Caratteristiche del sistema e delle tecnologie utilizzate per la sottoscrizione di documenti informatici tramite firma grafometrica[1].

1 Cos'è la firma grafometrica?

La Firma Grafometrica è una modalità di sottoscrizione di un documento informatico da parte di un soggetto opportunamente identificato mediante l'apposizione di una normale firma su un dispositivo specializzato (Tablet di firma) con una "penna elettronica" in grado di rilevare i dati della firma del sottoscrittore e associarli al documento informatico (in formato PDF) riprodotto sullo schermo dell'operatore e visibile da parte del sottoscrittore.

La Firma Grafometrica formata nel rispetto delle regole di cui alla normativa di riferimento[2], possiede i requisiti informatici e giuridici che consentono di qualificarla come Firma Elettronica Avanzata (ai sensi dell'art. 1, comma 1°, lett. q-*bis* del Codice dell'Amministrazione digitale).
Il documento informatico sottoscritto con Firma Grafometrica è realizzato in modo tale che vengano garantite:

- l'identificazione del firmatario;
- 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.

Sul piano giuridico 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.

2 Descrizione del sistema e delle tecnologie utilizzate per la firma grafometrica

La descrizione sotto riportata risponde a quanto previsto dalle Regole Tecniche all'art. 57 comma 1 alla lettera e): "*rendere note le caratteristiche del sistema realizzato atte a garantire quanto previsto dall'art. 56, comma 1*..."

Il Sistema di firma grafometrica si compone di elementi software ed hardware e di un processo di acquisizione di firma che è svolto dall'operatore di front-end, in conformità a quanto descritto nel seguito.

[1]Tale descrizione è resa ai sensi dell'art. 57 comma 1 lettere e), f), g) delle Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, pubblicate in G.U. N°117 del 21/05/2013
[2] Le normative di riferimento che regolano la materia sono contenute principalmente nel D.Lgs. n. 82/2005 (Codice dell'Amministrazione Digitale) e nel DPCM. del 22.03.2013.

2.1 Il software

Il software utilizzato è Scryba Sign realizzato da Medas, al quale è associato Biosign (componente client installata sulle singole postazioni di raccolta della firma grafometrica e che serve a raccogliere e cifrare in modo sicuro i dati biometrici).
L'interfacciamento tra Scryba Sign e Biosign avviene tramite il componente Medas Device Manager installato sulla postazione.

La soluzione si basa sul concetto fondamentale per cui la firma grafometrica è costituita non solo dal glifo (tratto) fine a se stesso ma anche da un insieme di parametri biometrici fondamentali ad 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:

- è prodotta personalmente da un comune cittadino, di proprio pugno, senza bisogno di alcun dispositivo personale e mediante un hardware di acquisizione (tavoletta) reso disponibile direttamente nell'ambito della soluzione;
- è automaticamente collegata al documento oggetto della firma
- è criptata tramite opportuna chiave pubblica (la componente privata è denominata Medas Masterkey) per renderla inviolabile da parte di chiunque;
- è integrata nel documento sotto forma di una firma digitale standard PAdES, cosicchè qualunque copia di Adobe Reader o di altro software compatibile con il formato PDF e con la firma PAdES possa visualizzarla;
- è corredata di elementi aggiuntivi opzionali richiesti dalla normativa per soddisfare i requisiti della FEA: copia del documento di identità, firma digitale dell'operatore che cura l'esecuzione della firma;

Il documento così confezionato è perfettamente auto consistente, fruibile con strumenti standard e di pubblico dominio, 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.

2.2 L'hardware

L'hardware utilizzato è composto da:

- un server locale,
- Postazioni di Lavoro comprensive di scanner per l'acquisizione del documento di identità dell'utente (attività necessaria una tantum al momento di accettazione del servizio di Firma grafometrica) e/o tavolette di firma con schermo sensibile direttamente connesse alla stazione di lavoro o Tablet con schermo sensibile.

2.3 Trattamento dei dati biometrici della firma

La soluzione proposta dalla Fondazione IRCCS Istituto Nazionale dei Tumori Milano per la sottoscrizione dei documenti informatici tramite l'acquisizione su tavoletta della firma autografa assicura l'impossibilità di acquisizione e riutilizzo dei dati di firma biometrica al di fuori del processo di firma specifico.
Particolari precauzioni tecniche sono state infatti adottate per garantire che in alcuna fase del processo di acquisizione ed abbinamento "documento-firma" i dati biometrici possano essere acquisiti in modo fraudolento e senza la volontà del sottoscrittore. Infatti:

a) lo scambio dei dati di firma tra la tavoletta con schermo sensibile e la stazione di lavoro che gestisce l'associazione documento-firma, avviene in modalità sicura (anti sniffing) cifrando i dati di firma utilizzando un algoritmo AES> a doppia chiave simmetrica RSA 2048 bit ed algoritmo di cifratura SHA256.
b) i dati di firma biometrica vengono immediatamente cifrati con chiave pubblica utilizzando il certificato di firma rilasciato alla Fondazione IRCCS Istituto Nazionale dei Tumori Milano di cui al precedente paragrafo, rendendo impossibile quindi il loro utilizzo in chiaro per sottoscrivere altri documenti.
c) 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 dalla Rete di Notai Biosign, rete di 14 notai appositamente costituitasi per la detenzione, conservazione e gestione delle chiavi private legate alla procedura MedAgree e che è autorizzato a decifrare i dati di firma esclusivamente su mandato dell'autorità giudiziaria.

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.

3 Il processo di firma dei documenti informatici

Nel seguito si descrivono le caratteristiche funzionali della soluzione adottata dalla Fondazione IRCCS Istituto Nazionale dei Tumori Milano 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.

Il processo di firma (o sottoscrizione) informatica prevede le seguenti fasi:

1. Identificazione certa dell'utente firmatario, come previsto dalle Regole Tecniche all'art. 57 comma 1 alle lettere a): *identificare in modo certo l'utente tramite un valido documento di*

riconoscimento..., con successiva acquisizione e registrazione dei dati anagrafici, dei dati relativi al Documento di Identità e con acquisizione digitale, tramite scansione, del Documento di Identità stesso;

2. Visualizzazione su apposito video del documento che il sottoscrittore dovrà firmare con indicazione dell'area (o delle aree) su cui verrà apposta la firma autografa una volta eseguita sul terminale di firma;
3. Apposizione, su richiesta dell'operatore, da parte dell'assistito della propria firma sul terminale, con conferma finale tramite pressione del tasto "OK" che compare sul terminale di firma stesso. Nel caso in cui si volesse ripetere la sottoscrizione, è possibile procedere facendo pressione sul tasto "Annulla" e ripetere l'apposizione di una nuova firma sul 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;*
4. Una volta premuto il tasto "OK", il sistema acquisisce il profilo della firma e le sue caratteristiche biometriche e visualizza il documento con la firma del sottoscrittore nell'area prevista; in tal modo garantendo quanto richiesto nelle Regole Tecniche all'art. 56 comma 1 lettera e): *possibilità del firmatario di ottenere evidenza di quanto sottoscritto;*
5. 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 di firma rilasciata alla Fondazione IRCCS Istituto Nazionale dei Tumori Milano dalla società **Aruba S.p.A.** iscritta nell'elenco dei certificatori presso l'Agenzia per l'Italia Digitale,
    c) i dati biometrici cifrati in fase di acquisizione della firma utilizzando la chiave pubblica del certificato di cui sopra.

    Questo procedimento permette quindi di adempiere a quanto previsto dalle Regole Tecniche all'art. 56 comma 1 alle lettere a): *identificazione del firmatario del documento* e b): *connessione univoca della firma al firmatario* ed h): *la connessione univoca della firma al documento informatico*;
6. Il documento informatico così prodotto può essere stampato e rilasciato al sottoscrittore su sua specifica richiesta per poi essere successivamente avviato al processo di conservazione a norma di legge secondo quanto previsto dalla Deliberazione CNIPA (ora Agenzia per l'Italia Digitale) n. 11/2004 del 19 febbraio 2004 "*Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali*" e s.m.i., soddisfacendo quindi quanto previsto dalle Regole Tecniche all'art. 56 comma 1 alla lettera d) *: la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma*;
7. Al termine del processo di firma tutti i dati di firma biometrica acquisiti vengono cancellati dalla memoria della stazione di lavoro e dalla tavoletta di firma.