UNIVERSITA' POLITECNICA DELLE MARCHE
Facoltà di Medicina e Chirurgia

Corso di Laurea Magistrale in:
SCIENZE DELLE PROFESSIONI SANITARIE
TECNICHE DIAGNOSTICHE

Tesi di Laurea:

Consensi informati dematerializzati: il progetto della Radiologia dell'ASUR Area Vasta 2

Candidato:
Dott. Ciriaci Damiano

Relatore:
Prof. La Riccia Luigi

Correlatore:
Prof. Olivi Emmanuele

Anno Accademico 2021-2022

Introduzione

Tutto l'universo della comunicazione nell'era della globalizzazione è stato fortemente influenzato dall'intervento di novità tecniche che hanno rivoluzionato le caratteristiche sia delle modalità operative, sia dei valori e degli aspetti culturali.

Le nuove tecnologie della comunicazione costituiscono uno degli elementi centrali della globalizzazione, perché contribuiscono alla diffusione del sapere aumentando le capacità e le qualità delle tecniche di trasmissione delle informazioni.

La società, nella quale oggi viviamo, è caratterizzata dall'affermarsi dell'informatica e dalla diffusione delle nuove tecnologie telematiche che, grazie all'uso sempre più ampio dei nuovi media comunicativi, del computer, dello Smartphone e soprattutto di Internet (che si è rilevato l'elemento chiave), possono mettere in contatto tutti, in qualsiasi momento e in ogni luogo.

In diagnostica per immagini questa rivoluzione ha avuto inizio negli ultimi decenni del secolo scorso con lo sviluppo di tecniche diagnostiche computerizzate e digitali, fino all'informatizzazione di tutti processi e alla raccolta di dati e informazioni inerenti tutta l'attività. Successivamente il cambiamento è progredito con la creazione e la progressiva integrazione dei documenti clinici del singolo paziente in un unico sistema, nonché con il fascicolo sanitario elettronico (FSE). L'introduzione della ricetta elettronica in molte regioni italiane porterà nel giro di poco tempo all'eliminazione del corrispettivo documento cartaceo.

La dematerializzazione del consenso informato (CI), rappresenta un ulteriore passo verso la completa dematerializzazione dei documenti prodotti in ambito sanitario.

Il CI costituisce il fondamento della liceità dell'attività sanitaria, in assenza del quale l'attività stessa costituisce reato. In considerazione dell'importanza legale del documento, è sicuramente necessario strutturare un processo che definisca l'interazione medico/paziente in maniera conforme ai requisiti

legislativi e tecnologici necessari per la sua implementazione.

Gli attuali sistemi RIS (Radiology Information System) possono gestire/archiviare una moltitudine di dati, nonché interconnettersi ai vari sistemi ospedalieri ed anagrafiche centralizzate per l'acquisizione, la verifica e l'autenticità dei dati.

Nelle nostre realtà siamo già ad un livello tale per cui tutti i referti prodotti dai sistemi RIS vengono firmati digitalmente dal Medico Radiologo e rispondono alle attuali leggi in materia.

L'obiettivo di questo lavoro è la definizione di un progetto per la dematerializzazione del Consenso Informato nell'ambito della Diagnostica per Immagini. Si vuole perseguire inoltre l'acquisizione e l'archiviazione del consenso firmato elettronicamente dal cittadino, al fine di una maggiore semplificazione, di una rapida consultazione e conseguente abbandono degli archivi cartacei, che hanno elevati costi in termini materiali e di spazio nonché di gestione. La consultazione nel tempo risulterebbe inoltre difficoltosa.

Verrà descritto lo stato dell'arte nell'Area Vasta di riferimento. Successivamente, in base alle normative attuali e ai dati clinici necessari, verrà delineato un progetto per la completa dematerializzazione dei consensi impiegati nella Diagnostica per Immagini nell'intera Area Vasta 2, partendo dall'utilizzo di modelli univoci di consenso informato per tutti i Presidi Ospedalieri fino all'acquisizione elettronica e alla successiva archiviazione.

1. ***Il Consenso Informato***

Siamo sempre più consapevoli che qualsiasi accertamento diagnostico non possa essere effettuato senza il valido consenso della persona interessata e che il paziente debba ricevere idonee informazioni in ordine all'esame cui sarà sottoposto, anche in relazione ai rischi medico–legali e quindi alle implicazioni assicurative che ne potrebbero derivare.

Il Consenso Informato è un obbligo contrattuale e la violazione del dovere d'informazione dà luogo a precise responsabilità (Legge 145, 28 marzo 2001 – La Convenzione di Oviedo dedica alla definizione del consenso il capitolo 2, art. da 5 a 9, in cui stabilisce, come regola generale che: "*un intervento, nel campo della salute, non può essere effettuato se non dopo che la persona interessata abbia dato consenso libero e informato. Questa persona riceve innanzitutto una informazione adeguata sullo scopo e sulla natura dell'intervento e sulle conseguenze e i suoi rischi. La persona interessata può in qualsiasi momento, ritirare liberamente il proprio consenso"* Si ricorda inoltre che il Codice Penale fa riferimento alla necessità di munirsi in via preventiva del consenso del paziente. L'Art. 50 infatti recita: "Non è punibile chi lede o pone in pericolo un diritto con il consenso della persona che può validamente disporne".

1.1 Legge 24/17 Gelli-Bianco – Consenso Informato Medico

Il consenso informato è definito e disciplinato, per la prima volta in Italia, dalla legge 219/17 (c.d. Legge "Gelli-Bianco") contenente "Norme in materia di consenso informato e di disposizioni anticipate di trattamento" (detta anche legge sul Biotestamento). In tale legge sono normati tutti gli aspetti procedurali del consenso informato, e sono indicati i 3 attori di tale processo:

- pazienti,
- équipe medica,
- struttura sanitaria.

Il Consenso Informato medico è il processo con cui il paziente decide in modo libero e autonomo, dopo che gli sono state presentate una serie di informazioni specifiche rese a lui comprensibili da parte del medico o equipe medica, se iniziare o proseguire il trattamento sanitario previsto (legge 219/17, art.1 commi 2,3).

Con "acquisizione del consenso informato" possiamo intendere l'espressione, da parte del paziente, dell'assenso (completo o parziale), dissenso o revoca, relativo a quanto proposto dallo Specialista, a conclusione dell'intero percorso di consenso informato. Tale acquisizione è solitamente una firma del paziente, ma la legge 219/17 prevede anche altre modalità, al fine di permettere l'espressione anche da parte di pazienti che siano inabili a firmare. La legge 219/17 identifica le due componenti del Consenso Informato in ambito sanitario:

- le informazioni;
- il processo con cui sono rese comprensibili e utili al paziente.

La legge 219/17 chiarisce inoltre:

- chi deve fornire le informazioni (ovvero l'equipe medica);
- chi si occupa della loro proposta al paziente (ovvero la struttura sanitaria).

1.1.1 Obbligo della Struttura: le informazioni

Le informazioni del consenso informato sono obbligo preciso della Struttura sanitaria (L.219/17, art. 1 comma 9). Le informazioni che il paziente deve comprendere, esplicitate nel terzo comma della L.219/17, riguardano:

- diagnosi,
- prognosi,
- benefici e rischi degli accertamenti diagnostici e dei trattamenti sanitari indicati,
- benefici e rischi delle possibili alternative agli accertamenti diagnostici e ai trattamenti sanitari indicati,
- conseguenze dell'eventuale rifiuto/rinuncia.

Chi redige un consenso informato ha un compito complesso perché deve tener conto di caratteristiche molto specifiche.

Gli elementi essenziali sono la chiarezza e la comprensibilità.

Inoltre deve essere completo, dettagliato e aggiornato. La normativa prevede che sia personale e specifico, contenente i dettagli e le particolarità del caso in esame.

Da quanto previsto nella legge 219/17, si nota che, per un adeguato consenso informato da parte del paziente, devono essere fornite 4 diverse tipologie di informazioni:

- informazioni dello specifico paziente (diagnosi),
- informazioni relative ai trattamenti individuati dal Medico come più utili al paziente,
- informazioni relative alle alternative,
- informazioni aggiuntive (probabile prognosi, conseguenze del rifiuto/revoca, eventuali indicazioni per l'assistenza psicologica prevista dall'art. 1 comma 5).

Gran parte di queste informazioni derivano dalle linee guida di cui alla legge 24/17, elaborate dalle società medico-scientifiche per ciascun trattamento e/o accertamento sanitario.

1.1.2 Obbligo del Medico

L'obbligo del Medico è di rendere comprensibili e utili le informazioni, affinchè siano utili al paziente per esprimere la propria decisione in maniera autonoma (l.219/17, art. 1 comma 2). Questo obbligo è compito e responsabilità specifica dell'équipe medico-sanitaria (legge 219/17, articolo 1, comma 2 e 10). Chi può dare il consenso informato?

Chiunque sia il diretto interessato di un atto medico, se maggiorenne, cosciente e capace, deve dare il proprio consenso al personale sanitario perché possa agire legittimamente.

Dato che si tratta di una manifestazione di volontà libera e consapevole, alcuni soggetti possono non essere nelle condizioni di soddisfare questi requisiti. Non si fa distinzione tra minorenni, interdetti e inabilitati, si parla generalmente di pazienti incapaci. Il paziente incapace "*deve ricevere*

informazioni sulle scelte relative alla propria salute in modo consono alle sue capacità per essere messo nelle condizioni di esprimere la sua volontà", come si evince nell'art. 3 comma 1.

Fermo restando quanto sopra, il consenso informato dal paziente incapace, sia esso interdetto o inabilitato, viene espresso dal tutore o dalla medesima persona inabilitata. Talvolta, da un amministratore di sostegno se la nomina prevede "l'assistenza necessaria o la rappresentanza esclusiva in ambito sanitario" (nell'art.3 comma 1, 219 del 2017). Le parti nominate nella procura per l'assistenza sanitaria hanno il titolo per operare nell'interesse della persona che rappresentano.

1.1.3 Quando serve il consenso informato?

Il consenso informato serve a rendere lecito un determinato atto sanitario, in assenza del quale si ricade nel reato.

È obbligatorio per il medico informare e acquisire il consenso del paziente prima della prestazione sanitaria. I tempi e le modalità devono permettere alla persona assistita di riflettere sulle informazioni ricevute, anche se esistono alcune eccezioni ben definite.

Non serve ottenere il consenso nelle situazioni di estrema urgenza che richiedono l'immediato intervento, ad esempio in condizioni che mettono a rischio di vita il paziente, perché si opera in ambito di "consenso presunto". Lo stesso vale quando si effettuano cure di routine, come ad esempio i prelievi ematici, in quanto si opera secondo "consenso implicito".

1.1.4 Consenso informato - Comunicazione

Nella maggior parte dei casi, il consenso informato scritto è quello che viene più spesso sottoposto ai pazienti. Sono previste forme alternative di comunicazione se coloro che devono esprimere il consenso sono persone impossibilitate a leggere o firmare. Le videoregistrazioni sono piuttosto diffuse ma sono ammessi anche altri dispositivi particolari che permettano una documentazione.

Questo processo è il cuore del nuovo consenso informato. Si tratta infatti del momento chiave che permette sia di instaurare un clima di fiducia tra medico/équipe sanitaria e quel dato paziente, sia di iniziare un efficace

coinvolgimento della persona nel suo proprio percorso terapeutico, cioè di avviare la “relazione di cura” in cui il paziente è soggetto attivo. Rendere comprensibili le informazioni diventa la chiave per porre il consenso informato alla base della “relazione di cura e di fiducia tra paziente e medico” (legge 219/17, art. 1, comma 2).

1.1.5 La tutela dell’articolo 32 della Costituzione

L’articolo 32 della Costituzione italiana riguarda la tutela della salute, uno dei diritti fondamentali della persona.

Il termine salute indica certamente assenza di malattia, ma più ampiamente va inteso come uno stato di benessere psichico e fisico.

Tuttavia, lo stesso articolo specifica che nessuno può essere obbligato ad un trattamento sanitario. Lo scopo principale di questa precisazione è di vietare sperimentazioni senza l’esplicito consenso dei partecipanti.

Il rifiuto a sottoporsi ad un determinato trattamento sanitario è una scelta tutelata dalla Costituzione. Quindi, l’azione medica necessita di ottenere il consenso del paziente.

La legge 219/2017 va oltre promuovendo e valorizzando "la relazione di cura e di fiducia tra paziente e medico che si basa sul consenso informato, nel quale si incontrano l'autonomia decisionale del paziente e la competenza, l'autonomia professionale e la responsabilità del medico." (art. 1, comma 2).

L’articolo 32 mira anche a salvaguardare la salute della collettività. Per questo motivo il secondo comma si legge “Nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge.”. L’ultima parte della frase si riferisce ai trattamenti necessari per la tutela della salute pubblica, come ad esempio le vaccinazioni.

L’articolo si conclude con il divieto per la legge di superare i limiti del “rispetto per la persona umana”.

1.1.6 GDPR e Consenso Informato

Il regolamento EU n° 679/2016 "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", detto anche "regolamento GDPR" o "nuovo Regolamento della Privacy", sta cambiando completamente il panorama della gestione dei dati personali, e quindi riguarda profondamente il Consenso Informato nei suoi vari momenti applicativi.

Dal 26 maggio 2018, il DLG 196/2003 fino ad allora vigente cessa di essere valido.

Secondo il GDPR, il processo di Consenso Informato si deve inserire in una architettura di Risk Management relativo ai dati. Si tratta di un cambiamento radicale nel modo in cui si gestiscono i dati sensibili, e non semplicemente -nella modifica degli enunciati nel contesto delle informative: l'applicazione del regolamento EU n° 679/2016 al Consenso Informato medico-sanitario è un argomento complesso, che coinvolge molti aspetti operativi e gestionali di una struttura sanitaria.

Questa una sintesi dei cambiamenti più innovativi:

Tabella 1: Differenze prima e dopo GDPR

Prima del GDPR (25/05/2018)	Dopo il GDPR (dal 26/05/2018)
Consenso come "modulo"	Consenso come processo soggetto alla "Privacy by Design e by Default", in un'architettura di Risk Management
La sicurezza dei dati raccolti era assicurata dalla loro conservazione da parte della Struttura (responsabile del trattamento)	La Struttura Sanitaria adotta un Sistema per il processo di Consenso medico e diagnostico che garantisca la sicurezza dei dati sin dalla progettazione, oltre che nel funzionamento dello stesso, ed è responsabile della scelta di tale Sistema.
	Obbligo di ricorrere unicamente a un responsabile del Trattamento che presenti "garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate" a soddisfare il Regolamento e garantire la tutela dei diritti del paziente" (Art.28 comma 1).

Un'importante innovazione del nuovo GDPR rispetto al DLGS 196/2003 è che ogni trattamento di dati personali (come il Consenso Informato) deve concorrere alla sicurezza dei dati, a partire dalla fase di progettazione fino alla struttura stessa (la cosiddetta "Privacy by Design e by Default"). Non basta dunque eliminare i dati identificativi diretti da un database per far perdere loro la caratteristica di "insieme di dati personali" (vedi Regolamento del Garante della Privacy, "Considerando" 35 del Regolamento generale sulla protezione dei dati 2016/679/UE).

In altre parole, una struttura sanitaria deve verificare che il proprio sistema per il Consenso Informato (già presente o in fase di acquisizione) protegga i dati "by design e by default", altrimenti avrà l'onere di adeguarlo.

Adeguare un Consenso Informato è dispendioso in termini economici e di risorse umane: “I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell’ambito degli appalti pubblici” (Garante della Privacy, Considerando n° 78 del Regolamento 2016/679/UE).

Le garanzie devono infatti essere sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento.” (Regolamento del Garante della Privacy, “Considerando” 81 al Regolamento 2016/679).

La responsabilità della struttura sanitaria si estende quindi anche alla verifica dei requisiti e alla scelta di un idoneo sistema per l’intero processo del Consenso Informato: creazione e proposta delle informative con i dati dei pazienti, proposta del consenso, raccolta e conservazione delle decisioni del paziente. Ogni elemento deve concorrere alla protezione dei dati “by design e by default”.

Ai fini della conformità, è fondamentale poter disporre di uno strumento centralizzato che gestisca i consensi dei vari tipi di soggetti (pazienti, ma anche dipendenti, semplici contatti, fornitori) e che permetta di applicare in modo coerente i diritti riconosciuti dal GDPR.

L’applicazione del regolamento GDPR consiste in una parte definita a livello europeo (con entrata in vigore il 25 maggio 2018) e una parte definita a livello nazionale.

È anche fondamentale che il paziente possa facilmente accedere alle informazioni relative a:

- ***revoca*** del consenso;
- ***disponibilità*** di copie dei consensi sottoscritti e della eventuale revoca.

1.2 Consenso Informato Radiologico

Nel documento SIRM[S1] "Atto medico Radiologico" si afferma che il consenso all'effettuazione dell'esame radiologico, giuridicamente valido, deve essere informato.

L'informazione corretta e completa deve essere:

a) semplice, perché il paziente non è esperto di medicina. Personalizzata in base alla cultura e alla comprensione dell'assistito, esauriente, perché l'informazione deve esplicitare i rischi prevedibili e veritiera, ma emotivamente equilibrata;
b) esplicita. Non può mai essere desunta o implicita ma deve rispettare le modalità previste. La forma scritta non è sempre obbligatoria ma è prova certa dell'avvenuta informazione e può rappresentare un momento utile di riflessione per il paziente;
c) libera. Non è valida su coercizione o acquisita con inganno o errore;
d) personale. Deve essere rilasciata esclusivamente al diretto interessato, salvo eccezioni. Nel caso di minore o di soggetto malato di mente o incapace di intendere e di volere il consenso, per essere valido, dovrà essere prestato da chi ne esercita la potestà: i genitori o il tutore legalmente designato, ovvero il rappresentante legale (tutore o curatore) dell'incapace. Tuttavia, i confini tra potestà e volontà dei minori sono molto labili: il minorenne ha diritto di essere informato e di esprimere i suoi desideri. Qualora sussista disaccordo tra la volontà dei genitori e il parere dei medici curanti, questi ultimi potranno presentare ricorso all'Autorità Giudiziaria;
e) consapevole e manifesta. Ottenuta dopo un'informazione corretta e completa dal paziente capace di intendere e di volere nel momento in cui viene espresso;
f) preventiva. Deve precedere l'intervento sanitario restando suscettibile di revoca;
g) specifica. Deve essere riferita unicamente alla prestazione, diagnostica e/o interventistica, che viene prospettata al paziente, salvo nei casi in cui si può configurare uno stato di necessità.

Nel nostro caso la raccolta del CI deve essere quindi effettuata da uno dei medici dell'area radiologica che concorre alla conduzione dell'esame. L'approvazione fornita dal paziente tramite sottoscrizione del CI potrà essere revocata in qualsiasi momento sino all'effettiva esecuzione dell'esame, in conformità al DPCM 22 febbraio 2013 (art. 57 c. 1, lettera h).

2. ***Firme Elettroniche***

È importante conoscere la legislazione in merito, e come nella firma cartacea è importante identificare in modo sicuro il firmatario prima di procedere alla firma.

2.1 Identificazione e autenticazione elettroniche

L'identificazione elettronica è un processo in cui si usano i dati di autenticazione personale in forma elettronica per identificare univocamente una persona fisica e una persona giuridica. L'autenticazione elettronica è il processo che permette di assicurare il riconoscimento dell'utente elettronico.

L'identificazione elettronica viene utilizzata, ad esempio, per accedere a servizi online.

Con il termine "riconoscimento", si intende la certezza incontrovertibile dell'associazione ad "una persona fisica, ad una persona giuridica o anche ad una persona fisica che rappresenta la persona giuridica". Questi soggetti sono appartenenti all'Unione Europea o comunque identificati con sufficiente ragionevolezza mediante uno dei regimi di identificazione elettronica riconosciuti dalla Commissione europea, inseriti nell'elenco pubblico dei regimi notificati ai sensi e per gli effetti dell'art. 9 del regolamento.

In materia di autenticazione elettronica, oltre ai canali di accesso attraverso le Carte di identificazione elettronica (come TS-CNS o la Carta di Identità elettronica), è stato avviato e realizzato in Italia il progetto Sistema Pubblico di Identità Digitale (SPID) che nasce con ambizioni europee ai fini del mutuo riconoscimento dei sistemi di autenticazione comunitari.

2.2 Firme Elettroniche - eIDAS/CAD

Il Regolamento eIDAS disciplina tre tipologie di firme elettroniche.

- ✓ **Firma Elettronica** - dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.
  In ambito informatico, è la **firma debole** in quanto non prevede meccanismi di autenticazione del firmatario o di integrità del dato firmato.
- ✓ **Firma Elettronica Avanzata (FEA)** - firma elettronica che soddisfi i seguenti requisiti:
  - è connessa unicamente al firmatario;
  - è idonea a identificare il firmatario;
  - è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
  - è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
- ✓ **Firma Elettronica Qualificata (FEQ)** – che in aggiunta a quelle di una firma elettronica avanzata possiede queste caratteristiche:
  - è creata su un dispositivo qualificato per la creazione di una firma elettronica;
  - è basata su un certificato elettronico qualificato;
  - ha effetto giuridico equivalente a quello di una firma autografa.

Il Regolamento stabilisce la non discriminazione dei documenti elettronici rispetto ai documenti cartacei. A livello nazionale le firme elettroniche introdotte da eIDAS non mutano sostanzialmente il quadro di riferimento; pertanto, non vi saranno disagi per gli attuali possessori di firme digitali.

Mentre nel Codice dell'Amministrazione Digitale (CAD - Decreto Legislativo 7 marzo 2005, n. 82) la firma elettronica viene definita come un insieme di dati in forma elettronica utilizzati come metodo di identificazione informatica, nel Regolamento eIDAS, al Capo I Art. 3, la firma elettronica è

descritta come dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici, ed utilizzati dal firmatario per firmare.

La locuzione "utilizzati dal firmatario per firmare" ha una funzione prettamente identificativa, comportando un rafforzamento della funzione dichiarativa (cioè la manifesta adesione al contenuto del documento firmato) e della funzione probatoria (cfr. art. 21 del CAD).

Tabella 2: L'efficacia giuridica delle firme elettroniche

	Firma elettronica	**Firma elettronica avanzata, qualificata o digitale**
CAD	Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (art.21)	Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 del codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria. (art.21)
eIDAS	Non sono negati effetti giuridici per via della sua forma elettronica. Spetta al diritto nazionale dei singoli Paesi europei definire gli effetti giuridici delle firme elettroniche (art. 25)	Ha un effetto giuridico equivalente a quello di una firma autografa. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri (mutuo riconoscimento).

2.2.1 Il Regolamento UE n° 910/2014 - eIDAS

Il Regolamento eIDAS (electronic IDentification Authentication and Signature) - Regolamento UE n° 910/2014 sull'identità digitale - ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e per i mezzi di identificazione elettronica degli stati membri.

Il regolamento fornisce una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni, e incrementa la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di e-business e commercio elettronico nell'Unione Europea.

Il regolamento:

- fissa le condizioni alle quali gli Stati Membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro;
- stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche;
- istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.

Rispetto ai sistemi di identificazione elettronica, eIDAS prevede che ciascuno stato membro possa notificare i sistemi di identificazione elettronica forniti ai cittadini e alle aziende per consentire un reciproco riconoscimento.

Il regolamento eIDAS è stato emanato il 23 luglio 2014 e ha piena efficacia dal 1 luglio del 2016.

Nella seguente immagine si evidenziano le tappe del regolamento eIDAS:

Immagine 1: Le tappe del regolamento e IDAS

2.2.2 Codice Amministrazione Digitale - CAD

Il Codice dell'Amministrazione Digitale (CAD) è un testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Istituito con il Decreto Legislativo 7 marzo 2005 n. 82, è stato successivamente modificato e integrato prima con il Decreto Legislativo 22 agosto 2016 n. 179 e poi con il Decreto Legislativo 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale.

Con l'ultimo intervento normativo il CAD è stato ulteriormente razionalizzato nei suoi contenuti. Si è proceduto ad un'azione di deregolamentazione (sia semplificando il linguaggio, sia sostituendo le precedenti regole tecniche con linee guida) a cura di AgID, la cui adozione risulterà più rapida e reattiva rispetto all'evoluzione tecnologica.

Inoltre, come evidenziato dalla relativa relazione illustrativa del Decreto Legislativo n. 217/17:

- è stata sottolineata con maggior forza la natura di carta di cittadinanza digitale della prima parte del CAD, con disposizioni volte ad attribuire a cittadini e imprese i diritti all'identità e al domicilio digitale, alla fruizione di servizi pubblici online e mobile oriented, a partecipare effettivamente al procedimento amministrativo per via elettronica e a effettuare pagamenti online;
- è stata promossa l'integrazione e l'interoperabilità tra i servizi pubblici erogati dalle pubbliche amministrazioni in modo da garantire a cittadini e imprese il diritto a fruirne in maniera semplice;
- è stata garantita maggiore certezza giuridica alla formazione, gestione e conservazione dei documenti informatici prevedendo che non solo quelli firmati digitalmente – o con altra firma elettronica qualificata - ma anche quelli firmati con firme elettroniche diverse possano, a certe condizioni, produrre gli stessi effetti giuridici e disporre della stessa efficacia probatoria, senza prevedere l'intervento di un giudice caso per caso;
- è stata rafforzata l'applicabilità dei diritti di cittadinanza digitale e promosso l'innalzamento del livello di qualità dei servizi pubblici e fiduciari in digitale, sia istituendo presso l'AgID l'Ufficio del Difensore civico per il digitale, sia aumentando la misura delle sanzioni irrogabili qualora i fornitori di servizi fiduciari violino le norme;
- è stato promosso un processo di valorizzazione del patrimonio informativo pubblico, riconducendolo tra le finalità istituzionali di ogni amministrazione.

2.2.3 Vantaggi di eIDAS

Potenziando le normative nazionali in materia di identificazione elettronica, il regolamento eIDAS ha l'obiettivo di agevolare l'uso transfrontaliero dei mezzi di identificazione elettronica dei singoli Stati membri.

Il Regolamento (articolo 25, comma 3) prescrive che:

" *Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri*.".

I formati che queste firme elettroniche qualificate devono possedere sono definiti nella Decisione di esecuzione (UE) 2015/1506 della Commissione dell'8 settembre 2015: fra quelli previsti vi rientra anche il formato PDF. Per verificare la validità delle firme elettroniche qualificate basate su certificati rilasciati da tutti i soggetti autorizzati in Europa, la Commissione europea ha reso disponibile un'applicazione open source: Il Digital Signature Service (DSS).

Grazie al principio del mutuo riconoscimento e della reciproca accettazione di schemi di IDentificazione elettronica (e-ID) interoperabili, per il tramite di Prestatori di servizi fiduciari (Trust Service Providers - TSP), eIDAS vuole semplificare l'impiego dei canali di autenticazione elettronici nei confronti delle pubbliche amministrazioni, sia da parte delle imprese che da parte dei cittadini. Il Regolamento mira a creare condizioni eque di concorrenza per i Prestatori di servizi fiduciari che attualmente operano in un contesto in cui le differenze fra le normative nazionali dei vari Stati membri sono fonte di incertezze giuridiche e di oneri supplementari.

L'obbligo di riconoscere le firme elettroniche qualificate introdotto nel Regolamento eIDAS (art. 25, comma 3) deve essere onorato; altrimenti, oltre a non consentire l'esercizio di un diritto dei cittadini dell'unione, si incorre in una procedura di infrazione.

2.2.4 Vantaggi per le imprese

Gli obblighi di accettazione reciproca da parte degli Stati membri nella fruizione dei servizi fiduciari qualificati, incentiveranno le imprese ad estendere le loro attività oltre le frontiere, senza andare incontro ad ostacoli nelle interazioni con le autorità pubbliche. Un'impresa, ad esempio, potrà partecipare elettronicamente ad un appalto pubblico indetto dall'amministrazione di un altro Stato Membro, senza rischiare il blocco della sua firma elettronica a causa di requisiti nazionali specifici e/o di problemi di interoperabilità.

Analogamente, un'impresa potrà firmare digitalmente contratti con la controparte di un altro Stato membro, senza doversi preoccupare di eventuali diversità interpretative delle norme giuridiche per servizi fiduciari quali i sigilli elettronici, i documenti elettronici o la validazione temporale.

2.2.5 Vantaggi per i cittadini

Grazie all'adozione del regolamento, i cittadini potranno trasmettere la dichiarazione dei redditi online ad un altro stato membro. Inoltre, nel campo della formazione gli studenti potranno iscriversi in modalità elettronica ad un'università estera. In campo sanitario i pazienti avranno la possibilità di accedere online alla propria cartella clinica, mentre i medici potranno accedere alle relative informazioni cliniche.

2.2.6 Servizi fiduciari

Nel regolamento eIDAS sono definiti servizi fiduciari:

- servizi di creazione, verifica e convalida di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato;
- certificati relativi a tali servizi;
- servizi di creazione, verifica e convalida dei certificati di autenticazione di siti web;
- servizi di conservazione di firme; sigilli o certificati elettronici relativi a tali servizi.

Viene detto **servizio fiduciario qualificato** un servizio fiduciario che soddisfa i requisiti stabiliti dal Regolamento eIDAS e ne fornisce le relative garanzie in termini di sicurezza e qualità.

I servizi fiduciari qualificati sono sottoposti alla vigilanza di appositi organismi governativi nazionali, in Italia l'AgID.

I prestatori di **servizi fiduciari qualificati** sono autorizzati a caratterizzare il servizio qualificato offerto attraverso l'uso del **marchio di fiducia UE** per i servizi fiduciari qualificati.

Tale marchio di fiducia è regolamentato dal Regolamento di esecuzione (UE) 2015/806 della Commissione del 22 maggio 2015.

A colori o in bianco e nero, in positivo o negativo, ha le seguenti quattro possibili rappresentazioni.

Immagine 2: Marchio di fiducia UE per i servizi fiduciari qualificati

Per ottenere la qualifica di prestatore di servizio fiduciario qualificato è necessaria una valutazione di conformità da parte degli organismi di valutazione accreditati in Italia.

Il Regolamento eIDAS ha previsto che per ottenere la qualifica di prestatore di servizio fiduciario qualificato gli interessati debbano sottoporsi ad una valutazione di conformità da parte di un organismo di valutazione accreditato ai sensi del Regolamento (CE) n. 765/2008.

Tali organismi sono accreditati in Italia da Accredia (Ente Italiano di Accreditamento).

2.3 Come ottenere la firma digitale

La firma digitale può essere richiesta da tutte le persone fisiche: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni, rivolgendosi ai prestatori di servizi fiduciari qualificati autorizzati da AgID, che garantiscono l'identità dei soggetti che utilizzano la firma digitale.

I prestatori di servizi fiduciari accreditati, sono soggetti pubblici o privati che, sotto la vigilanza di AgID, emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi).

La firma digitale viene generata grazie ad una coppia di chiavi digitali asimmetriche attribuite in maniera univoca ad un soggetto, detto titolare:

- la **chiave privata** è conosciuta solo dal titolare (Smart Card, Token, ecc.) ed è usata per generare la firma digitale da apporre al documento;
- la **chiave da rendere pubblica** è usata per verificare l'autenticità della firma.

Questo metodo è conosciuto come crittografia a doppia chiave e garantisce la piena sicurezza, dato che la chiave pubblica non può essere utilizzata per ricostruire la chiave privata.

L'associazione tra la chiave pubblica ed il titolare della corrispondente chiave privata si basa sull'emissione di un **"certificato digitale"** emesso dall'Ente Certificatore, e avviene solo dopo l'identificazione certa del firmatario.

Per questo, la **firma digitale** è la tipologia **più sicura** di **firma elettronica**

2.4 L'uso della firma digitale

Vi sono due modalità di utilizzare la firma digitale:

- **in "locale":** si intende la firma digitale generata in uno strumento nel possesso fisico del titolare, smart card o token;
- **da "remoto":** si intende la firma digitale generata usando strumenti di autenticazione (tipicamente user id + password + OTP o telefono cellulare) che consentono la generazione della propria firma su un

dispositivo (HSM) custodito dal certificatore (in terminologia europea, prestatore del servizio fiduciario qualificato).

La firma digitale offre numerosi vantaggi, tra cui il risparmio di tempo e costi, e incentiva la dematerializzazione dei documenti in molti settori della pubblica amministrazione, garantendo l'autenticità del firmatario, l'integrità, la piena validità legale del documento sottoscritto e il suo riconoscimento in tutti i Paesi europei.

2.4.1 SPID e la firma digitale

La firma digitale può essere ottenuta anche utilizzando lo SPID come sistema di riconoscimento.

Con l'istituzione del Sistema Pubblico di Identità Digitale (SPID), l'Italia mira a realizzare un sistema di identificazione elettronica che abbia caratteristiche adeguate affinché il suo utilizzo sia possibile anche al di fuori del territorio italiano.

SPID è un sistema aperto attraverso il quale pubbliche amministrazioni e imprese private (previo accreditamento da parte dell'Agenzia per l'Italia Digitale) possono offrire servizi di identificazione elettronica ed accesso a cittadini e imprese attraverso un'unica identità digitale.

I prestatori di tali servizi hanno il compito di garantire la corretta registrazione e messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese.

I servizi prevedono l'accesso con credenziali SPID di livello 2, in questo modo il cittadino ha la possibilità di dimostrare con certezza la sua l'identità ed ottenere così la firma digitale.

Sono in vigore dal 4 maggio 2021, inoltre, le Linee Guida per firmare documenti online con SPID, in conformità all'art. 20 del CAD. Le linee guida pongono le basi per realizzare, nel prossimo futuro, le funzionalità che consentiranno agli utenti di sottoscrivere documenti utilizzando SPID, e alle PA e ai privati di agevolare la dematerializzazione dei documenti [1].

2.4.2 SPID in Italia e in Europa

Le tecniche e i protocolli su cui si basa SPID sono già stati sperimentati a livello europeo e adottate dai progetti sperimentali Stork e Stork II (Secure idenTity acrOss boRders linKed).

L'AgID ha ultimato il processo che consente ai cittadini italiani di utilizzare la propria identità digitale SPID con credenziali di livello 2 e 3 (è facoltà degli Stati membri accettare il livello 1) per accedere ai servizi in rete delle pubbliche amministrazioni europee.

In quest'ottica – ai fini del mutuo riconoscimento dei mezzi di identificazione elettronica adottati tra Stati membri – l'Agenzia per l'Italia Digitale ha completato nel mese di luglio 2018 il processo di prenotifica alla Commissione Europea del sistema SPID, iniziato nel dicembre 2017.

Il processo di notifica è stato ultimato e lo SPID è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea C318 del 10 settembre 2018. La notifica comporta che dopo un anno, quindi dal 10 settembre 2019, l'identità digitale SPID deve poter essere usata per l'accesso ai servizi in rete delle Pubbliche Amministrazioni dell'Unione che richiedono credenziali di livello 2 o 3.

Lo SPID diviene quindi uno strumento unico per la nostra identità digitale in tutta l'Unione europea.

Tutte le pubbliche amministrazioni che rendono accessibili i propri servizi online con credenziali SPID di livello 2 o 3 (come anche attraverso la carta di identità elettronica), hanno l'obbligo di rendere accessibili detti servizi anche con gli strumenti di autenticazione notificati dagli altri Stati membri. Non rispettare tale obbligo, implica esporsi a una procedura di infrazione per violazione dell'articolo 6 del regolamento eIDAS (n.910/2014) [S1].

Le pubbliche amministrazioni possono adempiere agli obblighi aderendo al Nodo eIDAS italiano gestito da AgID.

2.4.3 Come richiedere SPID

Ad oggi, per ottenere SPID è necessario essere maggiorenni ed in possesso di un documento di identità italiano in corso di validità, della tessera sanitaria o codice fiscale, di un indirizzo e-mail e un numero di cellulare.

Per attivarlo occorre rivolgersi ad uno dei gestori di identità digitale abilitati dall'Agenzia per l'Italia Digitale (AgID). Il cittadino avrà così a disposizione un'unica identità digitale, utilizzabile da computer, tablet e smartphone.

L'identità è formata da nome utente e password, strettamente personali, con cui si può accedere ai servizi online della Pubblica Amministrazione e dei privati aderenti in modo sicuro e protetto, grazie anche a verifiche di sicurezza che prevedono, in molti casi, l'invio di una password temporanea (OTP - one time password) da inserire in fase di autenticazione.

2.5 La Carta di Identità Elettronica (CIE) entra in eIDAS.

La Carta di Identità Elettronica (CIE) è stata notificata alla Commissione europea e agli altri stati membri con la pubblicazione nella Gazzetta Ufficiale dell'Unione europea C309 del 13 settembre 2019, ed è stata integrata con il nodo eIDAS, in conformità con l'omonimo Regolamento (UE) n. 910/2014.

Questo comporta che potrà essere utilizzata per accedere ai servizi in rete non solo italiani, ma di tutte le pubbliche amministrazioni dell'Unione che richiedono credenziali di livello 1, 2 o 3. Gli altri stati membri hanno l'obbligo di far accedere ai propri servizi in rete i cittadini dotati di SPID, a partire dal 13 settembre 2020 diviene obbligatorio consentire l'accesso anche con la CIE.

È possibile l'accesso ai servizi in rete da smartphone su sistemi Android e IOS e in modalità Desktop con sistemi operativi Microsoft, Linux e MacOS.

Come SPID, così anche la CIE 3.0 diviene quindi uno strumento per attestare la nostra identità digitale in tutta l'Unione europea.

Le scelte tecniche effettuate per realizzare l'autenticazione online tramite la CIE fanno riuso, seppur con lievi differenze, dei medesimi paradigmi e protocolli adottati per SPID, consentendo così ai fornitori di servizi che

hanno già integrato SPID di procedere rapidamente all'integrazione di "Entra con CIE". Il Ministero dell'Interno è il gestore dell'identità digitale della CIE, con cui è necessario federarsi per consentire l'accesso ai propri servizi anche con la CIE.

2.5.1 Vantaggi CIE

I fornitori di servizi che consentono l'accesso tramite la CIE, pubbliche amministrazioni incluse, godono del medesimo importante vantaggio già introdotto con SPID: la manleva in merito alla verifica di identità del soggetto che si autentica al proprio servizio tramite la CIE.

In altri termini, è il Ministero dell'Interno che garantisce di aver correttamente identificato il soggetto e aver consegnato la CIE e i relativi codici al legittimo titolare, forte del processo di identificazione esercitato dagli ufficiali di anagrafe presso i Comuni italiani.

Il fornitore di servizi, analogamente a quanto posto in opera per SPID, dovrà limitarsi ad eseguire e conservare le evidenze informatiche del processo di autenticazione, correlando quest'ultimo alle operazioni effettuate dal cittadino tramite il servizio acceduto.

Il fornitore del servizio non avrà bisogno di stipulare alcuna convenzione con il Ministero dell'Interno, così come non ne ha bisogno se utilizza la CIE per verificare l'identità di un cittadino durante un incontro fisico.

2.5.2 Firma Elettronica con CIE

La Carta di Identità Elettronica **(**CIE**)** è rilasciata dallo stato italiano [S2] e può essere utilizzata come **dispositivo di firma elettronica avanzata** (**FEA**) per firmare documenti elettronici.

È possibile apporre una firma con CIE su file di qualsiasi estensione (.pdf, .jpg, .png, ecc.).

Le tipologie di firma consentite sono:

- "*PAdES***"** – se si intende produrre un file PDF firmato digitalmente;
- "*CAdES*" – per tutte le altre tipologie di file.

La firma con CIE è regolamentata dalla normativa italiana e riconosciuta dalle Pubbliche Amministrazioni che ne consentono l'uso.

La firma con la CIE soddisfa i requisiti del regolamento europeo eIDAS per la Firma Elettronica Avanzata (FEA).

Per quanto riguarda le caratteristiche tecniche del documento, così come il processo autorizzativo che ne consente l'emissione, la Carta di Identità Elettronica soddisfa pienamente tali requisiti in quanto:

- è un documento che deve essere richiesto al Comune di residenza/dimora oppure presso il consolato di riferimento per i cittadini italiani residenti all'estero. L'identificazione del richiedente, dunque, è affidata a un pubblico ufficiale;
- è un documento rilasciato dal Ministero dell'Interno che ne firma digitalmente i dati contenuti, rendendoli immutabili;
- la chiave di firma digitale è certificata dal Ministero dell'Interno e può essere usata solo dopo aver immesso un PIN, che può essere sostituito da una verifica biometrica in caso di utilizzo da smartphone;
- questa modalità di firma del documento ne garantisce le caratteristiche di autenticità e integrità.

È lo Stato italiano stesso, dunque, che certifica e garantisce l'identità del titolare della CIE, mentre gli elevati meccanismi di sicurezza presenti all'interno del documento ne proteggono i dati, garantendone l'inalterabilità.

Con l'art. 61 del DPCM del 22 febbraio 2013, anche la normativa italiana riconosce l'utilizzo della CIE come strumento di firma elettronica avanzata per i servizi e le attività di cui agli articoli 64 e 65 del "**Codice dell'Amministrazione Digitale**" (CAD).

2.6 Firma grafometrica

Un'altra tipo di firma molto diffusa è la Firma Grafometrica (FG) utilizzata già da diverso tempo in molte aziende pubbliche e private (Banche, Servizi Postali, Assicurazioni, ecc.). Un elemento che la rende molto diffusa è che il cliente/cittadino non ha bisogno di alcun dispositivo hardware e software per firmare, se non la sua firma autografa.

La *Firma Grafometrica* è un particolare tipo di **Firma Elettronica Avanzata (FEA)**, sottoscritta a mano su un particolare tablet (o tavoletta grafometrica) in grado di acquisire, oltre all'immagine della firma, anche i principali dati biometrici del tratto grafico apposto (posizione, tempo, pressione, velocità, accelerazione), in modo tale che:

a. la firma "autografa" sia strettamente associata al documento oggetto della sottoscrizione (DPCM 22.02.2013, art. 56, c.1, lett. h: "Le soluzioni di FEA garantiscono la connessione univoca della firma al documento sottoscritto");

b. la firma "autografa" protegga l'integrità del documento e della firma stessa come riportata nel documento (DPCM 22.02.2013, art. 56, c.1, lett. d: "Le soluzioni di FEA garantiscono la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma");

c. i dati biometrici di cui è costituita la firma siano adeguatamente protetti in modo che sia impossibile copiarli ed associarli in modo artificiale o fraudolento ad un diverso documento.
Tali dati saranno cifrati e univocamente associati al documento sottoscritto a garanzia della loro immodificabilità.

2.6.1 Firma grafometrica normativa: linee guida

Ecco le principali linee guida per esser conformi alle regole tecniche e agli adempimenti previsti in tema di biometria e come gestirli al meglio.

- *Acquisizione del consenso del paziente*

  L'utilizzo della FG deve essere sempre subordinato al consenso esplicito del paziente per l'accettazione del servizio di firma.

- *Identificazione del soggetto firmatario*

  Per la corretta gestione del processo di firma biometrica, occorre preventivamente identificare il paziente mediante un valido documento di riconoscimento.

- *Pubblicazione dell'informativa sul proprio sito*

  È indispensabile, previa erogazione del servizio di FG, pubblicare sul proprio sito la nota informativa sul servizio di FG.

- *Adozione polizza assicurativa*

  L'erogazione della firma grafometrica, prevede che ogni soggetto si doti di un'assicurazione per la responsabilità civile come richiesto *nell'Art. 57 comma 2 del DPCM del 22 febbraio 2013*, al fine di proteggere i titolari della firma e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche.

- *Invio della notificazione preventiva al garante privacy per il trattamento dei dati biometrici*

  L'art. 37 del Codice Privacy prevede l'obbligo di effettuare la notificazione al Garante (*si tratta, infatti, di dati ritenuti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato*). La stessa deve essere effettuata prima che inizi il trattamento, ed una sola volta, indipendentemente dalla durata e dal numero di operazioni di trattamento del medesimo tipo di dati che si effettua.

In particolare, per l'ultimo punto si è esonerati dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni e limitazioni**.**

a. *Il procedimento di firma è abilitato previa identificazione del firmatario;*
b. Sono *resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione*, che non comportino l'utilizzo di dati biometrici;
c. *La cancellazione dei dati biometrici grezzi e dei campioni biometrici* ha luogo immediatamente dopo il completamento della procedura di sottoscrizione, e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto;
d. *I dati biometrici e grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta.*

   Essi vengono memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica, con dimensione della chiave adeguata alla dimensione e al ciclo di vita dei dati. Il certificato digitale è emesso da un certificatore accreditato, ai sensi dell´art. 29 del Codice dell'amministrazione digitale.

   La corrispondente chiave privata è nella esclusiva disponibilità di un soggetto terzo fiduciario che fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. La chiave può essere frazionata tra più soggetti ai fini di sicurezza e integrità del dato. In nessun caso il soggetto che eroga il servizio di firma grafometrica può conservare in modo completo tale chiave privata. *Le modalità di generazione, consegna e conservazione delle chiavi sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all´art. 57, comma 1 lettere e) ed f) del D.P.C.M. 22 febbraio 2013,* contenente le Regole Tecniche in materia di Firma Elettronica Avanzata pubblicato in G.U. n. 117 il 21 maggio 2013. Tale decreto è entrato in vigore il 5 giugno 2013.
e. La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con *l'ausilio di tecniche*

crittografiche, con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;

f. *Sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software* e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati;

g. *I sistemi informatici sono protetti contro l'azione di malware e* sono, inoltre, adottati *sistemi di firewall* per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati;

h. Nel caso di utilizzo di sistemi di firma grafometrica *nello scenario mobile, sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili,* il fine è quello di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).

i. *I sistemi di gestione impiegati adottano certificazioni digitali e policy di sicurezza* che disciplinino, sulla base di criteri predeterminati, le condizioni di un loro utilizzo sicuro (in particolare, rendendo disponibili funzionalità di remote wiping, applicabili nei casi di smarrimento o sottrazione dei dispositivi).

j. *L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario*, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria. *Le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all´art. 57, comma 1, lettere e) ed f) del D.P.C.M. 22 febbraio 2013.*

k. *È predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare*, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

È consigliabile che la struttura erogante adotti specifiche procedure organizzative che chiarificano alcuni aspetti specifici legati alla gestione dei processi di:

a) adesione al servizio di FEA;

b) sottoscrizione di documenti informatici con firma grafometrica;

c) gestione del Data breach (violazione dei dati);

d) esibizione di documenti informatici sottoscritti con firma grafometrica.

Queste procedure devono essere definite e approvate dalla struttura erogante e condivise con tutti i soggetti coinvolti.

2.7 L'apposizione di firme e informazioni su documenti firmati

L'art. 20 co. 1-bis del Codice dell'Amministrazione Digitale dispone che il documento informatico su cui è "apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore" soddisfi il requisito della forma scritta e ha l'efficacia prevista dall'art. 2702 del codice civile.

In sunto l'AGID denota come la firma elettronica qualificata (FEQ) - o digitale - è il risultato di una procedura informatica, detta validazione, che garantisce l'autenticità, l'integrità e il non ripudio dei documenti informatici, definita anche firma "***FORTE"***

Dal 2006, è inoltre possibile usare il formato di firma Portable Document Format (PDF): il sito web di Adobe System illustra le specifiche del formato PDF necessarie per lo sviluppo di ulteriori prodotti di verifica e generazione

della firma digitale.

L'AgID ha pubblicato un documento[2] che si pone l'obiettivo di chiarire alcuni aspetti generali dei formati di firma CAdES (file con estensione *p7m*) e PAdES (file con estensione *pdf*) e la loro attitudine ad ospitare più firme e informazioni disponibili solo dopo la generazione della firma digitale quali, ad esempio, la segnatura di protocollo prevista dall'articolo 55 del D.P.R. 28 dicembre 2000, n. 445.

Come noto, un documento sottoscritto con firma digitale ha nel nostro ordinamento piena efficacia giuridica, a condizione che non sia modificato dopo l'apposizione della firma.

Con la diffusione dell'uso dei documenti informatici, sono sempre più numerose le richieste di chiarimento sul corretto utilizzo della firma digitale, con particolare riferimento ai casi in cui sia necessario apporre più firme su un medesimo documento o in cui si intenda aggiungere dei dati dopo la sottoscrizione, ad esempio, allo scopo di riportare gli estremi della segnatura di protocollo di un documento spedito o ricevuto da una pubblica amministrazione.

A tal fine, appare utile richiamare alcune nozioni sulle firme digitali.

Senza entrare in dettagli tecnici, la firma digitale consiste nella creazione di un file, definito "busta crittografica", che racchiude al suo interno il documento originale, l'evidenza informatica della firma e la chiave per la verifica della stessa, che, a sua volta, è contenuta nel certificato emesso a nome del sottoscrittore, come mostrato *nella Figura 1*. L'autenticità del certificato è garantita da un'Autorità di certificazione. Nella fattispecie in Italia l'autenticità è garantita dai certificatori accreditati ai sensi dell'articolo 29 del CAD (D.Lgs. n. 82/2005).

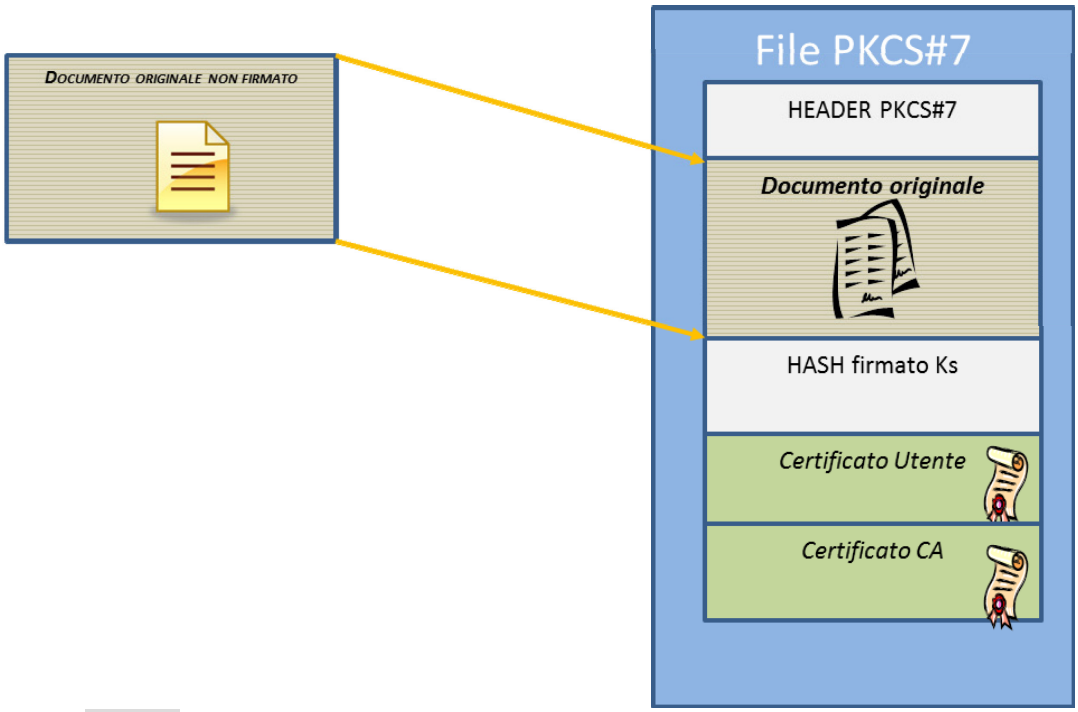


Figura 1: Firma Digitale

Gli standard europei (*Decisione della Commissione europea 2011/130/EU*) prevedono tre tipi di sottoscrizione digitale, identificati dagli acronimi CAdES, PAdES e XAdES, modalità di sottoscrizione adottate anche in Italia. Ai fini del nostro obiettivo verrà trattata solo la busta PAdES, in quanto utilizza il formato *.pdf,* molto diffuso e facile da consultare, nonché unico formato di firma utilizzato da SPID.

2.7.1 La firma PAdES

La firma digitale in formato PAdES è un file con estensione *.pdf*, leggibile con i comuni *reader* disponibili per questo formato.

Questa tipologia di firma, nota come "firma PDF", prevede diverse modalità per l'apposizione della firma, a seconda che il documento sia stato predisposto o meno ad accogliere le firme previste ed eventuali ulteriori informazioni. Tale firma rende il documento più facilmente accessibile, ma consente di firmare solo documenti di tipo PDF.

Il formato PDF consente inoltre di gestire diverse versioni dello stesso documento senza invalidare le firme digitale apposte.

2.7.2 Predisposizione del documento PDF

Il documento può essere predisposto, attraverso la gestione dei "moduli" (disponibile con la versione *professional* di Acrobat e di altri prodotti conformi), alla firma digitale da parte di utenti che dispongono di un prodotto conforme allo standard PDF (ISO 32000), fra questi Acrobat Reader.A tale scopo sarà necessario trasformare il documento in formato PDF e, successivamente, predisporre i campi firma.

Al fine di rendere utilizzabile il documento con versioni non professionali di applicazioni conformi allo standard PDF (es. Adobe Reader), è necessario salvare il documento attivando tali funzionalità.

Altra interessante caratteristica è che il documento in formato PDF consente di collocare fisicamente la firma digitale in un preciso punto del documento. Tale caratteristica è particolarmente utile nel caso di sottoscrizione di clausole vessatorie o, comunque, in ogni caso in cui la collocazione della firma abbia una qualche valenza.

2.7.3 Molteplici firme nel documento PDF

Qualora il documento non fosse stato predisposto per tutte le firme necessarie, è comunque possibile apporre ulteriori firme senza invalidare le precedenti.

A tale scopo, il formato PAdES implementa la funzione della gestione delle versioni (*versioning*): ogni versione successiva alla prima, contiene la versione integrale, non modificata, del documento precedente (comprese le firme digitali).

Ogni modifica al documento (ulteriore firma o aggiunta di testo o immagini) produce, infatti, una nuova versione che contiene la versione originale non modificata (*Figura 2*).

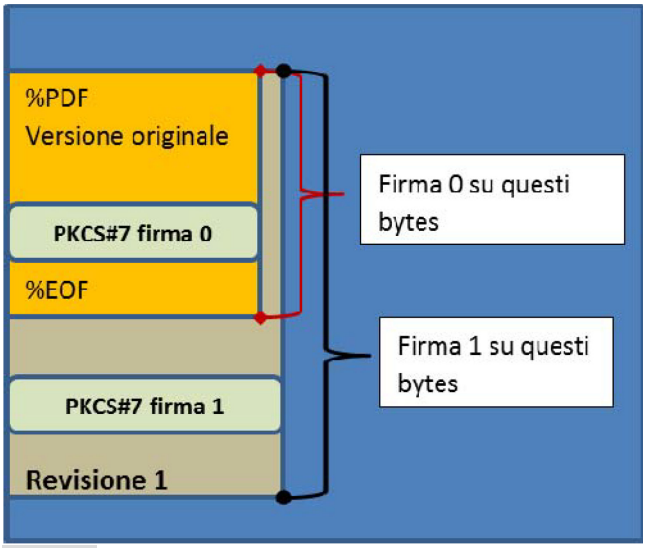


Figura 2 - busta formato PAdES – firme di versioni del documento firmato

Tale caratteristica della busta PAdES rende questo formato particolarmente idoneo anche nel caso in cui si renda necessario apportare delle modifiche al documento dopo averlo sottoscritto: ad esempio per riportarvi delle annotazioni, come i dati degli estremi di protocollo che sono disponibili solo successivamente alla sottoscrizione del documento stesso.

Ad una prima analisi, un documento sottoscritto sul quale sono riportate tali annotazioni potrebbe apparire corrotto in quanto modificato dopo la firma (*Figura 3*). Tuttavia, nella busta PAdES è presente ed è accessibile anche la versione non modificata del documento (*Figura 4*), che pertanto conserva piena efficacia giuridica. Non devono infatti trarre in inganno i messaggi mostrati dal *reader* del documento "*Almeno una delle firme non è valida*" e "*Il documento dopo la firma è stato modificato o si è danneggiato*", in quanto è comunque possibile accedere alla versione del documento correttamente sottoscritta, coerentemente con quanto previsto dalle regole tecniche di cui al D.P.C.M. del 22 febbraio 2013.

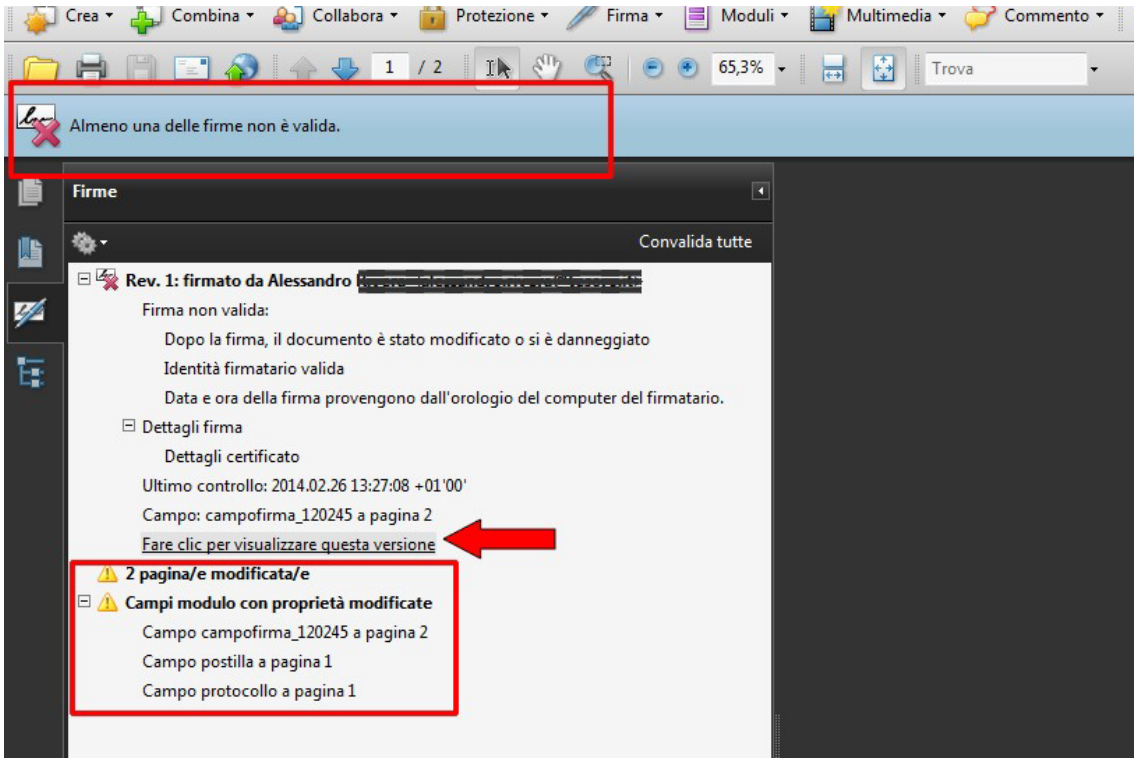


Figura 3 – accesso alla versione non modificata del documento firmato – formato PAdES

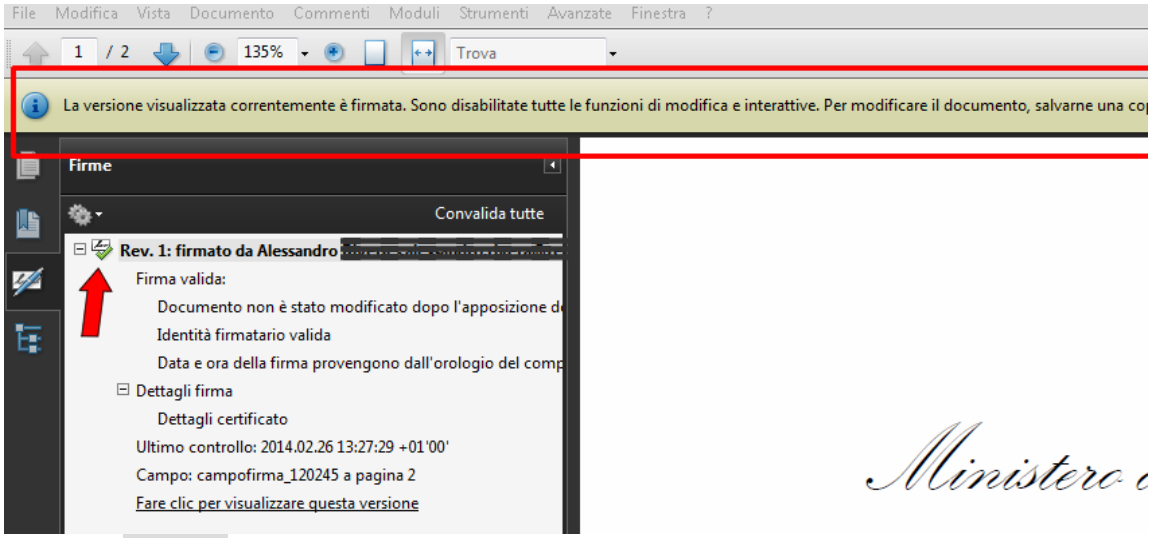


Figura 4 – busta formato PAdES- versione non modificata del documento sottoscritto digitalmente

Con un semplice "doppio click" sull'allegato si apre il documento trasmesso verificandone la firma(*Figura 5*).

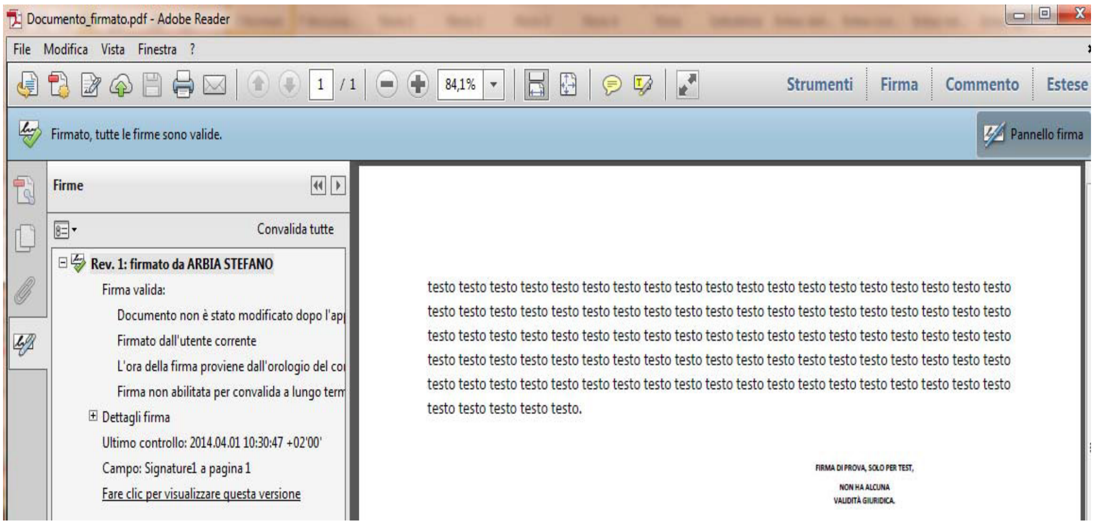


Figura 5 – Documento allegato nella versione originale

In conclusione, operazioni su un documento pdf già firmato - quali allegare il documento pdf in altro documento pdf, l'apposizione di una ulteriore firma digitale al documento, l'aggiunta di un campo testo o immagine al documento - non invalidano la firma digitale in quanto la stessa è comunque verificabile con successo.

2.8 Firma Elettronica in sanità

La normativa sin dal 1997 stabilisce che "*atti, dati e documenti formati dalla Pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*".

Difatti, la firma digitale è uno strumento informatico essenziale per dare validità legale ai documenti digitali e, dunque, necessario quando occorre sottoscrivere una dichiarazione ottenendo la garanzia di integrità dei dati oggetto della sottoscrizione e di autenticità delle informazioni, relative a chi ha apposto la firma. Un documento digitale e/o informatico, infatti, può essere modificato o riprodotto infinite volte ottenendo copie assolutamente identiche all'originale, diversamente dai documenti cartacei ove la persona che ne assume paternità viene identificata tramite la sottoscrizione autografa a garanzia della sua autenticità.

Pertanto, proprio per tutelare anche l'**autenticità** e l'**integrità** dei documenti digitali è stata introdotta la firma digitale, un **sistema di autenticazione di documenti informatici** che si riferisce in maniera univoca ad un solo soggetto ed al documento cui è apposta o associata, proprio come la **firma autonoma su carta**.

Ma quali sono le altre tipologie di firme elettroniche utilizzate in campo sanitario?

- **Firma elettronica avanzata (FEA):**
  - consente l'identificazione del firmatario,
  - garantisce la connessione univoca con lui,
  - consente di rilevare eventuali modifiche dei dati cui è apposta.

Nelle **aziende sanitarie/ospedaliere** e negli **studi medici**, la firma elettronica avanzata utilizzata *è la* firma grafometrica applicabile, ad esempio, per semplificare la **sottoscrizione** dei **consensi informati dei pazienti** e/o **le liberatorie per la privacy**.

- **Firma elettronica qualificata (FEQ):**
  - collega i dati di una firma elettronica ad una persona fisica,
  - necessita dell'utilizzo di un apposito dispositivo contenente dati e certificati in grado di identificare univocamente il firmatario.

Un esempio di **Firma Elettronica Qualificata** è la **Tessera Sanitaria - Carta Nazionale dei Servizi (TS-CNS)** poiché è una carta con chip, contenente dati anagrafici e codice fiscale dell'interessato.

La Firma digitale, come detto in precedenza, è una FEQ che:

- *conferisce validità legale* ai documenti digitali,
- è l'equivalente elettronico della firma autografa su carta, in quanto è associata al documento elettronico sulla quale è apposta,
- *ne attesta l'integrità* (dopo che è stata apposta la firma, il documento digitale non può essere alterato in nessuna sua parte),
- *possiede autenticità* (la firma digitale certifica l'autenticità delle informazioni relative al sottoscrittore),

- *garantisce la provenienza e la non ripudiabilità* (una volta che viene apposta la propria firma digitale sul documento questo non può essere disconosciuto dal firmatario).

La *firma digitale*, soddisfacendo i requisiti giuridici della forma scritta può essere utilizzata in diversi contesti e nello specifico in campo medico trova la sua applicabilità nella sottoscrizione dei referti**,** delle prescrizioni mediche o di altri documenti sanitari che sono consegnati ai pazienti in formato digitale o inviati al sistema di Fascicolo Sanitario Elettronico (FSE).

Integrando infatti il sistema di firma digitale con soluzioni software per aziende sanitarie/ospedaliere, ambulatori, studi medici, ecc., la firma digitale semplifica ed ottimizza i processi (riduzione dei costi di carta, d'archiviazione, ecc.), nonché l'esperienza dell'intera organizzazione**.**

2.9 Valore legale firma elettronica

La ***firma grafometrica*** ha valore di "piena prova" solo se colui che ha apposto detta firma la riconosce come propria e ammette che si tratta della sua sottoscrizione. Non ha valore di prova se il soggetto presunto firmatario la contesta, ossia non la riconosce come propria. In tal caso spetta alla controparte che si avvale della firma (in tal caso l'azienda) dimostrare, invece, che la sottoscrizione appartiene al soggetto che l'ha contestata.

Un documento informatico, sottoscritto con ***firma digitale***, ha l'efficacia probatoria **"forte"** prevista dall'articolo 2702 del Codice Civile **(scrittura privata)** e fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta. In modo più pratico, chi vuole contestare la firma sostenendo che non è la propria, lo deve dimostrare. Avviene dunque l'esatto contrario di quanto descritto per la firma grafometrica, dove al presunto firmatario basta la semplice contestazione. Spetta alla controparte dimostrare il contrario. Invece, l'onere della prova nel caso della firma digitale è sul titolare del dispositivo della firma digitale**.** La normativa della firma digitale stabilisce, infatti, che l'utilizzo del dispositivo di firma digitale

si presume riconducibile al titolare, salvo che questi ne dia prova contraria e difficilmente dimostrabile. In sintesi, dunque, la **firma digitale ha validità legale**.

Un altro aspetto della normativa della firma digitale che occorre considerare è rappresentato dalla validità della firma digitale nel tempo.

Il certificato della firma digitale, che identifica il titolare, ha infatti un determinato periodo di validità e può essere nel tempo revocato o sospeso**.**

La normativa sancisce che occorre collocare con precisione il documento nel tempo, dimostrando che la firma digitale è stata prodotta in un momento in cui il certificato era ancora valido, avvalendosi del servizio di marcatura temporale (fornito dall'ente certificatore) che consente di datare il documento.

3. ***Situazione attuale***

Attualmente ogni Presidio Ospedaliero (P.O.) di Area Vasta 2 utilizza un proprio modello di consenso informato, in alcuni casi molto diverso da presidio a presidio.

In tutti i presidi il consenso informato (esame con MDC, esclusione gravidanza, biopsia, ecc.) e il modulo anamnestico in RM, viene stampato e firmato in calce da Medico Radiologo e Paziente/Tutore.

Al contrario è già implementato il sistema di firma del referto radiologico tramite Firma Digitale.

Di seguito la descrizione del workflow attuale simile in tutti i P.O; per semplicità successivamente faremo sempre riferimento a un paziente esterno che si appresta ad eseguire una TC con Mezzo di Contrasto (MDC).

3.1 Workflow attuale

- *Prenotazione*

  La prenotazione dell'esame avviene telefonicamente presso il CUP Unico Regionale oppure direttamente ad uno sportello CUP "fisico"; ***in tal caso al paziente viene consegnato il foglio dell'informativa e consenso informato da leggere e portare il giorno dell'esame***
  Viene prenotata la prestazione sul software di CUP Regionale

- *Accettazione*

  Il giorno dell'esame il paziente si presenta con impegnativa presso la Segreteria della Radiologia, consegna l'impegnativa e l'amministrativo provvederà all'accettazione della prestazione programmata sul sistema eRIS. Invierà il paziente presso la sala TC.

- *Esecuzione*

  Il paziente viene accolto dal personale addetto.
  Un colloquio anamnestico con il Medico Radiologo lo informa sull'esame TC con MDC da eseguire spiegando i rischi/benefici collegati alla somministrazione di MDC iodato.
  Se d'accordo all'esecuzione dell'esame, ***il Radiologo stampa il consenso informato e lo sottoscrivono entrambi con firma autografa.***
  Successivamente viene eseguito l'esame TC con MDC.

- *Refertazione*

  Il Medico Radiologo compila il referto e lo firma digitalmente con la smart card.

  Successivamente consegna il Consenso Informato Firmato alla Segreteria che procederà all'archiviazione.

- *Archiviazione*

  Il Referto con apposta la Firma Digitale, viene archiviato sul sistema eRIS. La Segreteria del P.O. procede all'archiviazione del Consenso Informato nel proprio archivio.

***Ogni P.O. archivia il consenso informato nei propri archivi cartacei fisici in modo autonomo*.**

4. *Progetto dell'ASUR AV2*

4.1 Materiali e Metodi

L'obiettivo di questa tesi è valutare la possibilità di provvedere ad una dematerializzazione di tutti i consensi informati impiegati nella Radiologia dell'ASUR AV2 allo scopo di consentire agli interessati di firmarli elettronicamente e archiviarli in forma digitale.

Per tale realizzazione è necessario prima di tutto utilizzare dei modelli di consenso informato univoci per tutta l'AV2; attualmente, come precedentemente descritto, ogni sede dispone di una propria modulistica.

Successivamente verranno prese in considerazione tutte le modalità di firma elettronica esistenti e valutate quelle che si addicono al nostro scopo.

Il RIS utilizzato dalla nostra azienda, analogamente a quello impiegato nelle altre realtà regionali, è "eRis" dell'azienda Exprivia.

Si procederà ad analizzate tutte le modalità di inserimento, firma e archiviazione consensi.

Verrà eseguita anche una valutazione economica del costo del workflow "cartaceo" rispetto ad un workflow "digitale", tenendo in considerazione eventuali acquisti di hardware e/o software.

4.2 Consensi Informati "Uniformi"

In considerazione che ogni presidio impiega un modello di consenso informato personalizzato, è necessario procedere innanzitutto all'uniformazione di tutti i consensi informati utilizzati, in modo da mantenere una forma di comunicazione coerente in tutti i P.O. dell'AV2.

Questa uniformità è utile per gli operatori ma soprattutto per il paziente, il quale non si troverà a dover leggere e comprendere un'informativa e consenso informato differenti da presidio a presidio.

Per tale motivo, lo scopo è creare un'informativa al paziente diversa per ogni esame da eseguire, da consegnare personalmente o trasmettere tramite mail al momento della prenotazione.
L'informativa proposta sarà priva del modulo di consenso informato che

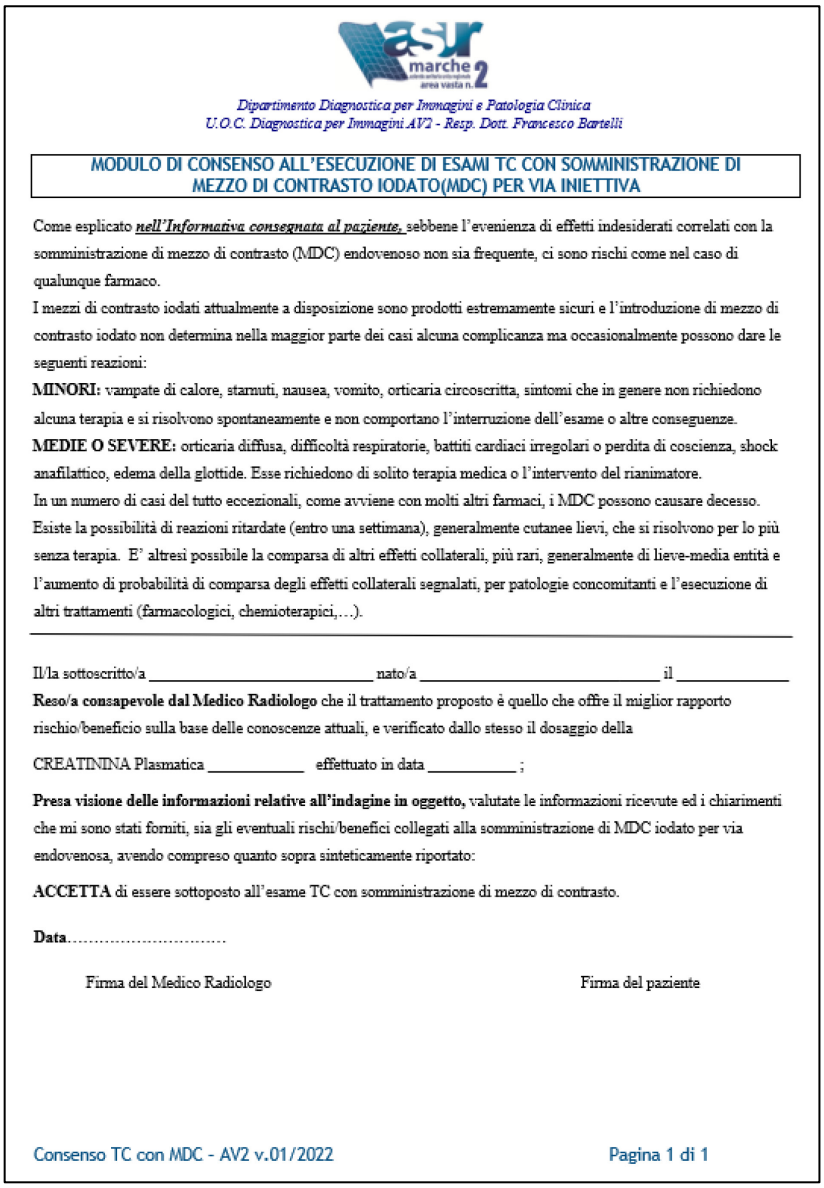
invece verrà sottoscritto in fase di esecuzione dell'esame.

La SIRM negli anni ha vagliato diversi documenti in materia ed ha stilato delle tracce su cui basare i consensi informati, i quali saranno redatti basandosi sui modelli definiti dalla SIRM e dall'esperienza clinica e professionale dei Medici Radiologi presenti nel territorio del'AV2.

Tutti i modelli verranno stilati anche prendendo in considerazione l'attuale GDPR "by design e by default".

Nel dettaglio abbiamo applicato un modello standard, riportando il logo dell'azienda, il nome del reparto e del dipartimento, il titolo del consenso informato, l'anno in cui è stato stilato, la versione e il numero delle pagine.

In allegato un esempio di consenso informato per esame TC con mdc:



Dipartimento Diagnostica per Immagini e Patologia Clinica
U.O.C. Diagnostica per Immagini AV2 - Resp. Dott. Francesco Bartelli

MODULO DI CONSENSO ALL'ESECUZIONE DI ESAMI TC CON SOMMINISTRAZIONE DI MEZZO DI CONTRASTO IODATO(MDC) PER VIA INIETTIVA

Come esplicato ***nell'Informativa consegnata al paziente,*** sebbene l'evenienza di effetti indesiderati correlati con la somministrazione di mezzo di contrasto (MDC) endovenoso non sia frequente, ci sono rischi come nel caso di qualunque farmaco.
I mezzi di contrasto iodati attualmente a disposizione sono prodotti estremamente sicuri e l'introduzione di mezzo di contrasto iodato non determina nella maggior parte dei casi alcuna complicanza ma occasionalmente possono dare le seguenti reazioni:
MINORI: vampate di calore, starnuti, nausea, vomito, orticaria circoscritta, sintomi che in genere non richiedono alcuna terapia e si risolvono spontaneamente e non comportano l'interruzione dell'esame o altre conseguenze.
MEDIE O SEVERE: orticaria diffusa, difficoltà respiratorie, battiti cardiaci irregolari o perdita di coscienza, shock anafilattico, edema della glottide. Esse richiedono di solito terapia medica o l'intervento del rianimatore.
In un numero di casi del tutto eccezionali, come avviene con molti altri farmaci, i MDC possono causare decesso.
Esiste la possibilità di reazioni ritardate (entro una settimana), generalmente cutanee lievi, che si risolvono per lo più senza terapia. E' altresì possibile la comparsa di altri effetti collaterali, più rari, generalmente di lieve-media entità e l'aumento di probabilità di comparsa degli effetti collaterali segnalati, per patologie concomitanti e l'esecuzione di altri trattamenti (farmacologici, chemioterapici,…).

Il/la sottoscritto/a _____ nato/a _____ il _____
Reso/a consapevole dal Medico Radiologo che il trattamento proposto è quello che offre il miglior rapporto rischio/beneficio sulla base delle conoscenze attuali, e verificato dallo stesso il dosaggio della

CREATININA Plasmatica _____ effettuato in data _____ ;

Presa visione delle informazioni relative all'indagine in oggetto, valutate le informazioni ricevute ed i chiarimenti che mi sono stati forniti, sia gli eventuali rischi/benefici collegati alla somministrazione di MDC iodato per via endovenosa, avendo compreso quanto sopra sinteticamente riportato:

ACCETTA di essere sottoposto all'esame TC con somministrazione di mezzo di contrasto.

Data.....

Firma del Medico Radiologo Firma del paziente

Consenso TC con MDC - AV2 v.01/2022 Pagina 1 di 1

Immagine 3 – Modulo consenso informato TC con MDC

4.3 eRIS

Il RIS che abbiamo a disposizione contiene già una sezione consenso informato (*Immagine 4 cerchiato in rosso*), all'interno possiamo inserirne uno nuovo (*Immagine 5*) cercando da quelli precedentemente già caricati su eRIS (*Immagine 6*), poi come vediamo nell'*Immagine 7* possiamo flaggare la consegna e la firma.

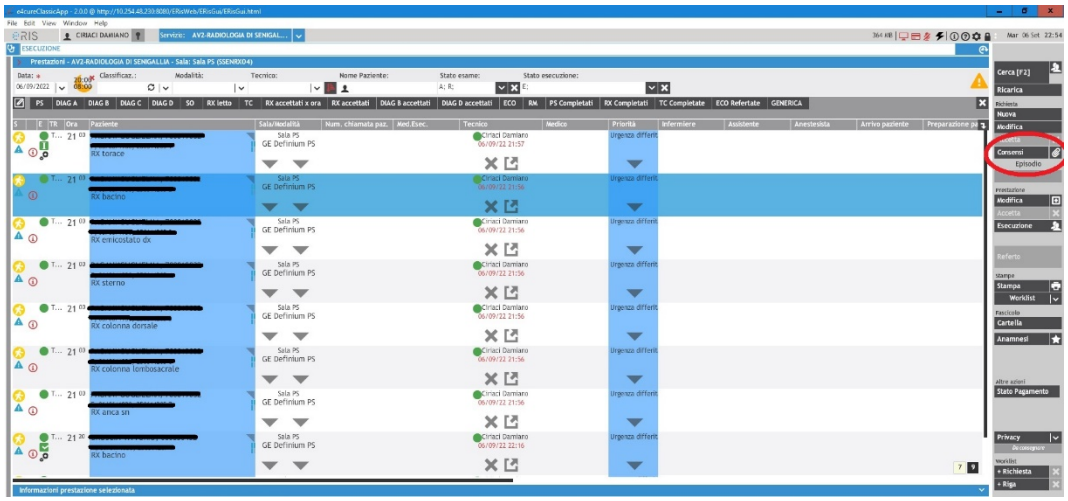


Immagine 4 – Schermata eRIS

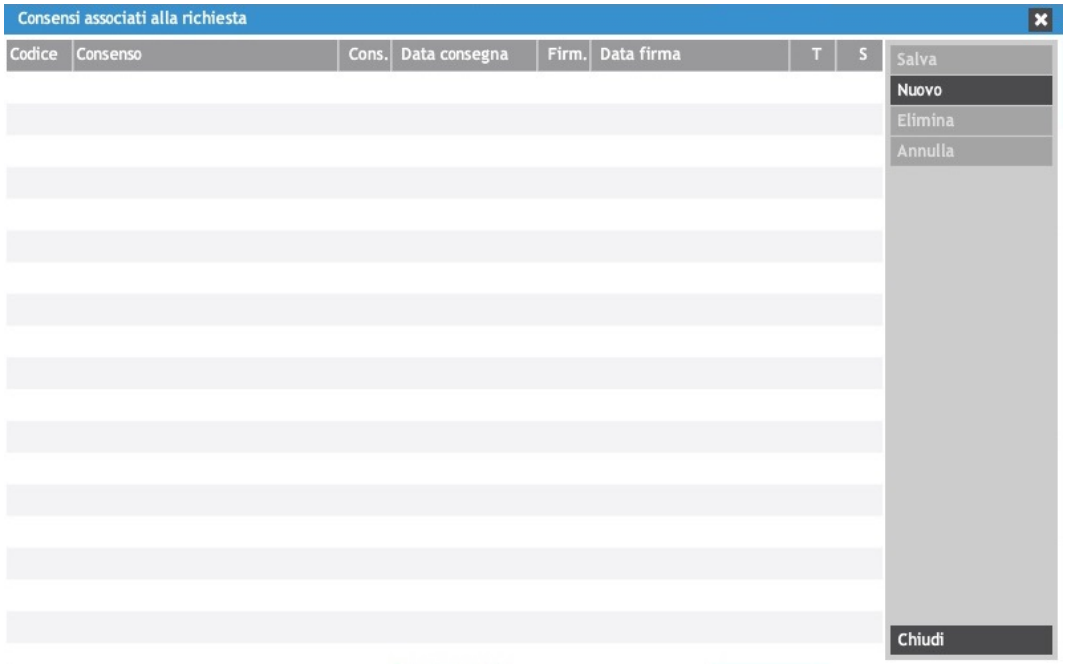


Immagine 5 – Consensi associati alla richiesta eRIS

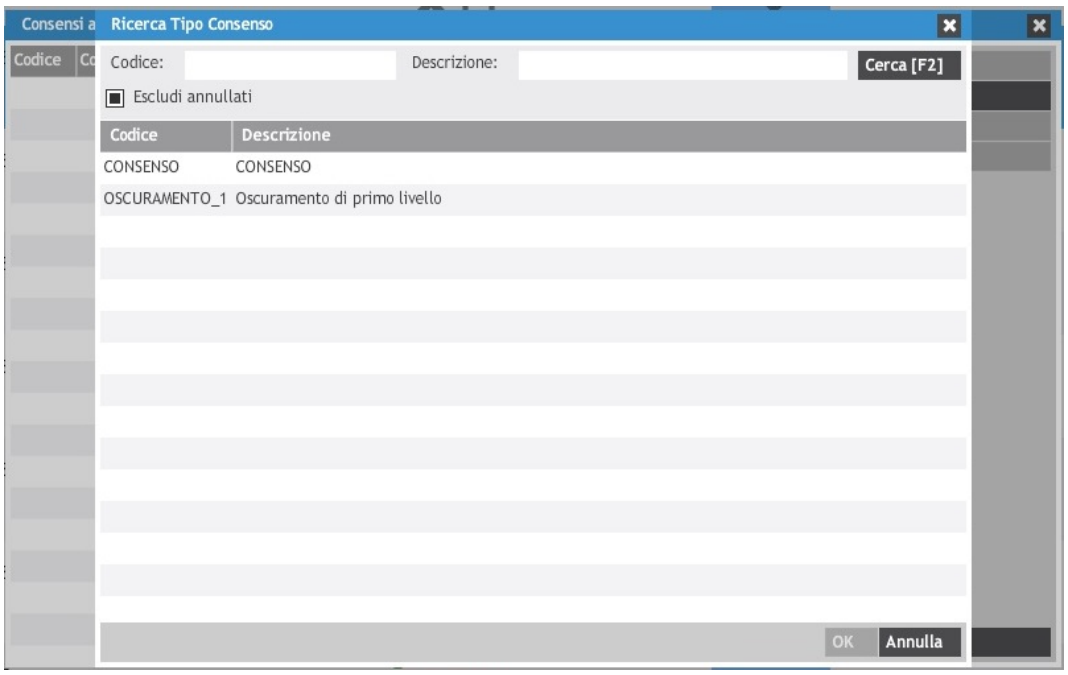


Immagine 6– Ricerca Consensi

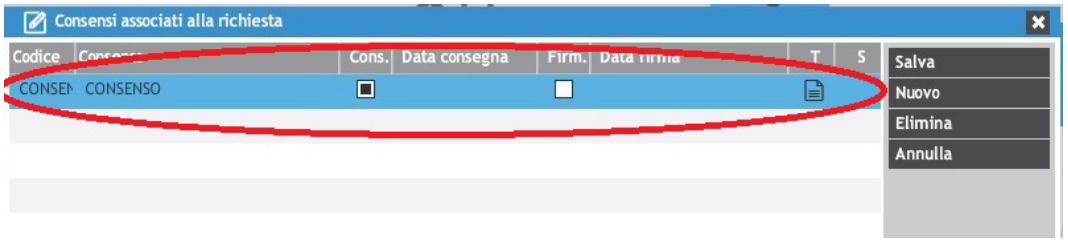


Immagine 7 – Consensi associati alla richiesta

Inoltre, dall'apposito modulo allegati a fianco ai consensi con il simbolo "graffetta" (*Immagine 4 cerchiato in rosso*), è possibile consultare tutti gli allegati compresi i consensi(*Immagine 8*).

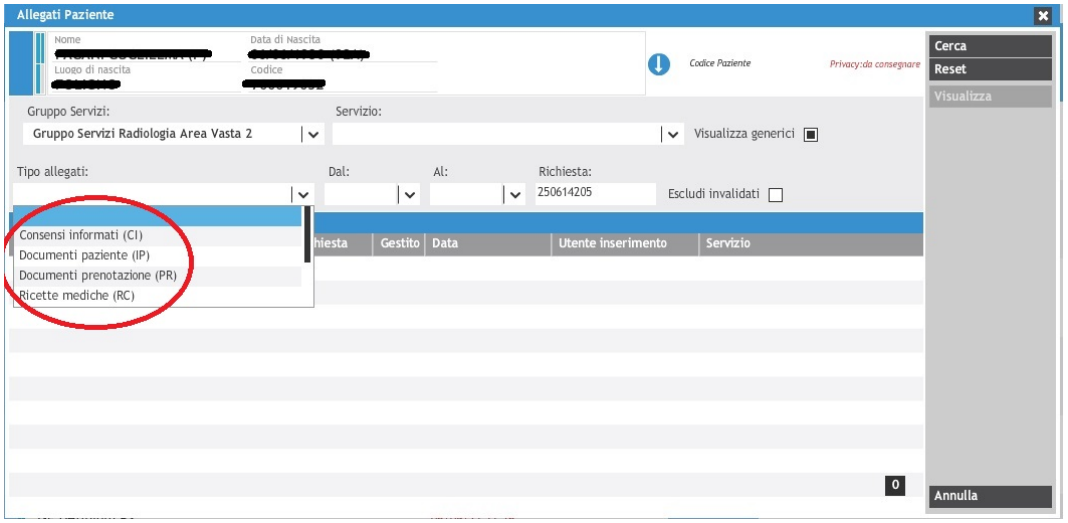


Immagine 8 – Allegati paziente

4.4 Firme Elettroniche: quali fanno al nostro caso

Le firme precedentemente analizzate visto la loro divulgazione negli ultimi anni e semplicità d'uso sono senza dubbio:

- SPID
- CNS-TS o Smart Card
- CIE

La CNS-TS è la più diffusa in quanto tutti i cittadini ne sono in possesso al giorno d'oggi e viene utilizzata molto spesso o quasi sempre per accedere ai servizi sanitari ma, la maggioranza, non ne comprende le potenzialità e molti non hanno mai attivato la CNS al suo interno.

Le prime consentono di avere un elevato grado di sicurezza essendo entrambe FEQ, mentre per tutti i tre i sistemi non abbiamo bisogno di raccogliere nessun dato personale del paziente, in quanto il riconoscimento nei sistemi avviene tramite enti certificatori.

Tuttavia, in alcuni contesti (Pronto Soccorso, Urgenza/Emergenza, ecc.) il paziente si potrebbe trovare impossibilitato a utilizzare SPID, CNS-TS o CIE per poter firmare, senza tenere in considerazione i cittadini "non al passo coi tempi" che potrebbero non essere in grado di utilizzare gli strumenti di cui sopra.

A tal proposito si potrebbero verificare due possibili scenari: il primo potrebbe consistere nell'utilizzo del metodo "cartaceo" effettuando una scansione del documento firmato; l'alternativa, utilizzare una firma "più facile da reperire" come la Firma Grafometrica.

La Firma Grafometrica in questi casi aiuta perché consente di non utilizzare la carta, e permette al contempo una Firma Elettronica e l'archivio digitale "diretto".

4.5 Come funzionano le Firme Elettroniche

4.5.1 TS-CNS

Dal 2011 e per i cittadini maggiorenni [S3], se la tessera è dotata di microchip è possibile abilitare la Tessera Sanitaria come Carta Nazionale dei Servizi (CNS).

Di seguito i passaggi da seguire per l'abilitazione, che consente di utilizzare la tessera come strumento di autenticazione per accedere ai servizi online della pubblica amministrazione e alla Firma Digitale.

a. *Attivazione della TS-CNS*

   Per attivare la propria tessera sanitaria come strumento di autenticazione è necessario che il cittadino recuperi i codici PIN, PUK e CIP relativi alla propria TS-CNS presso gli sportelli regionali abilitati, presentando la tessera sanitaria e un documento di identità.

Se si è in possesso di una TS-CNS già attiva (e del codice PIN) non ancora scaduta, al ricevimento della nuova per attivarla si può utilizzare il servizio on line.

b. *Registrazione della TS-CNS, dopo aver recuperato PIN e PUK*

   Sarà necessario a tale scopo:

   - un computer con connessione ad Internet;
   - un lettore di smart card correttamente installato.

   Per concludere l'abilitazione della TS-CNS è essenziale inserire la tessera nel lettore di smart card ed effettuare la registrazione.

c. *TS-CNS abilitata*

   A questo punto, è possibile eseguire l'accesso alle aree autenticate e alla Firma Digitale attraverso la TS-CNS inserendo la smart card nel lettore e il codice PIN quando viene richiesto.

Per firmare digitalmente avrete bisogno solo della vostra *TS-CNS e il PIN*, ovviamente chi offre il servizio di Firma dovrà predisporre di un lettore smart card.

4.5.2 SPID

Il documento stilato dall'AgID [1] per la firma con lo SPID prevede tre figure: il *fornitore di servizi nella federazione SPID (SP), i gestori di identità digitali nel contesto della federazione SPID (IdP) e l'utente finale, il cittadino.*

È importante che il SP conosca il codice fiscale del firmatario; il SP quindi:

a. presenta all'utente la sezione "Firma con SPID", alla cui selezione il SP mostra l'elenco dei IdP che offrono il servizio di firma. L'utente seleziona il proprio IdP e si autentica inserendo utente/password o acquisendo il QR Code se disponibile;
b. il SP predispone il documento (documento predisposto per la firma, nel nostro caso il consenso informato), apponendovi un proprio sigillo elettronico qualificato sottoponendolo, presso la propria piattaforma, all'utente affinché possa essere visionato, eventualmente scaricato e conservato;
c. il SP rende manifesto all'utente che il processo prevede l'invio del documento all'IdP prescelto, acquisendone il consenso esplicito. L'utente è anche avvisato in modo chiaro e manifesto che tale documento gli sarà reso successivamente disponibile dal proprio IdP, e gli viene consigliato di leggerlo nuovamente in tale occasione. Per proseguire l'utente seleziona la sezione "Prosegui con la Firma";
d. il SP invia il documento predisposto per la firma al punto b dell'IdP e, avuta evidenza del successo dell'invio, inoltra la sessione dell'utente al relativo IdP con una richiesta di autenticazione speciale (di livello pari almeno a 2), denominata "firma con SPID". Tale richiesta contiene il codice fiscale del soggetto che deve apporre la firma, acquisito al punto a.

Consenso alla sottoscrizione (presso l'IdP)

a. L'IdP procede con l'autenticazione dell'utente con credenziali di livello 2 o superiore, verificando che si tratti del firmatario atteso dal SP in base al codice fiscale ricevuto con la richiesta di cui al *punto d della precedente procedura.*

b. Informa l'utente che il processo di autenticazione è volto alla sottoscrizione, comunicando all'utente il nome del SP che sta richiedendo la sottoscrizione del documento e il nome del file contenente il documento in oggetto.
c. Consente all'utente di visionare il documento e scaricarlo.
d. Propone all'utente di procedere con la sottoscrizione. Il dissenso alla sottoscrizione da parte dell'utente comporta l'invio di una risposta di autenticazione con esito negativo al SP e il termine del processo.
e. Visualizza la pagina destinata a contenere il contenuto grafico del sigillo elettronico qualificato, informando l'utente in merito alla obbligatorietà o facoltatività della firma.
f. Acquisisce il consenso dell'utente ad apporre la firma.
g. Procede alla apposizione del sigillo elettronico qualificato (o di più sigilli nel caso siano previste più firme), formando dunque il documento firmato con SPID.
h. Propone all'utente di inviargli il documento firmato con SPID via posta elettronica, e/o di scaricarne una copia, e/o di renderglielo disponibile nella propria area riservata in base al servizio.
i. Invia al SP il documento firmato con SPID con le modalità descritte nel documento.
j. Invia al SP la risposta di autenticazione della firma SPID recante l'esito positivo della procedura, reindirizzando l'utente presso il SP. Nel caso in cui il punto precedente non abbia successo, l'IdP informa l'SP e l'utente in merito al mancato successo del processo di firma.

Il processo di cui ai *punti f e g è reiterato per ogni firma*.

Al termine del processo qui descritto, salvo che l'utente non abbia scelto di avvalersi dei servizi di conservazione dei documenti firmati, l'IdP rimuove dai propri sistemi il documento oggetto della sottoscrizione, nel pieno rispetto di quanto disposto dal Regolamento GDPR.

4.5.3 Firma CIESign

La Carta di Identità Elettronica **(**CIE**)** è rilasciata dallo Stato italiano [3] e può essere utilizzata come **dispositivo di firma elettronica avanzata** (**FEA**) per firmare documenti elettronici.

Per firmare un file con la Carta di Identità Elettronica si usano metodi molto simili a SPID , solo che in questo caso occorre esserne materialmente in possesso (modalità di firma "in locale"), e conoscere il PIN.

La firma con CIE è possibile in tutte le Pubbliche Amministrazioni che ne consentono l'uso con l'apposito banner "*Firma con CIE*".

Attualmente sono disponibili due modalità di firma.

- "*Desktop"* – la firma elettronica avviene tramite un computer collegato a un lettore di smart card contactless per la lettura della CIE, su cui deve essere installato il "Software CIE". La verifica della firma elettronica nella modalità Desktop può essere effettuata con l'app "CIE ID";
- "*Mobile*" – la firma elettronica avviene tramite uno smartphone dotato di interfaccia NFC su cui deve essere installata l'app "**CieSign**", che permette anche di effettuare la verifica della firma elettronica.

4.5.4 Firma grafometrica - utilizzo

La FG a livello di utilizzo è la più semplice poiché si firma come per qualsiasi documento cartaceo.

Se l'utente è già stato riconosciuto e ha depositato la sua FG, può procedere all'utilizzo della FG presso l'azienda.

All'utente viene fatto visionare il documento da firmare: se d'accordo appone la sua firma sul tablet che viene registrata e applicata al documento in oggetto.

La firma grafometrica ha valore probatorio a tutti gli effetti di legge, così come la firma apposta manualmente su un documento cartaceo. Diventa quindi un utile strumento per il miglioramento e la dematerializzazione dei documenti sanitari**.**

5. ***Fase Operativa***

In base all'analisi della situazione attuale, ai consensi informati a disposizione e alla tipologia di Firme Elettroniche proposte per l'utilizzo, verranno proposti dei miglioramenti e degli upgrade hardware e software.

Innanzitutto, data la tipologia di documento simile al referto Medico, è consigliabile utilizzare una firma PaDES, che utilizzando i *.pdf* porta con sé molteplici vantaggi in chiave di successiva consultazione e archiviazione, nonché di firma.

5.1 Dematerializzazione Consensi - eRIS

Il RIS contiene già dei moduli per raccogliere il consenso informato e alcuni strumenti per la sottoscrizione della Firma Digitale con Smart Card.

Sarà indispensabile dematerializzare i consensi informati in file *.pdf* editabile per inserirvi alcuni dati (come la creatinina plasmatica) per poterli aggiungere all'interno di eRIS. Gli stessi devono essere disponibili per la doppia firma del Medico Radiologo e del paziente.

Per far ciò abbiamo bisogno di integrare con eRIS i software di firma TS-CNS, SPID, CIE e gli strumenti per la FG.

Una volta firmato da entrambe le parti il file con firma PaDES viene archiviato alla voce "Consenso" nella cartella paziente del sistema eRIS.

In relazione ai dati del paziente, nel nostro RIS, in caso di necessità di stampa dei consensi, si avrà la compilazione automatica dei campi nome, cognome, data di nascita ed eventualmente anche di dati inerenti alla prestazione; tale funzione è applicabile anche ai nuovi consensi informati.

5.2 Firma Elettronica: come fare?

Il software che verrà utilizzato nel processo di acquisizione della firma elettronica deve prevedere sia l'uso e gestione delle FEA (FG, CIESign,ecc..) e anche delle FEQ (SPID, SmartCard, Firma Remota, ecc…).

Le applicazioni dell'azienda sanitaria che necessitano di apporre una firma elettronica ad un documento informatico lo trasmettono all'apposito applicativo, il quale si occupa di tutte le fasi dell'acquisizione della firma.

Il software, una volta acquisita la firma, invia all'applicazione chiamante, nella fattispecie eRIS, un documento informatico contenente la firma elettronica dell'interessato. Tale documento viene poi controfirmato con firma digitale dal Medico.

L'apposizione della FG, SPID, CIESign avviene tramite specifiche postazioni di lavoro sulle quali è installato il modulo software ed è connesso con il dispositivo hardware tablet che rende possibile l'acquisizione del tipo di firma scelta, nonché la visualizzazione a schermo del documento che verrà sottoscritto.

Tutte le postazioni di lavoro dovrebbero esser censite dalla società fornitrice della soluzione di firma per proteggere il certificato pubblico, con il quale sono cifrati i dati biometrici e i gestori di identità digitali.

5.3 Implementazione Hardware/Software

Per effettuare questa implementazione sarà necessaria una valutazione dell'Hardware/Software da acquistare o aggiornare.

Come sopra riportato, si provvederà alla dematerializzazione dei consensi informati firmandoli elettronicamente ed archiviandoli digitalmente.

Per la dematerializzazione dei consensi abbiamo già parlato di come gli stessi verranno creati in formato pdf ed integrati in eRIS nell'apposita sezione.

Per quanto riguarda la firma abbiamo progettato l'utilizzo di SPID, TS-CNS, CIE e in assenza di queste la firma grafometrica.

Per la firma grafometrica sarebbe necessario l'acquisto di una tavoletta grafica, non utilizzabile per le altre tipologie di firma, mentre l'impiego di

tablet risulterebbe idoneo allo scopo e soprattutto molto utile per la rappresentazione sullo schermo del consenso che il paziente sarà chiamato a sottoscrivere. L'interazione con il tablet nei vari passaggi e nel caso di SPID o CIE-ID consentirebbe di visualizzare il QRCode oppure immettere user e password.

La nostra azienda tramite il portale Cohesion della Regione Marche già permette di utilizzare tali strumenti (*Immagine 9*) per l'accesso ad alcuni servizi. Sarebbe interessante ed utile poter utilizzare lo stesso sistema di autenticazione anche per la Firma Elettronica, dato che l'azienda e la Regione Marche già ne sono fornite. Anche in una prospettiva economica si otterrebbe un vantaggio notevole.

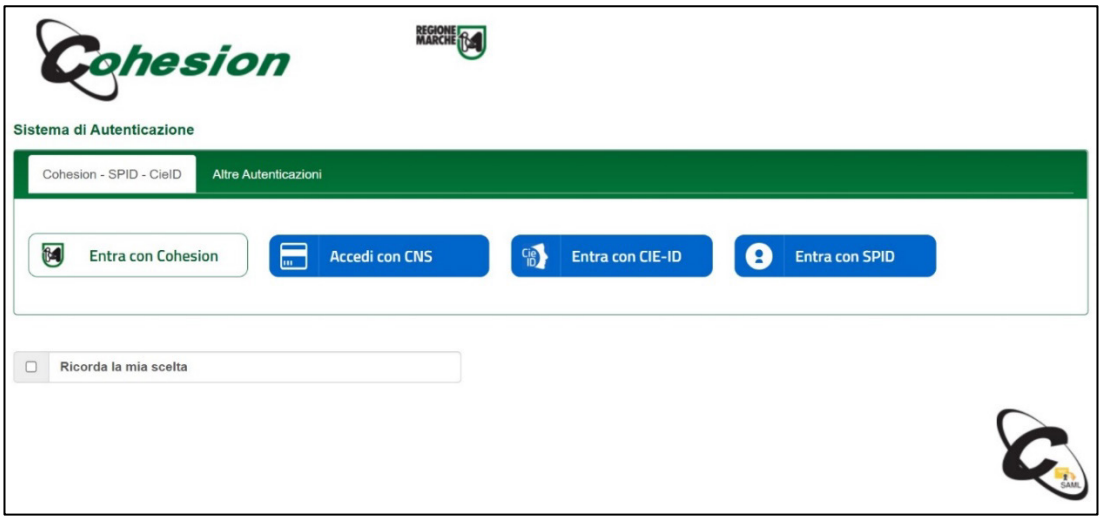


Immagine 9 – Sistema di autenticazione Cohesion

Per tutti i motivi sopra elencati l'utilizzo del tablet risulta la scelta migliore; ne dovrà essere presente uno in ogni diagnostica radiologica che prevede l'utilizzo di m.d.c., in quanto alcuni tipi di consenso, quale quello relativo all'esclusione dello stato di gravidanza, sono utilizzati in quasi tutta la diagnostica per immagini.

Ovviamente per l'impiego della TS-CNS sarà necessario l'acquisto di lettori smart card in aggiunta ai tablet.

Nel caso dei software, qualora non si possa utilizzare il portale Cohesion per la firma, dovremmo mettere in progetto l'acquisto di software per la firma oltre all'upgrade di hardware e software per l'interazione con eRIS.

5.4 Nuovo Workflow

- *Prenotazione*

  La prenotazione dell'esame avviene telefonicamente al CUP Unico Regionale oppure direttamente ad uno sportello CUP "fisico" ***in tal caso al paziente viene consegnato il foglio dell'informativa e consenso informato da leggere e portare il giorno dell'esame***. Viene prenotata la prestazione sul software di CUP Regionale

- *Accettazione*

  Il giorno dell'esame il paziente si presenta con impegnativa presso la Segreteria della Radiologia, consegna l'impegnativa e l'amministrativo provvederà all'accettazione della prestazione programmata sul sistema eRIS. ***Informa inoltre il paziente che può firmare il consenso informato e i documenti sanitari, in modalità elettronica, se è in possesso di TS-CNS, SPID, CIE può firmare con queste modalità altrimenti con FG.*** Ovviamente come abbiamo già descritto la FG necessità in fase di primo utilizzo dell'identificazione "fisica" del cittadino. Infine l'amministrativo invierà il paziente presso la sala TC.

  Esecuzione

  Il paziente viene accolto dal personale addetto. Un colloquio anamnestico con il Medico Radiologo lo informa sull'esame TC con MDC da eseguire spiegando i rischi/benefici collegati alla somministrazione di MDC iodato. Se d'accordo all'esecuzione dell'esame, ***il Radiologo fa visualizzare il consenso informato sul tablet e il paziente lo sottoscrive con TS-CNS, SPID, CIE o FG, mentre il Radiologo lo valida con la sua Firma Digitale.***

  Successivamente viene eseguito l'esame TC con MDC.

- *Refertazione*

  Il Medico Radiologo compila il referto e lo firma digitalmente con la

Smart Card.

- *Archiviazione*

  Il referto e il ***consenso informato con apposte le firme elettroniche vengono archiviati nella cartella paziente alla voce "Consensi" nel sistema eRIS.***

6. *Analisi dei Costi*

Per poter misurare in termini economici i numeri di cui parliamo, si è pensato di stimare dei costi nelle metodiche in cui si sottoscrivono più consensi informati, ossia per Esami TC con MDC e RM con e senza MDC, facendo una stima degli esami eseguiti da Gennaio a Giugno 2022 in tutti i P.O. dell'AV2.

Per fare questa statistica purtroppo il nostro RIS analizza solo il numero di prestazioni e non di pazienti, ovviamente un paziente che esegue quattro prestazioni RM (esempio: RM Encefalo senza e con MDC, Angio RM, RM Collo…) firma un solo modulo anamnestico e un solo consenso informato; quindi, abbiamo necessità di normalizzare questo dato.

Per fare ciò valuteremo il rapporto numerico prestazioni/pazienti all'interno di una settimana tipo, che è stata scelta in base ad un periodo routinario di attività (lontano da Festività, scadenze, ecc..), prenderemo in considerazione la settimana dal 21 al 27 Marzo 2022, per ricavare questo dato.

Questo ci consente di stimare il numero di pazienti e i costi derivati dal consumo di carta/toner in 6 mesi di attività recente.

Successivamente verranno stimati anche i costi Hardware e Software da acquistare per la dematerializzazione completa.

Stimando dei costi medi per una risma da 500 fogli di carta A4 da 80g/m^2 per stampa durevole nel tempo di una marca molto diffusa, il costo è di circa 5,50 € a risma.

Tenendo in considerazione le stampanti più diffuse dell'AV2 e i toner che acquista l'azienda, il costo medio è di circa 400 € a stampante e di 100 € a

Toner per stampa in Bianco e Nero originale che stampa in media 2500 fogli.

Immaginiamo di avere in dotazione organica una stampante per uso di ogni singola TC e una per ogni RM, e di stampare un 1 foglio di consenso informato (CI) per TC con MDC, 1 foglio di modulo anamnestico (MA) per RM senza MDC e 2 fogli (MA+CI) per RM con MDC.

Le dotazioni TC e RM dell'Area Vasta 2 sono:

- Senigallia 1 – 1 TC e 1 RM
- Fabriano – 2 TC e 1 RM
- Jesi – 2 TC e 1 RM
- Loreto – 1 RM

Nella *Tabella 2* abbiamo ricavato il numero di pazienti dal numero delle prestazioni, con il numero dei pazienti abbiamo stimato nella *Tabella 3* i costi delle stampe del 1° semestre 2022, mentre nella successiva *Tabella 4* sono stati stimati i costi per l'installazione dei sistemi per le firme elettroniche.

In questa stima non abbiamo tenuto conto dei lettori di smart card (che in alcuni casi sono già presenti) e nel caso di nuove installazioni hanno un costo irrisorio (circa di 25€ caduno), dei costi annuali di gestione ed assistenza del servizio. Non si è tenuto conto del costo dei lettori smart card soprattutto perché sono delle spese che si vanno a dividere su tutti i processi da dematerializzare, e non tenendo in considerazione tutti i documenti in questa stima questo dato è stato volutamente omesso.

Sono stati calcolati un numero di tablet pari ad uno per diagnostica e uno per ogni sportello di segreteria.

Calcolando il numero di stampanti pari al numero di Tablet da utilizzare, abbiamo calcolato con la seguente formula gli anni necessari per pareggiare l'investimento delle firme elettroniche.

$$\frac{\boldsymbol{Costo\ avvio\ FE - (Costo\ cad.stampanti\ \times\ n.stampanti)}}{\boldsymbol{Costo\ annuale\ stampe}} = \boldsymbol{N.anni}$$

Tradotto in numeri:

$$\frac{\mathbf{19.500 - (400\ \times\ 19)}}{\mathbf{(850,12\ \times\ 2)}} = \mathbf{6,99}$$

Ovviamente questo dato si riferisce solo ai consensi in oggetto, se pensiamo quanti altri consensi informati (gravidanza, biopsie, ecc…) possiamo dematerializzare e a quanti altri servizi ospedalieri possiamo estendere queste tecnologie, va da sé che anche aumentando i costi per gli hardware, manutenzione e gestione avremo bisogno di molto meno tempo per ammortizzare l'investimento iniziale.

Tabella 2 – Prestazioni ed Esami eseguiti 1 semestre 2022

P.O.	Numeri Esami			Fattore conversione esami/pazienti		Numero Pazienti			TOTALE PAZIENTI
	RM noMDC	RM MDC	TC	RM	TC	RM noMDC	RM MDC	TC	
Senigallia	802	682	2.618	1,360	1,586	590	501	1.651	2.742
Fabriano	350	858	2.290	1,140	1,429	307	753	1.603	2.662
Jesi	1.405	773	4.422	1,240	1,422	1.133	623	3.110	4.866
Loreto	1.025	2	0	1,247	0,000	822	2	0	824

Tabella 3 – Costo stimato stampe 1 semestre 2022

P.O.	Numeri Pazienti			Numero Risme 500 fogli A4		TOTALE RISME	Numero Toner B/N 2500 fogli		TOTALE TONER	TOTALE € Carta	TOTALE € Toner	TOTALE €
	RM noMDC	RM MDC	TC	RM	TC		RM	TC		5,5 € cad	100 € cad	
Senigallia	590	501	1651	3,19	3,30	6,49	0,64	0,66	1,30	35,68	129,73	165,41
Fabriano	307	753	1603	3,62	3,21	6,83	0,72	1,28	2,01	37,56	200,69	238,26
Jesi	1133	623	3110	4,76	6,22	10,98	0,95	2,49	3,44	60,38	343,97	404,35
Loreto	822	2	0	1,65	0,00	1,65	0,33	0,00	0,33	9,08	33,02	42,10

TOTALE A.V.2 €	**850,12**

Tabella 4 – Costo stimato installazione Hardware/Software

P.O.	Numero POSTAZIONI			Totale Tablet	Totale Costo Tablet	Costi Installazione una Tantum €	TOTALE AVVIO €
	Segreteria	RM	TC		500€ cad.		
Senigallia	3	1	1	5	2.500	3.000	5.500
Fabriano	3	1	2	6	3.000	3.000	6.000
Jesi	3	1	2	6	3.000	3.000	6.000
Loreto	1	1	0	2	1.000	1.000	2.000
TOTALE AV 2	10	4	5	19	9.500	10.000	**19.500**

7. *Discussione*

La dematerializzazione è un processo che ha come obiettivo la creazione di un flusso di documenti digitali aventi pieno valore giuridico, che vada prima ad affiancare e poi, sul lungo periodo, a sostituire la normale documentazione cartacea negli archivi di qualunque attività pubblica o privata.

In Italia una sperimentazione sulla Dematerializzazione del Consenso Informato (DCI) effettuata in ambito Radiodiagnostico, è quella effettuata dalla SIRM, riportata nel "Documento di sintesi della Sperimentazione - Dematerializzazione del Consenso Informato in ambito radiologico" a cui hanno aderito 16 strutture di Radiodiagnostica e diverse aziende IT.

Tale sperimentazione aveva i seguenti obiettivi:

a) Identificare le migliori soluzioni tecnologiche per l'implementazione della DCI;
b) sperimentare l'utilizzo della DCI in diversi ambiti radiologici;
c) misurare l'impatto della DCI sull'attività di un reparto di radiologia;
d) identificare vantaggi e svantaggi dell'applicazione della DCI sui flussi di lavoro radiologico.

Solo 8 centri hanno portato a termine la sperimentazione.

Tutti i centri coinvolti nella sperimentazione hanno identificato e utilizzato per la firma del consenso informato e del questionario anamnestico per i pazienti lo strumento di firma grafometrica, mentre per il medico dell'area radiologica è stato utilizzato lo strumento di firma elettronica qualificata. La sperimentazione ha quindi avuto esito positivo con buona adesione dei pazienti e disponibilità da parte del personale medico, tecnico e amministrativo a partecipare a tutte le fasi di realizzazione del progetto.

Le linee Guida SIRM-AgID sono state pubblicate anche nella Gazzetta Ufficiale (GU) Serie Generale n.65 del 19-03-2018, per mezzo del Comunicato concernente la circolare n. 1 del 24 gennaio 2018, recante: «Linee guida per la dematerializzazione del consenso Informato in diagnostica per immagini».

Inoltre, anche Quotidiano Sanità [S4] nel Maggio 2018 ha pubblicato un articolo *"Il consenso informato si fa digitale. Prima sperimentazione nell'area radiologica. Circolare AgID su metodi e tecnologie"* dando risalto alla notizia.

Con la finalità di comprendere la propensione dei medici dell'area radiologica verso la dematerializzazione del CI i soci SIRM sono stati invitati a completare un questionario composto da 15 domande [4]. Al sondaggio hanno aderito 1791 radiologi (18% del totale di iscritti SIRM) e la grande maggioranza dei rispondenti (95%) si è dimostrata favorevole al DCI.

I Principali Vantaggi e Svantaggi della soluzione adottata secondo il parere dei rispondenti al questionario, sono elencati sotto (*Tabella 5*):

Tabella 5 – Vantaggi e Svantaggi Radiologi SIRM

Vantaggi	**Svantaggi**
Archiviazione digitale del consenso informato, procedura più sicura rispetto all'archiviazione del consenso informato cartaceo.	*Procedura complessa, poiché richiede l'implementazione della firma grafometrica, che a sua volta prevede una prima fase di identificazione e registrazione del pz, che deve esibire la carta d'identità e dare il consenso alla firma grafometrica.*
Facile e veloce recupero del documento in caso di necessità (contenziosi medicolegali) rispetto al documento in formato cartaceo (archivi tradizionali spesso dislocati dal nosocomio).	*Necessità di coinvolgimento uffici competenti (uff. legale, uff. privacy, responsabile archiviazione e conservazione dati), necessita stipula assicurazione (non del tutto compresa dai broker e dagli enti sanitari stessi).*
Riduzione del consumo di carta e quindi dei costi di archiviazione.	*Impossibilità di essere utilizzata nei pazienti che vogliono mantenere l'anonimato non esibendo il documento d'identità ma solo la carta dei servizi (sufficiente per sottoporsi ad indagine radiologica), in questi casi deve essere utilizzato il percorso tradizionale con firma su cartaceo.*
Identificazione certa del titolare della firma	Necessità di spazi dedicati dove predisporre i tablet per firma grafometrica.
Acquisizione certa delle variabili di consenso in modo tale da poter essere interrogabili per statistiche o classificazioni	Procedimento gravoso per il personale sanitario
Completa tracciabilità di ogni fase del processo di firma	*Difficoltà e a volte impossibilità alla firma grafometrica per pazienti affetti da patologie motorie (es sclerosi multipla) che invece riescono a firmare il documento cartaceo.*

Si evince che alcuni di questi svantaggi sottolineati in realtà siano oramai risolti dalle firme con TS-CNS, SPID e CIE che sono più facili da utilizzare (basti pensare alla TS-CNS che altro non è che una carta con il PIN, non vi ricorda qualcosa?

Quante volte usiamo il Bancomat/Carta di credito ogni giorno; carta con PIN.

Invece, per l'utilizzo dello SPID, è sufficiente possedere uno smartphone, mentre per la CIESign è necessario possedere la CIE, il PIN e uno smartphone.

Siamo già preparati ad utilizzarle, ma la "pigrizia tecnologica" e la scarsa accettazione di essa ne rende difficile l'attuazione. Molte cose stanno cambiando in tal senso in questi ultimi anni, anche a causa della pandemia. Infatti, si è registrato un maggior impiego dei dispositivi elencati con conseguenti nuove attivazioni, e nel caso della CIE anche la sua progressiva sostituzione alla Carta Identità Cartacea.

Ricordiamo anche che nel 2018 alcuni dei servizi come SPID e CIE erano ancora agli arbori. Per quanto riguarda lo SPID sono entrate in vigore solo dal 4 maggio 2021 le Linee Guida per firmare documenti online [1].

La CIE che conosciamo oggi (detta CIE 3.0) viene prodotta da inizio 2016, ma solo nel 2019, con l'abilitazione di tutti i comuni a sostituire la carta d'identità cartacea con la CIE, inizia la vera diffusione di questo strumento.

Il manuale d'uso riguardo alla CIE è stato pubblicato solo pochi mesi fa, ovvero il 28/03/2022.

Si denota, inoltre, che fino a quattro anni fa avevamo poche possibilità (oltre alla FG) per firmare documenti sanitari e in così pochi anni, anche grazie alla spinta dall'Unione Europea, abbiamo visto l'affermarsi e la divulgazione di una vasta scelta di strumenti digitali per la firma.

In altri settori diversi dalla sanità la dematerializzazione dei documenti sta prendendo campo, ma nel cercare di attuare questo processo in sanità abbiamo visto che lo “scoglio” più grande è il riconoscimento digitale del cittadino e la sua firma.

Quanto sono diffusi questi strumenti tra la popolazione italiana? Di quali numeri stiamo parlando?

Partiamo intanto dalla considerazione fatta poc’anzi che non possono sottoscrivere il consenso informato i minori e le persone “incapaci”. Non disponendo di dati certi delle persone incapaci in Italia, in considerazione che questo lederebbe la loro privacy ai sensi del GDPR, faremo riferimento al fatto che tutti i maggiorenni siano abili.

L’ISTAT stima che in Italia ci sono 58.983.122 persone residenti al 1° Gennaio 2022.

I minori di anni 18 risultano pari a 9.199.286, e sottraendo questi valori abbiamo come risultano un numero di 49.783.836 cittadini maggiorenni: quasi 50 milioni.

Analizzeremo quali sistemi di firma, tra quelli che andremo a implementare, siano più diffusi e come incidono.

7.1 Firma digitale: più di 20 milioni le utenze attive

Secondo il monitoraggio che AgID [S5] (*Tabella 6 e Grafico 1)* hanno effettuato sui dati forniti dai certificatori accreditati, a giugno 2022 (e da maggio 2014) sono oltre 27 milioni le utenze attive di firma digitale (e di conseguenza i certificati qualificati). Di queste l'80% si basa su firma digitale remota (che non richiede l'utilizzo di smart card o token). Sempre nel 2022, risultano quasi 3 miliardi le firme digitali remote generate *(Grafico 2).*

Tabella 6 – Monitoraggio AgID Firme Digitali

Periodo di rilevamento	Certificati qualificati di firma digitale attivi (cumulativo a fine periodo)		Numero di firme digitali remote generate nel periodo
	Totale	*di cui con firma remota (%)*	
Avvio - Mag 14	5.319.800	*n.d.*	n.d.
Giu 14 - Lug 15	8.104.615	*55,00%*	n.d.
Lug 15 - Apr 16	11.170.257	*60,00%*	n.d.
Mag 16 - Dic 16	14.400.872	*60,00%*	665.206.174
Gen 17 - Giu 17*	18.880.320	*72,35%*	804.513.324
Lug 17 - Dic 17	18.657.725	*81,48%*	1.071.865.899
Gen 18 - Giu 18	20.690.513	*82,74%*	971.137.425
Lug 18 - Dic 18	20.288.382	*81,96%*	1.034.548.974
Gen 19 - Giu 19	20.652.065	*80,40%*	1.429.713.138
Lug 19 - Dic 19	22.067.401	*81,41%*	1.681.406.616
Gen 20 - Giu 20	22.482.521	*82,44%*	1.679.899.416
Lug 20 - Dic 20	24.656.235	*79,23%*	1.968.699.786
Gen 21 - Giu 21	26.265.987	*81,65%*	2.202.413.066
Lug 21 - Dic 21	29.235.137	*84,98%*	2.615.823.004
Gen 22 - Giu 22	27.413.067	*83,50%*	2.818.664.581

* Il dato relativo ai certificati qualificati di firma digitale attivi si riferisce al 31 luglio 2017

Grafico 1 – *Firme Digitali attive (cumulativo a fine periodo)*

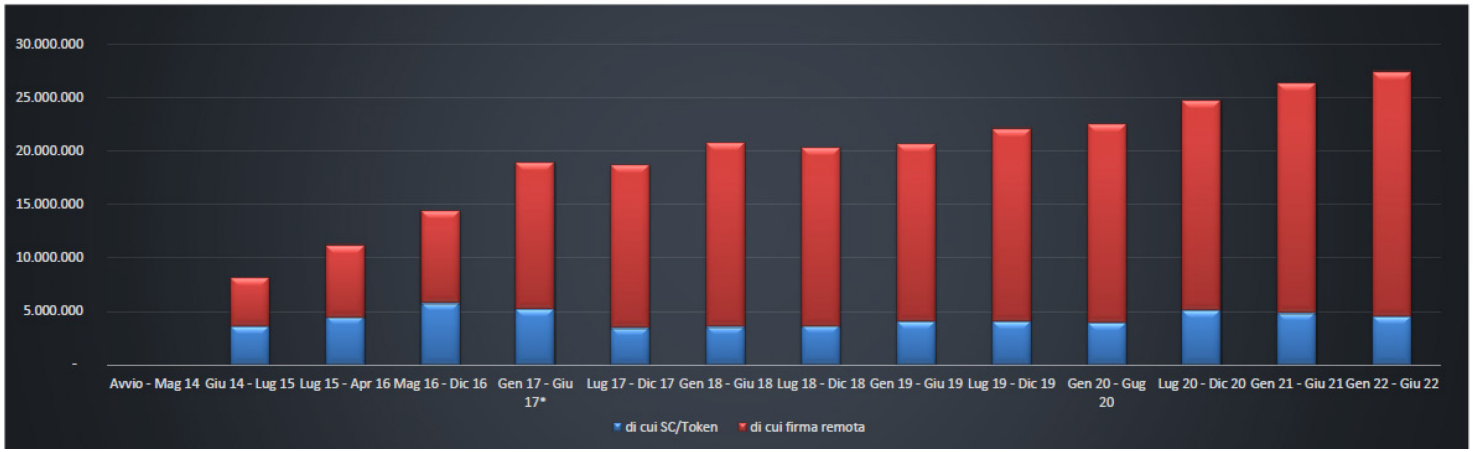
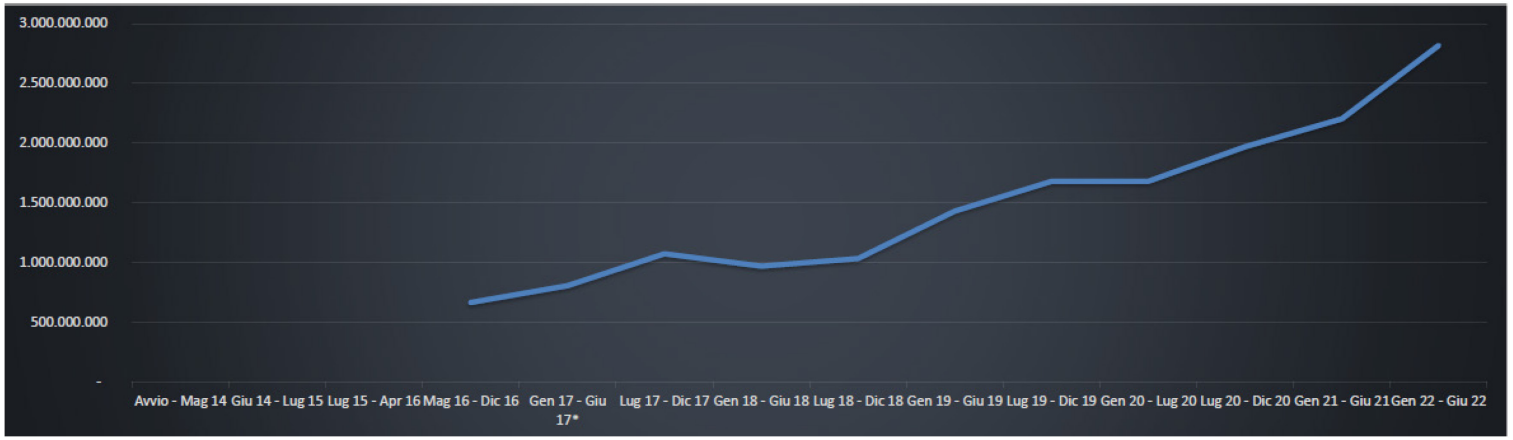


Grafico 2 – *Firme Digitali remote generate nel periodo*



Si nota come le firme remote stiano sempre più sostituendo le firme digitale fisiche (smart card, token, ecc..). Ad esclusione della TS-CNS, per la FD avremo quasi solamente strumenti di firma remota nei prossimi anni.

7.2 Spid e Cie: attivazioni in crescita

È una crescita record quella del Sistema Pubblico di Identità Digitale (SPID) In Italia negli ultimi 12 mesi. Secondo dati diffusi dall'Agenzia per l'Italia Digitale e dal Ministero per l'Innovazione Tecnologica e la Transizione Digitale, sono più di 30 milioni le utenze SPID attive lungo la penisola.

In crescita anche i numeri della Carta di identità elettronica (CIE), che ha superato 30 milioni di carte rilasciate. Un'occasione per dare maggiore rilevanza a questo strumento (parliamo della vera identità digitale di ogni cittadino di fronte allo Stato), che fin dall'inizio ha subìto una sorta di discriminazione istituzionale nell'accesso ai servizi della PA online.

In data 06/05/2022 l'AgID pubblica un nuovo traguardo [S6], raggiungendo in anticipo l'obiettivo annuale. In dodici mesi sono state rilasciate 10 milioni di identità digitali, utilizzate 800 milioni di volte dai cittadini per accedere ai servizi online.

Superano oggi i 30 milioni le identità digitali SPID in Italia, di cui quasi 10 milioni attivate solo negli ultimi 12 mesi.

Qualche dato inerente lo SPID:

- *Numero di identità SPID erogate* [S7]

  (numero aggregato, totale dei gestori) al 31/08/2022

  31.798.494

Si noti anche l'andamento nel 2022 (*Grafico 3*) e l'andamento negli ultimi anni (*Grafico 4*)

- *Gestori di identità digitale attivi*

  ultimo aggiornamento 01/03/2019

  9 Gestori (*Immagine 10*)

- *Amministrazioni attive*

  Numero di pubbliche amministrazioni che consentono l'accesso ai servizi online attraverso SPID al 30/03/2022:

  12.297

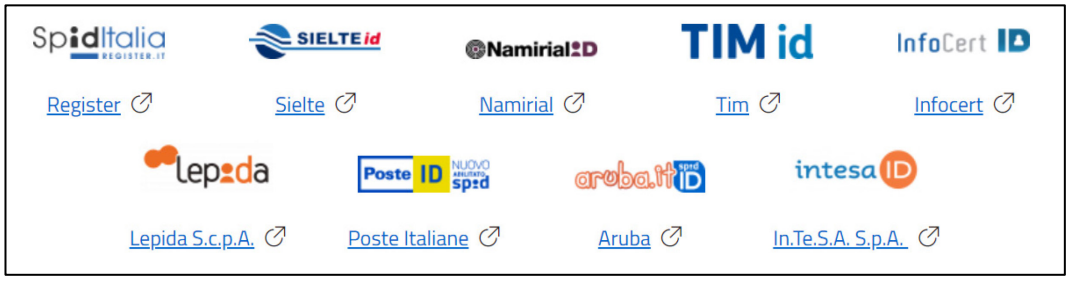


Immagine10 – Gestori di Identità Digitale

Grafico 3 – Attivazione SPID negli anni

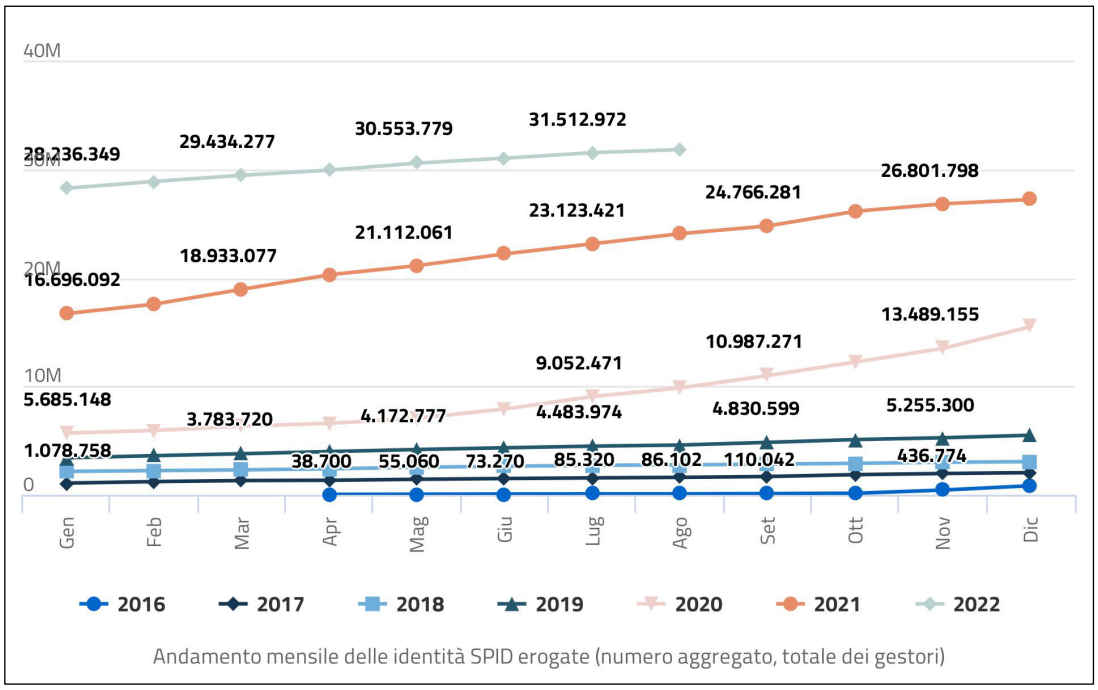
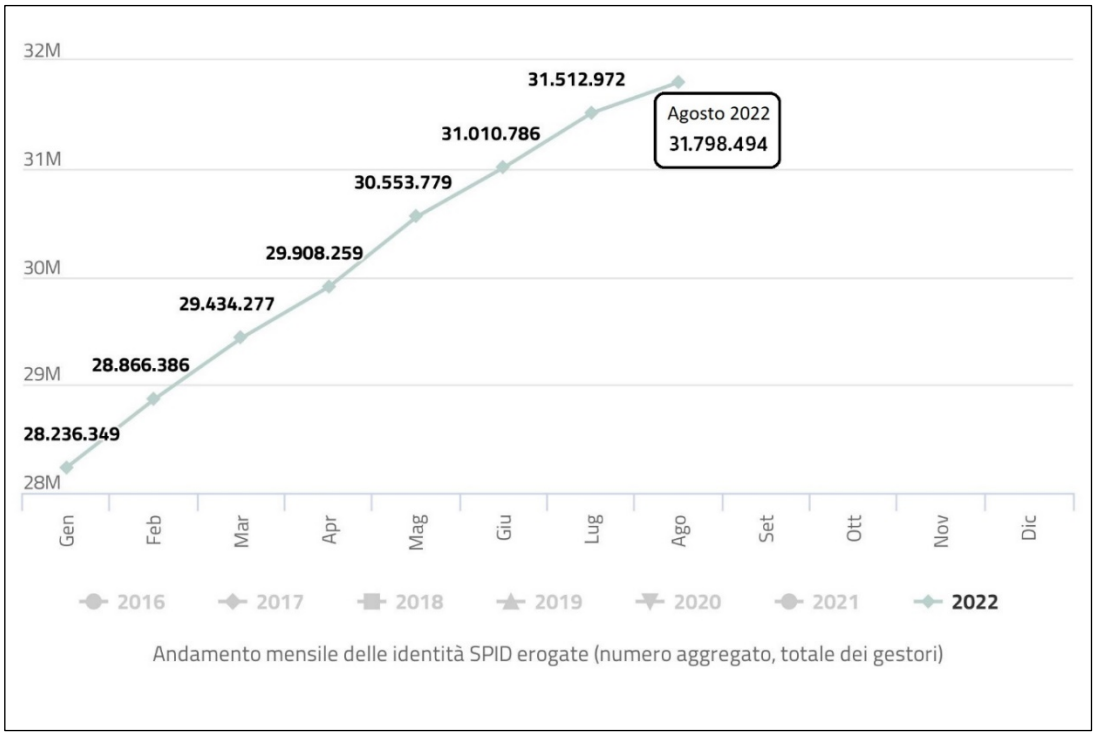


Grafico 4 – Attivazione SPID anno 2022



7.3 L'identità digitale in Italia - Diffusione

Esaminando i dati sopra con i dati ISTAT dei cittadini residenti maggiorenni abbiamo:

- 49.783.836 cittadini maggiorenni al 1° Gennaio 2022
- *Firme Digitali* *29.235.137 attive al 1 Gennaio 2022*, 27.413.067 al 30 giugno 2022
- *SPID* *28.236.349 attive al 1 Gennaio 2022.* 31.798.494 al 30 agosto 2022
- *CIE* *30.754.491 al 14 settembre 2022.*

Nelle firme digitali vediamo comprese anche la TS-CNS attivate per l'uso di firma digitale oltre che ai servizi di firma offerti da altri gestori, negli ultimi sei mesi il servizio di firma digitale ha visto un po' di contrazione, mentre si vede come lo SPID (*Grafico 4*) abbia visto una grande accelerazione. Invece per quanto riguarda la CIE nel tempo si avrà tutta la copertura nazionale, ma non è chiaro quante persone ad oggi la utilizzino per l'accesso e la firma.

Stimando qualche percentuale, al 1° gennaio 2022 sono disponibili in percentuale alla popolazione maggiorenne:

- *Firme Digitali* *58,72%*
- *SPID* *56,72%*
- *CIE* *61,77% (dato al 14 settembre 2022)*

Analizzando questi dati vediamo come il fenomeno sia diffuso quasi al 60%, nel caso di CIE anche oltre e di come sia in continua espansione. Questo dato fornirà anche una maggiore spinta alla crescita del nostro progetto, e ci indica anche che investire nella dematerializzazione con questi strumenti avanzati per la firma elettronica è la strada nuova e corretta da percorrere.

Conclusioni

Nell'era della dematerializzazione è evidente come l'identità digitale di ogni cittadino favorisca l'accelerazione dei processi all'interno della sanità e delle pubbliche amministrazioni.

Dalla partecipazione a bandi di gara e concorsi alla firma di contratti e la modifica di assetti societari, dal sistema di fatturazione ai documenti sanitari, sono molti gli utilizzi della firma e identità digitale, ormai largamente diffusi.

Grazie all'identità digitale la Pubblica Amministrazione fornisce l'accesso semplice e sicuro ai suoi servizi online. Per accedere a tali servizi in qualsiasi momento si può scegliere tra il Sistema Pubblico di Identità Digitale (SPID) e la Carta d'Identità elettronica (CIE).

Con SPID e CIE, ad esempio, è possibile richiedere online il cambio di residenza o un certificato, prenotare una prestazione sanitaria, inviare la propria dichiarazione dei redditi, consultare la propria situazione fiscale o contributiva, accedere ai bonus, agli ammortizzatori sociali o compilare l'ISEE. Il tutto in pochissimi click e senza bisogno di ricordare tante password diverse per ciascun servizio.

Un risultato di rilievo, anche in chiave di accelerazione della transizione digitale, che può essere trainata anche dalla maggiore domanda di servizi pubblici online e dal maggiore utilizzo che ne fanno cittadini e imprese.

Offrire a tutti i cittadini la stessa modalità di accesso ai servizi online è inoltre la chiave per raggiungere la semplificazione amministrativa dei rapporti tra cittadini e PA di cui tanto si parla da tempo. Si tratta di un primo concreto passo per offrire, nel solco delle azioni previste nel Piano nazionale di ripresa e resilienza (PNRR), un'esperienza di maggiore qualità nell'accesso ai servizi digitali, in linea con gli ambiziosi obiettivi del Digital Compass Europeo.

Entro i prossimi dieci anni l'Europa dovrà aver intrapreso una transizione digitale in grado di sviluppare quattro asset principali, tra cui la digitalizzazione dei servizi pubblici.

Stessa strada da far percorrere anche alle cartelle cliniche dei pazienti e alle identità digitali dei cittadini.

Un cambiamento importante per la vita di tutti i giorni, perché prevede diversi principi di base, tra cui: la realizzazione di ambienti online sicuri e affidabili, crescenti competenze tecnologiche, possibilità di accesso a sistemi e dispostivi sostenibili a livello ambientale e incentrati sulla persona, assicurando protezione ai minori nello spazio online e nuovi servizi sanitari digitali per tutti.

Con il Digital Compass Europeo [S8], l'UE traccia una rotta per gli obiettivi digitali da raggiungere entro il 2030. L'Europa mira a dare maggior forza alle imprese e ai cittadini in un futuro digitale incentrato sulla persona, sostenibile e più prospero.

L'UE traccia questi obiettivi per la digitalizzazione dei servizi pubblici:

- servizi pubblici fondamentali online al 100%;
- *sanità online, con il 100% dei cittadini che abbiano accesso alla propria cartella clinica;*
- *identità digitale, con l'80% di cittadini in possesso dell'identità digitale.*

Quindi abbiamo la necessità e l'obbligatorietà di garantire al cittadino l'accesso ai servizi sanitari, nonché la possibilità di consultare e firmare i propri documenti sanitari (nel nostro caso) dando maggiori opportunità, più inclusione, più partecipazione, più consapevolezza alle sue scelte e dando maggior valore alla nostra attività di Professionisti della Salute.

Oramai nell'era degli smartphone quasi tutta la popolazione ha un facile accesso a tutti i servizi, ma la sanità ha ancora un posto marginale.

Tantissime sono le iniziative sul territorio italiano dell'implementazione di servizi sanitari digitali (FSE, CUP, ecc..) intraprese in quasi tutte le regioni. Da parte nostra c'è il compito di coinvolgere in maniera crescente il cittadino per una maggior consapevolezza e un migliore accesso alla sanità pubblica.

Sperando che in un futuro alquanto prossimo per accedere ai servizi ospedalieri, firmare i documenti e consensi informati sia necessario solo il nostro smartphone e la nostra memoria (user/password).

Bibliografia

[1] Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD – *AgID*

[2] L'apposizione di firme e informazioni su documenti firmati - *AgID*

[3] Software Cie Manuale Utente 28/03/22 – *Ministero dell'Interno – Istituto Poligrafico Zecca dello Stato*

[4] Documento di sintesi della Sperimentazione - Dematerializzazione del Consenso Informato in ambito radiologico – *AgID – SIRM*

Sitografia

[S1] http://sirm.org – *Società Italiana Radiologia Medica ed Interventistica (SIRM)*

[S2] https://www.cartaidentita.interno.gov.it/cittadini/firma-con-cie
- *Firma con CIE – CieSign*

[S3] https://sistemats1.sanita.finanze.it/portale/modalita-di-accesso-cittadini – *Sistema Tessera Sanitaria – Modalità di Accesso*

[S4] https://www.quotidianosanita.it/lavoro-e-professioni/articolo.php?articolo_id=61446 – *Quotidiano Sanità*

[S5] https://eidas.agid.gov.it/Statistiche/Diffusione.pdf
- *Diffusione Firma Digitale AgID*

[S6] https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2022/05/06/digitale-superati-i-30-milioni-identita-spid
– Digitale: superati i 30 milioni di identità SPID – AgID

[S7] https://avanzamentodigitale.italia.it - *Avanzamento Trasformazione Digitale*

[S8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it
– Decennio digitale europeo: obiettivi digitali per il 2030