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

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 del gruppo Alliance Medical di:

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

Ai sensi dell'art. 57, c.1, lettera g), Il gruppo Alliance Medical si impegna a pubblicare il presente documento sul sito aziendale (www.alliancemedical.it).

In particolare, Il gruppo Alliance Medical 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 **TuoDossier**) in due modalità:

a) in modo autonomo tramite il portale **TuoDossier**, 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 di Registrazione (di seguito OdR) 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).

Nelle pagine che seguono si descrivono nel dettaglio le caratteristiche e le tecnologie usate distinguendole in due capitoli:

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

[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

FIRMA ELETTRONICA AVANZATA GRAFOMETRICA (FEA GFM)

1. Cos'è la firma elettronica avanzata grafometrica (di seguito FEA GFM)?

La FEA GFM 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'OdR e visibile da parte del sottoscrittore.

La FEA GFM 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 FEA GFM è realizzato in modo tale che vengano garantite:

- l'identificazione del firmatario;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
- la connessione univoca della firma al documento sottoscritto;
- l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati;
- la possibilità per il firmatario di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- l'individuazione del soggetto che eroga soluzioni di FEA al fine di utilizzarla nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali.

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

Il sistema di FEA GFM si compone di elementi software e hardware e di un processo di acquisizione di firma che è svolto dall' OdR, in conformità a quanto descritto nel seguito.

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 FEA GFM 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 FEA GFM è costituita non solo dal glifo (tratto) fine a sé 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 FEA GFM 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, 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' OdR 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] 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 22.02.2013.

2.2. L'hardware

L'hardware utilizzato è composto da:

- un server locale;
- un PC con monitor 20" incorporato;
- uno scanner per l'acquisizione del documento di identità dell'utente (attività necessaria una tantum al momento di accettazione del servizio di FEA GFM);
- una tavoletta di firma con schermo sensibile prodotta dalla società **Wacom**, modello DTU -1141B, direttamente connesse alla stazione di lavoro. Per maggiori informazioni tecniche sulle caratteristiche della tavoletta di firma accedere al link: https://www.wacom.com/it-it/for-business/products/pen-display-dtu-1141.

2.3. Trattamento dei dati biometrici della firma

La soluzione proposta da ciascuna società del gruppo Alliance Medical che ha attivato la FEA GFM (di seguito AZIENDA) 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 all'AZIENDA 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

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' OdR, 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 firmatario;
    b. l'impronta informatica del documento stesso e la sua cifratura utilizzando la chiave pubblica del certificato di firma rilasciata all'AZIENDA 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*;

Qualora il firmatario aderisse all'attivazione del portale **TuoDossier** avrà a disposizione sullo stesso portale tutta la documentazione da lui sottoscritta (sia in accettazione che da remoto). Diversamente, qualora il firmatario non aderisse all'attivazione del portale **TuoDossier** riceverà tramite e-mail i documenti relativi alla FEA sottoscritti in accettazione.

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.

FIRMA ELETTRONICA AVANZATA PKI (FEA PKI)

1. Cos'è la firma elettronica avanzata PKI (di seguito FEA PKI)?

La FEA PKI (Public Key Infrastructure) è un tipo di firma digitale che utilizza un'infrastruttura a chiave pubblica per garantire l'autenticità, l'integrabilità e la non ripudiabilità di documenti e comunicazioni elettroniche. Questa tecnologia si basa su un sistema crittografico asimmetrico che utilizza una coppia di chiavi: chiave pubblica e chiave privata.

La chiave privata è conosciuta solo dal proprietario e viene utilizzata per creare la firma digitale. La chiave pubblica è distribuita pubblicamente e viene utilizzata per verificare la firma.

La FEA PKI , formata nel rispetto delle regole di cui alla normativa di riferimento[3], permetterà all'utilizzatore di sottoscrivere documenti informatici garantendo:

- l'identificazione del firmatario;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma;
- la connessione univoca della firma al documento sottoscritto;
- l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati;
- la possibilità per il firmatario di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- l'individuazione del soggetto che eroga soluzioni di FEA al fine di utilizzarla nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali.

2. Descrizione del sistema e delle tecnologie utilizzate per la FEA PKI

Il sistema di FEA PKI si compone di elementi software e hardware e di un processo di acquisizione di firma che è svolto dall' OdR, in conformità a quanto descritto di seguito. Il sistema che gestisce la FEA PKI è basato sulla soluzione informatica denominata **Scryba Sign** prodotta dalla società Medas S.r.l. 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.
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 del gruppo Alliance Medical 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 del gruppo Alliance Medical 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 dal gruppo Alliance Medical 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 "Password") e codice variabile temporaneo (detto

[3] 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 22.02.2013.

"OTP": One Time Password); La Password è quello impostata direttamente dall'OdR in fase di registrazione del paziente mentre l'OTP viene generato ad ogni accesso ed è trasmesso al firmatario tramite SMS.
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 Scryba Sign può utilizzare il suo certificato per la sottoscrizione del documento informatico ricevuto.

3. Processo di firma dei documenti informatici

Il processo di firma (o sottoscrizione) informatica prevede le seguenti fasi tutte di responsabilità del Firmatario:

1. **Ricezione credenziali d'accesso al portale TuoDossier**: Dopo aver espresso il consenso orale all'adesione alla FEA PKI e aderito all'attivazione del portale in accettazione, il firmatario riceve dall'OdR le istruzioni e le modalità con cui collegarsi al portale **TuoDossier**;
2. **Accesso al portale TuoDossier**: Il firmatario accede al portale con l'Username (codice fiscale) e la Password (ricevuta via SMS al momento dell'adesione al servizio) e l'OTP ricevuto via SMS al momento dell'accesso al portale;
3. **Identificazione documento da firmare**: Il firmatario identifica un documento informatico da firmare (es.: un nuovo consenso inserito in accettazione);
4. **Applicazione della FEA PKI sul documento**: Il firmatario utilizza l'apposito comando per firmare il documento inserendo le credenziali di firma, tra cui la Password ricevuta in fase di adesione al servizio, e l'OTP ricevuto al momento della firma;
5. **Verifica sottoscrizione documento**: Il firmatario verifica sul portale l'esito positivo dell'operazione di firma appena effettuato, constatando che il documento precedentemente selezionato risulti ora sottoscritto.