia Svizzera d'Assicurazioni SA
Rappresentanza Generale e Direzione per l'Italia
Imp. Autor. alleser. delle ass. con D. di ric. Del M. Ind., Comm. Ed Artig. del 26/11/1984 pubbl. sul suppl. n.2 G.U. n. 357 del 31/12/1984 Provv. ISVAP n. 00757 del 19/12/1997 pubbl. su G.U. n. 298 del 23/12/1997