Specifiche del sistema e delle tecnologie utilizzate nel Servizio di Firma Elettronica Avanzata (F.E.A.) erogato da Casa di cura Prof. Nobili Srl

(ai sensi dell'Art. 57, c.1, Lett. e), f) del DPCM 22.02.2013)

Premessa

Il presente documento è redatto ai sensi del D.P.C.M. 22/02/2013 recante "Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali…", in particolare ai sensi dell'art. 57, C. 1, Lett. e) ed f) che stabilisce a carico di chi eroga soluzioni di F.E.A. (Firma Elettronica Avanzata di:

- Rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'art. 56, c.1;
- Fornire le specifiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto dalla normativa in vigore.

In particolare Casa di Cura Prof. Nobili Srl intende offrire ai suoi utenti (di seguito **Firmatari**) la possibilità di sottoscrivere elettronicamente tramite "Firma Elettronica Avanzata Grafometrica" (di seguito **F.E.A**.) documenti informatici (es: il consenso alla costituzione ed alimentazione del Dossier Sanitario Elettronico) che saranno sottoposti all'utente da operatori Amministrativi durante i percorsi assistenziali svolti all'interno della Casa di Cura Prof. Nobili Srl (di seguito anche **Struttura**).

Ai sensi dell'Art. 57, c.1, Lett. g), la Casa di Cura Prof. Nobili Srl rende disponibile il presente documento sul sito web http://www.casadicuranobili.it. in cui vengono descritte le tecnologie ed i passaggi utilizzati per la raccolta della firma grafometrica.

Firma Elettronica Avanzata (F.E.A)

Di cosa si tratta?

La Firma Elettronica Avanzata (F.E.A. oppure Firma Grafometrica) è una modalità utilizzata per sottoscrive un documento informatico da parte di una persona opportunamente identificata mediante l'apposizione di una normale firma su un dispositivo elettronico (Tavoletta per la raccolta della firma) per mezzo di una penna elettronica in grado di rilevare specifici dati della firma del sottoscrittore e associarli al documento informatico (generato in formato PDF) riprodotto sullo schermo dell'Operatore e visibile da parte del Sottoscrittore.

La **F.E.A**. raccolta e formata nel rispetto delle regole di cui alla normativa di riferimento (D.Lgs. n. 82/2005 – Codice dell'Amministrazione Digitale e nel D.P.C.M. 22/02/2013), possiede i requisiti informatici e giuridici che consentono di qualificarla come Firma Elettronica Avanzata (ai sensi dell'Art. 1, C. 1, Lett. q-bis del Codice dell'Amministrazione Digitale).

Il documento informatico sottoscritto con la **F.E.A**. è realizzato in modo tale che vengano garantite:

- L'identificazione del soggetto firmatario che sottoscrive il documento
- La connessione univoca della firma al soggetto firmatario
- Il controllo esclusivo in capo al soggetto sottoscrivente del sistema di generazione della firma
- La connessione univoca della firma al documento sottoscritto
- La **non modificabilità** e **non alterabilità** del documento sottoscritto
- La possibilità per il firmatario di ottenere, a richiesta, evidenza di quanto sottoscritto
- La connessione univoca della firma al documento sottoscritto

Sul piano giuridico la firma tramite **F.E.A**. ha la stessa validità legale del documento cartaceo sottoscritto con firma autografa, anche ai fini probatori e pertanto ha l'efficacia prevista dall'Art. 2702 del Codice Civile.

La FEA è disciplinata da:
1. Regolamento EU 910/2014 (di seguito "eIDAS");
2. Decreto Legislativo 82/2005 e ss.mm (di seguito "CAD");
3. Decreto del Presidente del Consiglio dei Ministri del 22.02.2013 (di seguito "DPCM").

Descrizione del sistema e delle tecnologie utilizzate per la firma grafometrica
Quanto sotto riportato risponde a quanto previsto dalle Regole Tecniche (Art. 57 C. 1 Lett. e) ossia …*rendere note le caratteristiche del sistema realizzato atte a garantire quanto previsto dall'Art. 56, C. 1...*

Il Sistema di Firma Elettronica Avanzata si compone di elementi software ed hardware e di un processo di acquisizione di firma che è svolto da un operatore appositamente formato, in conformità a quanto descritto nel seguito.

Trattamento dei dati biometrici della firma

La soluzione adottata da Casa di Cura Prof. Nobili Srl per la sottoscrizione dei documenti informatici mediante Firma Elettronica Avanzata assicura l'impossibilità di acquisizione e riutilizzo dei dati biometrici di firma (considerati dati particolari sulla base dell'Art. 9 Par. 1 del GDPR) al di fuori del processo di firma specifico.

Particolari precauzioni tecniche sono state infatti adottate per garantire che in nessuna fase del processo di acquisizione ed abbinamento "documento - firma" i dati biometrici possano essere acquisiti in modo fraudolento e senza la volontà del firmatario. Infatti:

- Lo scambio dei dati di firma tra il dispositivo di acquisizione (Tablet) e la postazione di lavoro che gestisce l'associazione documento-firma, avviene in modalità sicura attraverso l'uso di un apposito modulo di encryption hardware che presenta un alto livello di sicurezza anti intrusione (a titolo di esempio, l'algoritmo AES 256 bit encryption e scambio di chiavi RSA 2048).

- I dati di firma biometrica rilevati dal dispositivo di acquisizione vengono immediatamente cifrati con chiave pubblica utilizzando il certificato di firma rilasciato sulla PdL di firma di cui al precedente paragrafo, rendendo impossibile quindi il loro utilizzo in chiaro per sottoscrivere altri documenti.

- La chiave privata del certificato di firma di cui sopra, unico strumento abilitato a decifrare (e quindi a visualizzare in chiaro le caratteristiche grafiche della firma e i dati biometrici che la caratterizzano) sono detenute dall'Ente Certificatore incaricato da Confirmo per l'erogazione del servizio FEA ed utilizzabili solo esclusivamente su mandato dell'autorità giudiziaria.
- In mobilità, il dato grafometrico viene letto sul Tablet, preso in carico dalla App di firma, cifrato con chiave di cifratura pubblica ed integrato nel file PDF, il quale viene a sua volta firmato digitalmente (con firma non qualificata o certificato selfsigned). Il dato biometrico è sicurizzato all'interno del PDF.
- Sia in Sede che in mobilità la soluzione proposta risponde positivamente ai requisiti di sicurezza/tecnologici di seguito riportati:

    - La trasmissione dei dati ai moduli server avviene in modalità sicura.
    - Tutti gli scambi di informazioni tra i diversi server nel sistema informativo centralizzato saranno autenticati e cifrati in HTTPS.

L'ambiente in cui tali dati verranno resi disponibili risulta "protetto" garantendo che la decifratura, strettamente finalizzata alla perizia calligrafica, possano poi sopravvivere ed essere utilizzati in altri contesti.

Sistema informatico di firma

Il sistema di firma grafometrica adottato da **Casa di Cura Prof. Nobili Srl** e offerto da **Confirmo Srl** garantisce la protezione dei dati biometrici che rendono riconducibile, in modo univoco, la firma apposta sul tablet al firmatario. La connessione tra il tablet di firma e la postazione di lavoro dell'operatore avviene in modalità protetta utilizzando un algoritmo AES 256 bit encryption e scambio di chiavi RSA 2048. La cifratura dei dati biometrici avviene tramite un certificato pubblico con chiave asimmetrica ed algoritmo di cifratura. Successivamente i dati vengono inglobati nel pdf insieme alla generazione di una firma PadES, attraverso l'applicazione di una firma digitale tecnica, basata su un ulteriore certificato con chiave privata ed idoneo algoritmo. I dati biometrici non vengono in nessun modo memorizzati in chiaro, né dal tablet né dall'applicazione di firma. L'insieme dei valori biometrici viene inoltre connesso, in modo univoco ed indissolubile, al documento informatico visualizzato e sottoscritto dal **firmatario**, in modo che la stessa firma grafometrica non possa essere associata ad un altro documento. Inoltre, al fine di rendere immodificabile l'intero documento firmato dal **firmatario**, a chiusura di ogni transazione viene applicata una firma digitale qualificata. Il documento digitale sottoscritto dal **firmatario** viene memorizzato in formato PDFa1-a e firmato digitalmente in modalità PAdES, in modo da soddisfare i requisiti normativi legati all'autoconsistenza, non modificabilità e leggibilità dello stesso. Al termine del processo di firma il file è archiviato nel repository documentale aziendale.

Il software

Il software utilizzato è **Confirmo** Sviluppato da Confirmo S.r.l. e che serve a firmare elettronicamente i documenti utilizzando tutti i tipi di firma elettronica ad oggi disponibili secondo i regolamenti Eidas e Agid tra cui la firma elettronica avanzata di tipo grafometrico che prevede l'uso dei dati biometrici di firma.
Confirmo offre un set di API che consente una facile e rapida integrazione con l'applicativo gestionale "H20" sviluppato da AFEA Spa.

La soluzione si basa sul concetto fondamentale per cui **la F.E.A**. è costituita non solo dalla rappresentazione grafica del tratto fine a se stesso (glifo) ma anche da un insieme di parametri biometrici fondamentali ad esso associati, quali ad esempio la pressione del tratto sul supporto di firma, la continuità del tratto, la sequenza con cui le operazioni di scrittura, nell'ambito della firma stessa, vengono eseguite.

La firma grafometrica acquisita dal sistema:

- E' prodotta personalmente da una persona (Firmatario), di proprio pugno, senza bisogno di alcun dispositivo personale e mediante un hardware di acquisizione (dispositivi di acquisizione) reso disponibile direttamente nell'ambito della soluzione.
- E' automaticamente collegata al documento oggetto della firma.
- Viene cifrata tramite opportuna chiave pubblica per renderla inviolabile da parte di chiunque.
- E' integrata nel documento sotto forma di una firma digitale standard PAdES, cosicché qualunque copia di Adobe Reader o di altro software compatibile con il formato PDF e con la firma PAdES possa visualizzarla.
- E' corredata di elementi aggiuntivi opzionali richiesti dalla normativa per soddisfare i requisiti della **F.E.A**.: firma digitale dell'operatore che cura l'esecuzione della firma.

Il documento così realizzato risulta perfettamente auto consistente, fruibile con strumenti standard e di pubblica reperibilità, facile da gestire, archiviare, conservare, esibire e riprodurre.
Questa auto consistenza si traduce nella possibilità di utilizzare il documento, di avere evidenza dell'identità del sottoscrittore e di tutti i dettagli dell'organizzazione che lo ha prodotto indipendentemente dal sistema informatico specifico.

La componente Hardware

Per la raccolta della firma vengono utilizzati dispositivi di acquisizione con schermo sensibile connessi ad un computer tramite un collegamento cifrato.
I dispositivi di acquisizione dei dati biometrici sono in grado di rilevare posizione (coordinate x, y dei punti), tempo e pressione della firma, velocità ed accelerazione.
La comunicazione tra Computer e dispositivi di acquisizione avviene in modalità cifrata utilizzando un algoritmo AES 256 bit encryption e scambio di chiavi RSA 2048. E' stato oggetto di accurata analisi la criticità legata alla possibilità di fare il dump della memoria a seguito del crash di una applicazione, ovvero una fotografia di tutto ciò che il processo ha allocato in memoria fino a quel momento tra cui anche i dati biometrici, se non opportunamente gestiti da software.
Confirmo utilizza un algoritmo che cifra i dati biometrici simultaneamente all'acquisizione non lasciando mai in memoria la totalità dei punti (comunicazione a blocchi).

L'hardware utilizzato è composto da:

- Un server in Cloud
- Postazioni fisse di firma organizzate per la raccolta della Firma Elettronica Avanzata, composte da un PC con monitor (postazione di lavoro) con connesso tablet con schermo sensibile prodotta dalla società Samsung, modello Galaxy TAB S6 con schermo da 10,4" direttamente connesse alla postazione di lavoro.
- Maggiori informazioni tecniche sulle caratteristiche dei dispositivi di firma sono disponibili sul sito: https://www.samsung.com/it/tablets/galaxy-tab-s/galaxy-tab-s6-10-5-inch-gray-128gb-lte-sm-t865nzaaitv/

Il processo di firma dei documenti informatici

Casa di Cura Prof. Nobili Srl utilizza, quale componente hardware per la raccolta della firma, tablet Samsung Galaxy TAB S6 che permettono di rilevare con precisione i valori biometrici del **firmatario** che appone la firma. I tablet sono caratterizzati da un ampio display TFT LCD a colori da 10,4" e da una apposita penna attraverso la quale il **firmatario** sottoscrive il documento elettronico visualizzato sul display. Il display del tablet mostra la firma in tempo reale mentre il **firmatario** firma sul display, rendendo l'esperienza del tutto analoga alla scrittura su carta.

Il tablet in generale consente di:

- Prendere visione del documento eseguendo, se necessario, lo "scroll" dello stesso
- Sottoscrivere il documento e confermare la firma apposta
- Cancellare, in caso di errore, la firma apposta per riproporne un'altra
- Annullare l'operazione di firma

Le operazioni di cui sopra sono rese possibili attraverso l'utilizzo di una apposita penna elettronica e di appositi tasti funzione presenti sul display del tablet ed il **firmatario** mantiene sempre il controllo esclusivo del sistema di generazione della firma.

Nel seguito si descrivono le caratteristiche funzionali della soluzione adottata da Casa di Cura Prof. Nobili Srl evidenziando gli aspetti che assicurano il rispetto dei requisiti richiesti dalla normativa alle soluzioni di firma elettronica avanzata, quali:

- La connessione univoca della firma al firmatario;
- Il controllo esclusivo in capo al soggetto sottoscrivente del sistema di generazione della firma;
- La connessione univoca della firma al documento sottoscritto;
- L'immodificabilità ed inalterabilità del documento sottoscritto;
- La possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;

- La connessione univoca della firma al documento sottoscritto

Si descrive di seguito il processo di trattamento e cifratura del dato biometrico e della sua associazione al documento PDF:

- Il tablet è autonomamente dotato di tecnologia grafometrica e non sarà necessario utilizzare apparecchiature esterne per la cattura della firma;
- I dati biometrici della firma acquisititi vengono ricevuti dall'APP. Se si è connessi ad un server l'APP opererà in modalità ON-LINE. Se il documento è stato copiato sul device, l'APP è in grado di operare Off-Line;
- Sul vettore si ricava l'immagine della firma, calcolata a partire dai dati biometrici acquisiti. L'immagine della firma viene integrata nel documento PDF;
- I dati biometrici vengono cifrati asimmetricamente, utilizzando la chiave pubblica fornita dalla CA, ed incorporati nel documento PDF. La coppia di chiavi di cifratura (pubblica/privata) è generata da un Notaio, che conserva, in via esclusiva ed in sicurezza, la chiave privata;
- Un primo hash (HASH1) viene calcolato sul documento. L'HASH1 viene firmato con una chiave privata auto generata (RSA-2048) che, dopo la firma, viene cancellata. Si conserva la corrispondente chiave pubblica;
- L'HASH1 firmato e la relativa chiave pubblica sono incorporati nel documento. Questo permette di proteggere l'HASH1, e garantisce l'integrità del documento con i dati biometrici criptati;
- L'HASH1 viene verificato da Adobe Reader, in grado di controllarne l'integrità;
- Per associare i dati biometrici al documento (document binding) viene utilizzato un secondo hash (HASH2). L'HASH 2 viene calcolato utilizzando un algoritmo SHA 256, calcolato su HASH1 e sui dati biometrici in chiaro;
- L'HASH2 viene salvato nel documento;
- L'HASH2 viene validato dal tool di analisi forense al momento dell'estrazione del vettore biometrico, secondo procedura definita in caso di contenzioso;
- Nel caso in cui il documento PDF abbia "n" firme, il processo viene ripetuto "n" volte;
- Il documento PDF raccolte tutte le firme del cliente, viene sigillato con una firma digitale non qualificata;
- Il documento PDF sigillato viene inviato al server, che chiama il server di firma per apporre una firma digitale qualificata (ed eventualmente una marcatura temporale);

Tutto il processo avviene secondo standard ISO 32000-1.

Si descrive di seguito il processo di acquisizione dei consensi relativi alla Firma Grafometrica (FEA) e successivamente alla costituzione ed alimentazione del Dossier Sanitario Elettronico (D.S.E.)

1) Visualizzazione sul tablet dell'informativa sintetica relativa alla Firma grafometrica (FEA)

2) Visualizzazione sul tablet dell'informativa sintetica relativa alla costituzione del Dossier Sanitario Elettronico (DSE).

3) A seguito dell'avvenuto riconoscimento del firmatario da parte del personale addetto alla procedura, viene chiesto al soggetto interessato di verificare che i dati anagrafici mostrati sulla schermata del tablet siano corretti ed aggiornati e quindi ne viene chiesta la conferma tramite la specifica funzionalità presente nell'App Confirmo.

4) In caso affermativo si procede alla raccolta della firma grafometrica tramite specifica funzione nell'app Confirmo. Nel caso in cui si volesse ripetere la procedura, è possibile farlo mediante l'uso dei pulsanti presenti nella schermata del tablet e quindi ricominciare da capo.

5) Al termine del processo di acquisizione della firma grafometrica si viene passati ad un ulteriore schermata su cui viene proposto di esprimere (negare) il consenso alla costituzione ed alimentazione del Dossier Sanitario Elettronico (DSE) attraverso la selezione delle voci presenti. Il paziente può quindi operare una delle tre possibili scelte offerte: Concedere il consenso, negare il consenso oppure acconsentire sia alla costituzione del DSE con inserimento sullo stesso degli eventi anteriori alla sua costituzione (pregresso).

6) In caso di ripensamento da parte del soggetto interessato è sempre possibile tornare alla gestione dei consensi mediante l'uso dei pulsanti presenti nella schermata del tablet. In tal modo viene garantito il rispetto del requisito richiesto dalle Regole Tecniche all'art. 56 comma 1 lettera c): il controllo esclusivo del firmatario del sistema di generazione della firma;

7) Al termine dell'acquisizione viene predisposto un documento informatico di tipo .pdf che contiene:

   a) Il documento originario con la firma apposta dal sottoscrittore;

   b) L'impronta informatica del documento stesso e la sua cifratura utilizzando la chiave pubblica del certificato crittografico tecnico la cui chiave privata è detenuta dalla Certification Authority Intesa.;

   c) I dati biometrici cifrati in fase di acquisizione della firma utilizzando la chiave pubblica del certificato di cui sopra;

8) Al termine del processo di firma tutti i dati di firma biometrica acquisiti vengono eliminati definitivamente dalla memoria della stazione di lavoro e dal dispositivo di acquisizione della firma.

I clienti che hanno aderito al servizio possono richiedere, in qualsiasi momento e gratuitamente, una copia dell'informativa e del consenso all'uso della firma grafometrica direttamente agli uffici amministrativi della struttura (cfr. DPCM 22-02-2013, art. 57, comma 1, lettera c).

Con analoga modalità possono richiedere, in qualsiasi momento tramite apposito modulo, la revoca della dichiarazione di accettazione tornando quindi ad operare con la tradizionale firma autografa su documentazione cartacea.

Informazioni riguardanti la copertura assicurativa (DPCM 22-02-2013, art. 57, comma 2)

Al fine di proteggere i titolari della Firma Elettronica Avanzata e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche, i soggetti di cui all'articolo 55, comma 2, lettera a) Casa di Cura Prof. Nobili Srl si è dotato di una copertura assicurativa per la Responsabilità Civile rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali per un ammontare non inferiore ad euro cinquecentomila (€ 500.000).
Di seguito i riferimenti della polizza stipulata dalla struttura:

Polizza n. 448751510 emessa da Generali Italia Spa

Castiglione dei Pepoli, 01 Ottobre 2024