Descrizione delle caratteristiche del sistema e delle tecnologie utilizzate nell'ambito del Servizio di Firma Elettronica Avanzata erogato da Humanitas

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

Il presente documento è redatto ai sensi del decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 recante "Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli…omissis…" (in seguito DPCM 22.02.2013), in particolare ai sensi dell'art. 57, comma 1, lettere e) ed f) che stabilisce a carico di chi eroga il servizio, in particolare di Humanitas di:

e) rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'art. 56, c. 1;
f) specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto.

Ai sensi dell'art. 57, c.1, lettera g), Humanitas si impegna a pubblicare il presente documento sul sito aziendale (http://www.humanitas.it).

In particolare, Humanitas intende offrire ai suoi pazienti (di seguito FIRMATARI) la possibilità di sottoscrivere elettronicamente documenti informatici (quali a mero titolo di esempio, non esaustivo: il consenso al portale "Humanitas con Te", i consensi relativi a specifici trattamenti sanitari) in due modalità:

a) in modo autonomo tramite il portale "Humanitas con Te", accessibile on line; le firme elettroniche in questo caso potranno essere apposte utilizzando un certificato di Firma Elettronica Avanzata basata su un'infrastruttura a chiave pubblica (di seguito FEA PKI);
b) tramite operatore nel caso di documenti informatici generati durante i percorsi assistenziali svolti all'interno della struttura sanitaria; le firme elettroniche in questo caso potranno essere apposte utilizzando la Firma Elettronica Avanzata Grafometrica (di seguito FEA GFM).

Nel seguito si descrivono nel dettaglio le caratteristiche e le tecnologie usate distinguendole in due capitoli:

- Firma Elettronica Avanzata PKI (FEA PKI);
- Firma Elettronica Avanzata Grafometrica (FEA GFM).

FIRMA ELETTRONICA AVANZATA PKI (FEA PKI)

DESCRIZIONE DEL SISTEMA

In questo paragrafo si illustra come il sistema ottemperi a quanto previsto dall'art. 56, c. 1 del DPCM 22.02.2013.

Di seguito si descrivono puntualmente le caratteristiche del sistema in relazione ad ogni punto del suddetto articolo.

- **Identificazione del Titolare di firma** (di seguito FIRMATARIO) (art. 56, c. 1, lettera a) del DPCM 22.02.2013).

  L'identificazione del FIRMATARIO è garantita dalla procedura di identificazione del FIRMATARIO allo sportello di Humanitas che prevede le seguenti attività:

  - presenza fisica del FIRMATARIO presso uno sportello di Humanitas;
  - identificazione de visu del FIRMATARIO da parte dell'Operatore di Registrazione (di seguito OdR) di Humanitas, adeguatamente formato e certificato da Humanitas;
  - presentazione al FIRMATARIO delle condizioni e limiti d'uso del Servizio di FEA PKI da parte dell'OdR;
  - manifestazione da parte del FIRMATARIO all'OdR del consenso orale al Servizio di FEA PKI;
  - raccolta dei dati personali del FIRMATARIO da parte dell'OdR;
  - scansione (copia per immagine di documento analogico) di un valido documento d'identità del FIRMATARIO da parte dell'OdR;
  - sottoscrizione con Firma Digitale Remota (FDR) da parte dell'OdR della "Dichiarazione di accettazione delle condizioni del Servizio di FEA PKI" in cui viene verbalizzata l'acquisizione del consenso orale alla FEA PKI e nel quale sono allegate copia del documento d'identità e l'informativa;

- **Connessione univoca della firma al FIRMATARIO** (art. 56, c. 1, lettera b) del DPCM 22.02.2013).

  L'associazione del Firmatario alla firma è garantita dal Certificato X509, che ha come titolare il FIRMATARIO stesso;

- **Controllo esclusivo in capo al FIRMATARIO del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima** (art. 56, c. 1, lettera c) del DPCM 22.02.2013). Il controllo esclusivo del certificato di FEA PKI da parte del Firmatario è garantito da un meccanismo di autenticazione forte (Strong Authentication), necessario per accedere al certificato al fine di sottoscrivere documenti informatici. Il meccanismo di autenticazione forte è basato su una password (Personal Identification Number: PIN OTP) digitata dal FIRMATARIO durante la procedura di generazione del certificato e da un codice variabile ad ogni accesso (One Time Password: OTP);

- **Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma** (art. 56, c. 1, lettera d) del DPCM 22.02.2013). I documenti informatici sottoscritti con la soluzione Scryba Sign e certificato di FEA PKI hanno il formato PAdES (conforme alla specifica pubblica ETSI TS 102 778 e alla normativa comunitaria). I documenti sottoscritti con questo formato sono standard e indipendenti dalla piattaforma Scryba Sign; essi sono visualizzabili e verificabili con l'applicazione Acrobat Reader che consente anche di visualizzare gli attributi del certificato di firma; ovviamente la verifica darà evidenza che il certificato utilizzato è emesso da CA non qualificata essendo appunto una FEA e non una Firma Digitale o Firma Elettronica Qualificata;
- **Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto** (art. 56, c. 1, lettera e) del DPCM 22.02.2013). Ogni documento informatico sottoscritto dal FIRMATARIO con la FEA PKI è accessibile e visualizzabile sul portale "Humanitas con te".
- **Individuazione del Soggetto che eroga le soluzioni di Firma Elettronica Avanzata** (art. 56, c. 1, lettera f) del DPCM 22.02.2013). Il soggetto che eroga il servizio di FEA PKI è Humanitas che si avvale della soluzione tecnologica realizzata dalla Società Medas srl di Milano. L'evidenza dell'identificazione del soggetto erogatore è garantita dal fatto che i certificati sono generati istanziando l'attributo 'Organizzazione' con il valore: "Istituto Clinico Humanitas ";
- **Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati** (art. 56, c. 1, lettera g) del DPCM 22.02.2013). Il documento informatico prodotto da Humanitas e sottoposto al FIRMATARIO per le sottoscrizioni mediante FEA PKI è privo di elementi dinamici come macro istruzioni o codice eseguibile e quindi soddisfa quanto stabilito nella norma;
- **Connessione univoca della firma al documento sottoscritto** (art. 56, c. 1, lettera h) del DPCM 22.02.2013). Il formato PAdES con cui sono sottoscritti tutti i documenti informatici include l'impronta del documento stesso sottoscritta con il certificato FEA PKI del FIRMATARIO garantendo che la sottoscrizione apposta sia univocamente connessa al documento sottoscritto.

DESCRIZIONE DELLE TECNOLOGIE

In questo paragrafo vengono descritte le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto, in conformità all'art. 57, comma 1, lettera f) del DPCM 22.02.2015.

La soluzione Scryba Sign

Il sistema che gestisce la FEA PKI è basato sulla soluzione informatica denominata "Scryba Sign" prodotta dalla società Medas srl di Milano. Scryba Sign per la gestione della FEA PKI utilizza certificati X509 non qualificati rilasciati da un suo modulo "CA". La soluzione interagendo con le altre componenti di seguito descritte assicura il pieno rispetto dei requisiti di sicurezza richiesti dalla normativa sulla FEA.

Architettura del sistema Scryba Sign

Il sistema Scryba Sign è lo strumento che gestisce due macro funzionalità:

A) generazione dei certificati FEA PKI associati ad un FIRMATARIO;

B) sottoscrizione dei documenti informatici con firma FEA PKI.

A) Componenti di Scryba Sign dedicate alla generazione dei certificati FEA PKI associati ad un FIRMATARIO

Scryba Sign quando espleta le funzioni di generazione dei certificati utilizza le seguenti componenti:

- Modulo web services che integra l'anagrafica dei pazienti di Humanitas per consentire di inserire i dati personali dei FIRMATARI senza doverli reinserire manualmente evitando così anche errori di disallineamento tra i dati presenti nell' Anagrafica Humanitas e dati riportati nel certificato X509 FEA PKI;
- Generazione di certificati X509 non qualificati generati dal modulo "Scryba Sign CA";
- Database dei firmatari utilizzato anche per l'archiviazione dei certificati FEA PKI in modalità cifrata;

B) Componenti di Scryba Sign dedicate alla sottoscrizione dei documenti informatici con firma FEA PKI

Scryba Sign quando espleta le funzioni di sottoscrizione dei documenti informatici utilizza le seguenti componenti:

- Modulo software che interfaccia le varie applicazioni che producono documenti informatici che devono essere sottoscritti con firma FEA PKI (queste applicazioni sono chiamate "producer"); questo modulo consente attraverso delle specifiche web services alle applicazioni informatiche utilizzate da HUMANITAS di poter inviare a Scryba Sign documenti informatici affinché essi vengano sottoscritti con una firma FEA PKI da parte del FIRMATARIO;
- Modulo di verifica poteri di firma. Una volta ricevuti i documenti da firmare Scryba Sign, attraverso questo modulo, verifica che il firmatario sia dotato di un certificato di firma FEA PKI valido e che egli abbia il potere di firma idoneo; Scryba Sign infatti nella registrazione del FIRMATARIO nel proprio database identifica anche quali documenti egli possa sottoscrivere; il potere di firma opera in base alla tipologia dei documenti e alla loro provenienza;
- Modulo di sottoscrizione dei documenti informatici; questo modulo interagendo con l'applicazione chiamante chiede al FIRMATARIO di introdurre le proprie credenziali forti: password di firma (detta "PIN OTP") e codice variabile (detto "OTP": One Time Password); Il PIN OTP è quello inserito direttamente dal FIRMATARIO in fase di registrazione mentre l'OTP viene generato ad ogni accesso ed è trasmesso al FIRMATARIO tramite sms o tramite specifici token connessi tramite porte usb o non connessi (dotati di un piccolo display dove compare il codice). Dal punto di vista tecnico l'identificazione forte utilizza lo standard OATH per la generazione degli OTP. Solo dopo che il firmatario si è identificato allora Scryba Sign può utilizzare il suo certificato per la sottoscrizione del documento informatico ricevuto.

FIRMA ELETTRONICA AVANZATA GRAFOMETRICA (FEA GFM)

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 (D.Lgs. n. 82/2005 – Codice dell'Amministrazione Digitale e nel DPCM 22-02-2013), 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.

2.1 Il software

Il software utilizzato è Scryba Sign realizzato da Medas, al quale è associato il modulo software 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 software 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 sé stesso 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:

- è prodotta personalmente da un 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, cosicché 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,
- Postazione di identificazione (possono essercene più d'una)
  - un PC con monitor (postazione di lavoro) con connesso
    - uno scanner per l'acquisizione del documento di identità dell'utente (attività necessaria una tantum al momento di accettazione del servizio di Firma grafometrica),
- Postazione di firma con FEA GFM - Fissa (possono essercene più d'una)
  - un PC con monitor (postazione di lavoro) con connesso

- una tavoletta di firma con schermo sensibile prodotta dalla società Wacom Co., Ltd., modello STU-530 (o similari equivalenti) direttamente connesse alla postazione di lavoro. Per maggiori informazioni tecniche sulle caratteristiche della tavoletta Wacom accedere al sito: https://www.wacom.com .

- Postazione di firma con FEA GFM - Mobile (possono essercene più d'una)
  - un tablet Microsoft Surface (o modelli similari equivalenti) con schermo sensibile alla pressione. Per maggiori dettagli si rimanda al sito: https://www.microsoft.com .

2.3 Trattamento dei dati biometrici della firma

La soluzione proposta da Humanitas per la sottoscrizione dei documenti informatici con FEA 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 nessuna 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 Wacom (o tablet Microsoft Surface) e la postazione di lavoro che gestisce l'associazione documento-firma, avviene in modalità sicura (anti sniffing) cifrando i dati di firma utilizzando un algoritmo AES (Advanced Encryption Standard) a doppia chiave simmetrica RSA 2048 bit ed algoritmo di cifratura SHA256.
b) i dati di firma biometrica vengono immediatamente cifrati con crittografia asimmetrica con chiave pubblica utilizzando il certificato di firma rilasciato a Humanitas, 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, utilizzabili solo esclusivamente su mandato dell'autorità giudiziaria.

L'ambiente in cui tali dati verranno resi disponibili risulta "protetto" garantendo che a seguito della decifratura, strettamente finalizzata alla perizia calligrafica, i dati non 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 da Humanitas 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 a Humanitas dalla società Medas srl su certificato di 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 è accessibile al cittadino via internet tramite il portale "Humanitas con Te". Inoltre il documento informatico viene successivamente avviato al processo di conservazione a norma secondo quanto previsto dal DPCM 03-12-2013 (Regole tecniche in materia di sistema di conservazione […]) 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.

Rozzano (MI), 30 aprile 2020