Descrizione delle caratteristiche del sistema e delle tecnologie utilizzate nell'ambito del Servizio di Firma Elettronica Avanzata basata su un'infrastruttura a chiave pubblica (FEA PKI) 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.

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

Humanitas intende offrire ai propri pazienti la possibilità di usufruire di un servizio di firma elettronica avanzata che consenta loro di sottoscrivere documenti informatici relativi ai rapporti con Humanitas stessa. A titolo esemplificativo, ma non esaustivo, con tale firma i pazienti (di seguito FIRMATARI) potranno sottoscrivere i consensi in formato elettronico al dossier 'Humanitas con te", il portale di Humanitas, che consente ai cittadini di accedere ai propri documenti informatici clinici (referti e immagini).

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 di Servizio di FEA PKI" in cui viene verbalizzata l'acquisizione del consenso orale 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;
- **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, la quale a sua volta utilizza certificati X509 non qualificati generati da Aruba PEC S.p.A. 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 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 sono descritte di seguito 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 dalla società Aruba PEC spa. 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;
- Interfaccia con CA Aruba PEC tramite utilizzo di web services specifiche che consentono l'enrollment di certificati X509 non qualificati generati da Aruba PEC;
- 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 che devono essere sottoscritti con firma FEA PKI (queste applicazioni sono chiamate "producer"); questo modulo consente attraverso delle specifiche web services alla applicazioni informatiche utilizzate da HUMANITAS di poter

inviare a Scryba Sign documenti informatici affinché ad essi sia sottoposta 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.