Firma digitale

La dematerializzazione completa dei documenti

Prof. Crescenzio Gallo
c.gallo@unifg.it

Introduzione

Dematerializzazione: processo che ha come obiettivo ultimo 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 presente negli archivi di qualunque attività pubblica o privata.

Introduzione

La dematerializzazione porta con sé una serie di vantaggi pratici rappresentati in prima istanza dall'**incremento di efficienza e la riduzione dei costi**.

La gestione del tradizionale documento cartaceo è infatti particolarmente onerosa e, se vogliamo, carente da diversi punti di vista: difficoltà di condivisione, facilità di smarrimenti, elevati tempi di ricerca e via discorrendo.

Introduzione

La dematerializzazione permette di produrre documenti digitali che abbiano pieno valore giuridico.

Ciò significa, tra le varie cose, che anche con i documenti elettronici è necessario adottare un sistema che consenta di accertare in maniera chiara ed univoca il sottoscrittore di un documento.

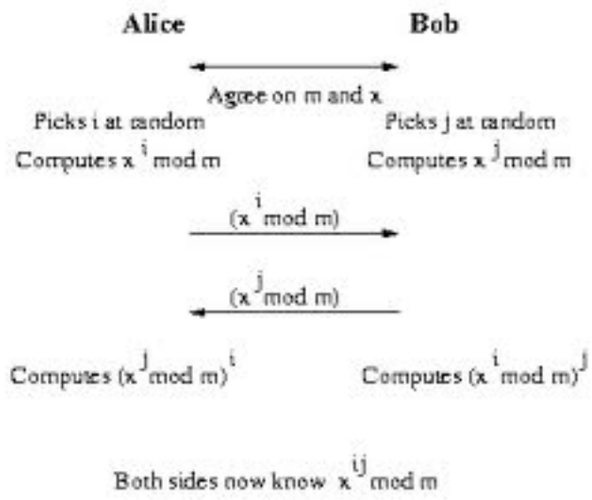
Introduzione

Nella tradizionale gestione della documentazione cartacea ciò è rappresentato dalla **firma autografa**: la firma apposta di pugno da chiunque sottoscriva un documento è considerato un elemento distintivo aventi caratteristiche uniche e personali.

Introduzione

Perché, quindi, non applicare un concetto simile anche al documento elettronico? Si tratta della **firma digitale**, un concetto già in uso da qualche anno e che sta ultimamente assumendo un'importanza via via maggiore proprio grazie alla spinta verso una gestione documentale sempre più digitalizzata.

Introduzione



E' dalla seconda metà degli anni '70 che è iniziato a circolare il concetto di firma digitale con la descrizione da parte di Whifield Diffie e Martin Hellman del primo schema di firma digitale, seppur fermo ad una fase concettuale.

Introduzione

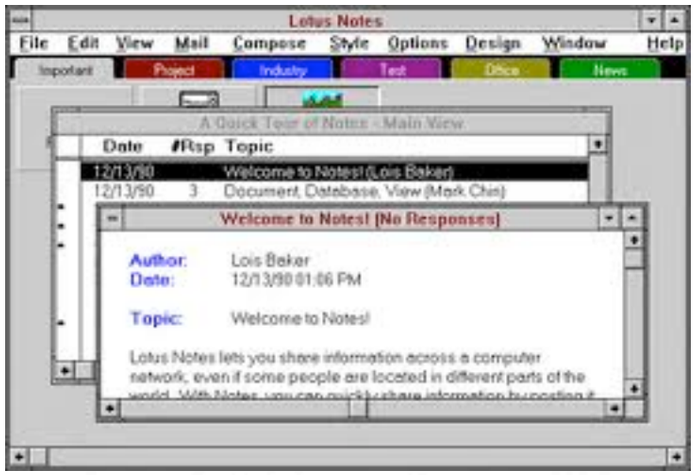
Key Generation	
Select p, q	p, q both prime, p≠q
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Solamente qualche anno dopo, nel 1977, venne inventato l'**algoritmo RSA** da Ronald Rivest, Adi Shamir e Len Adleman che consentì di gettare le basi per realizzazione dei primi schemi di firma digitale.

Introduzione



- Nel 1989 è stato Lotus Notes 1.0 il primo software largamente disponibile in grado di usare l'algoritmo RSA.
- Da allora gli studi e le tecnologie legati alla firma digitale sono proseguiti su un cammino evolutivo che ha portato, per varie tappe, alle tecnologie di firma digitale di cui possiamo disporre oggi.

Firma elettronica qualificata

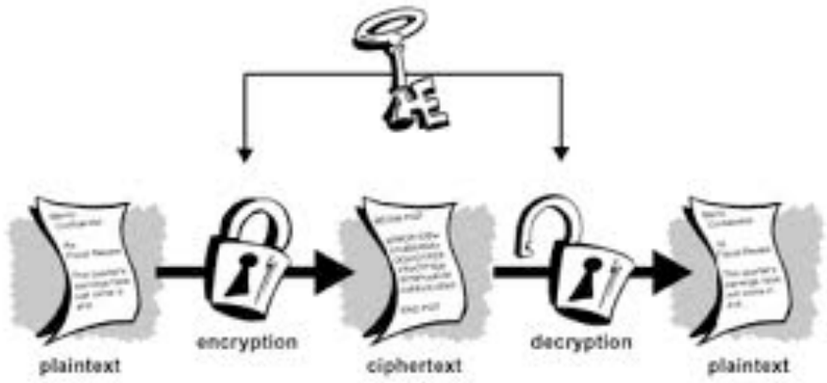
Se è dal 1979 che si parla, almeno concettualmente di firma digitale, è solamente 20 anni dopo nel 1999 che entrano in vigore le prime regole tecniche in materia di firma digitale, assieme alla Direttiva Comunitaria 1999/93/CE, dove si parla di firma digitale con riferimento a ciò che oggi viene definito in maniera molto più rigorosa come **Firma Elettronica Qualificata**.

Firma elettronica qualificata

E' lo strumento tecnologico che permette di sottoscrivere documenti digitali al massimo livello di **sicurezza**, **affidabilità**, **valore probatorio**.

Nel nostro paese, basato sulla *civil law*, ovunque sia richiesta la forma scritta e si desideri liberarsi della forma cartacea del documento, la firma digitale è la soluzione più naturale.

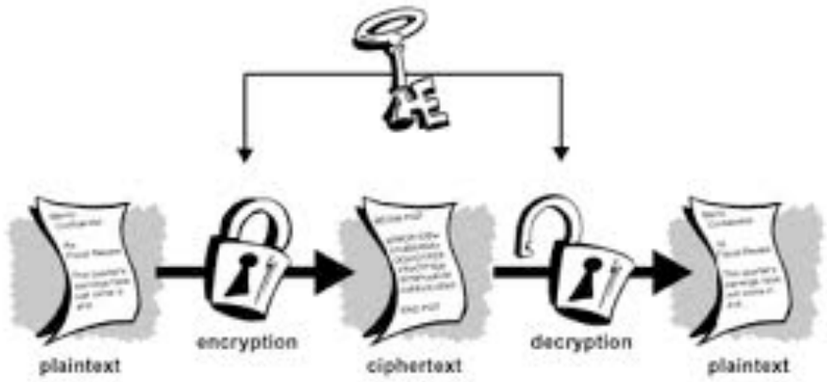
Firma elettronica qualificata



- Cerchiamo di capire quali sono i presupposti necessari affinché sia possibile utilizzare la firma digitale.

- Anzitutto è bene chiarire che il principio di funzionamento della Firma Elettronica Qualificata si basa sul concetto di ***crittografia asimmetrica***: dal documento che viene sottoposto alla firma si ricava un'**impronta**, che viene successivamente criptata con una chiave privata.

Firma elettronica qualificata



- Per mezzo di una **chiave pubblica** si potrà accertare se la firma è stata crittografata con la corretta **chiave privata**.
- Si tratta di operazioni comunque automatiche e trasparenti all'utente, che non ha bisogno di conoscere il meccanismo di funzionamento.

Firma elettronica qualificata

La Firma Elettronica Qualificata necessita di tre elementi:

un **dispositivo di firma** ad elevata sicurezza, che contiene la chiave privata e che sia in possesso esclusivo del titolare. Si tratta, per entrare nel concreto, di una smartcard o di una chiavetta USB, cui vanno aggiungendosi recentemente servizi di firma remota basati su server centralizzati che ospitano le chiavi di molti utenti.

Firma elettronica qualificata

In secondo luogo è necessario un **certificato qualificato**: si tratta di un attestato elettronico mediante il quale il fornitore dei servizi di certificazione dichiara di avere identificato il titolare del dispositivo di firma o degli strumenti per l'accesso al servizio di firma remota e di averglieli consegnati.

Firma elettronica qualificata

Infine è necessario un **software** che sia in grado di operare e gestire il dispositivo di firma e di produrre documenti firmati mediante la chiave privata e completi di una copia del certificato qualificato, il quale consentirà di verificare la firma e accertare così il sottoscrittore del documento.

Firma grafometrica

Una tecnologia estremamente interessante e che rappresenta un'evoluzione del concetto di firma digitale e un punto di convergenza tra la modalità tradizionale e quanto reso possibile dalla tecnologia è la **firma grafometrica**.

Sarà capitato più o meno a tutti di firmare la ricevuta di un pacco o l'autorizzazione di una carta di credito tramite un apposito stilo e su di uno schermo: in tutti questi frangenti abbiamo avuto a che fare proprio con una firma grafometrica.

Firma grafometrica

In termini un po' più rigorosi, la firma grafometrica prevede l'impiego di un dispositivo apposito, come ad esempio una tavoletta grafica, capace di acquisire il movimento della penna durante una firma apposta di pugno, in maniera tradizionale.

Firma grafometrica

Ciò consente di acquisire numerosi **dati biometrici** (posizione, velocità e pressione del tratto, spostamenti effettuati dalla mano con la penna sollevata) che incrociati tra loro creano proprio quella firma univoca che viene collegato all'impronta del documento allo scopo di impedire l'alterazione del testo.

Firma grafometrica

L'**ibridazione** di modalità tradizionale e tecnologia mette a disposizione maggiori risorse per affrontare i casi di disconoscimento della firma: i dati biometrici possono essere infatti decifrati e affidati ad un perito calligrafo il quale potrà utilizzare le tradizionali tecniche di analisi oltre ad avvalersi dello strumento informatico e di quelle informazioni in più che esso è in grado di registrare rispetto alle tecniche tradizionali.

Firma grafometrica

La firma grafometrica pertanto offre da un lato la protezione dell'integrità del documento e la piena digitalizzazione/dematerializzazione come la firma digitale, e dall'altro la semplicità e l'intuitività della firma di pugno.

Firma grafometrica

Sebbene sia oggi estremamente rilevante la diffusione di dispositivi, soprattutto consumer, dotati di touchscreen, attualmente questi dispositivi non sono adatti per poter essere utilizzati per applicazioni di firma grafometrica.

Gli attuali sensori touchscreen hanno infatti una ***risoluzione troppo bassa*** (dei punti di contatto, non dell'immagine) e non possono fornire il dato della pressione del tratto istante per istante.

Firma grafometrica

Sebbene a livello normativo non esista nessuna norma che stabilisca un livello minimo di qualità delle informazioni raccolte dal sistema di firma grafometrica, è ovviamente scontato sottolinare che nel caso di una firma registrata con una qualità non sufficientemente elevata, il perito calligrafo non potrà disporre degli elementi necessari per confermare l'autenticità della firma.

Firma grafometrica

Al momento l'attenzione si focalizza su sensori specializzati, disponibili come device dedicati oppure sovrapposti al touchscreen di alcuni tablet o PC destinati a questo uso particolare.

Ma non è difficile immaginare che questa tecnologia si diffonderà su un numero sempre maggiore di modelli, soprattutto se questa tipologia di firma avrà il successo che sta promettendo.

Firma grafometrica

Attualmente i sistemi di firma grafometrica possono essere utilizzati da istituzioni, pubblica amministrazione e via discorrendo, in maniera tale che il cittadino possa firmare di proprio pugno un qualsiasi documento senza che vi sia la necessità di dover possedere uno strumento dedicato per la firma digitale.

Sicurezza e attendibilità

- Sul fronte della sicurezza uno dei vantaggi della firma digitale è rappresentato non solo dall'identificazione immediata del sottoscrittore, ma soprattutto dall'**impossibilità di modificare il contenuto** del documento una volta firmato: abbiamo infatti visto che la firma digitale viene collegata all'impronta del documento e crittografata, per questo motivo anche l'alterazione di un solo bit produrrebbe un'anomalia immediatamente riscontrabile.
- Ciò, se ci pensiamo, non è possibile con le normali firme su carta, in quanto il contenuto di un documento potrebbe essere facilmente alterabile senza lasciare alcuna traccia.

Sicurezza e attendibilità

- Il processo di rilascio del dispositivo di firma e del certificato qualificato (con importanti responsabilità in capo al Certificatore) e lo strumento della revoca del certificato in caso di perdita o furto del dispositivo, rendono praticamente impossibile impersonare un altro individuo, a meno di falsificare la documentazione in fase di rilascio (di cui però rimane traccia per 20 anni).
- L'unico caso in cui sia possibile compromettere questo processo di sicurezza è, ancora una volta, ad opera dell'anello più debole della catena: l'utente. Un suo comportamento superficiale, come ad esempio lasciare incustoditi i dispositivi come smartcard o chiave USB, assieme magari al relativo PIN di controllo.

Sicurezza e attendibilità

- Spostando l'attenzione sulla firma grafometrica, illustrata in precedenza, questa è capace di offrire un grado di attendibilità superiore alla tradizionale firma su carta.
- Sebbene il processo di verifica dell'autenticità della firma è comunque condotto dal perito calligrafo, bisogna considerare, come già accennato in precedenza, che esso dispone di molte più informazioni e strumenti di analisi più sofisticati per poter effettuare la propria verifica, dal momento che il dato originario è intrinsecamente più ricco di informazioni e registrato in forma digitale.

Sicurezza e attendibilità

Laddove infatti un **perito** che abbia a che fare con una firma tradizionale, vergata su carta, dovrà risalire agli spostamenti e alla velocità della mano analizzando lo spessore e le striature dell'inchiostro, l'incisione della carta ed incrociare queste informazioni con quelle della penna, del tipo di inchiostro e della carta su cui è stata apposta la firma, il perito che si approccia all'analisi di una ***firma grafometrica*** potrà disporre di tutti questi dati in forma numerica e discreta assieme ad altre informazioni che non è possibile ricavare da una firma su carta, come ad esempio i movimenti compiuti dalla mano e dalla penna quando non sono a contatto con il foglio.

Sicurezza e attendibilità

- Un tale grado di precisione e di ricchezza di informazioni, ha però ovviamente un risvolto cui prestare particolare attenzione.
- Il **software** che acquisisce i dati deve immediatamente criptarli in modo che siano poi accessibili solo al perito. Non deve essere possibile catturare i dati in chiaro della firma di un cittadino, perché quei dati potrebbero essere usati per firmare altri documenti all'insaputa del sottoscrittore.

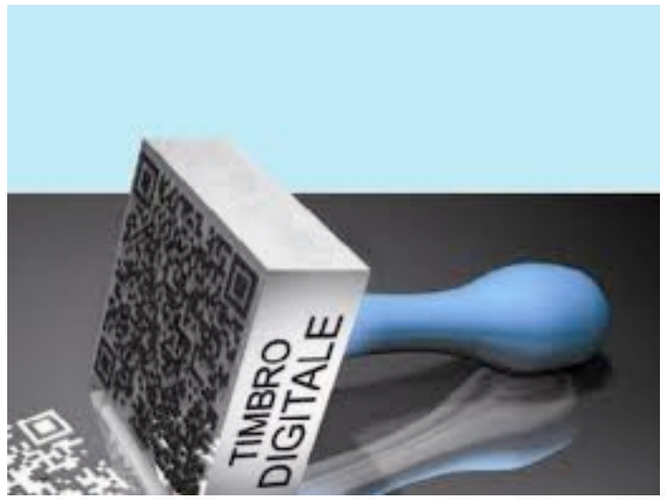
Sicurezza e attendibilità

A tal proposito la normativa vigente è particolarmente chiara: a differenza, infatti, della firma digitale qualificata, la firma grafometrica deve essere contestualizzata e gestita da un soggetto identificato che abbia la responsabilità dello svolgimento del processo, dell'identificazione del sottoscrittore e della raccolta del consenso ad utilizzare tale tecnologia in relazione ad una specifica tipologia di documenti.

Sicurezza e attendibilità

Per sgomberare il campo da ogni dubbio: non dobbiamo pensare al cittadino che firma di pugno un bonifico dal proprio smartphone mentre è seduto in tram, ma ad una modalità particolare che consente di **dematerializzare** documenti firmati da cittadini privi di altri strumenti di firma digitale.

Timbro digitale



Il ***timbro digitale*** rappresenta una tecnologia autorizzata dal CNIPA (ora DigitPA) in grado di poter mantenere il valore legale di un documento informatico stampato su carta e quindi trasformato in un **documento analogico**.

L'applicazione pratica sul servizio certificativo è intuitiva: **poter richiedere on line un documento, visualizzarlo sul proprio personal computer e addirittura stamparlo per produrlo al soggetto privato che ne abbia fatto esplicita richiesta**, il tutto abbattendo la dimensione spazio – temporale e i costi di produzione del servizio: di fatto, un ufficio pubblico aperto 24 h su 24.

Il timbro digitale rappresenta una ***soluzione tecnologica in grado di innovare il modo di lavorare nella pubblica amministrazione*** migliorando i servizi erogati al cittadino.

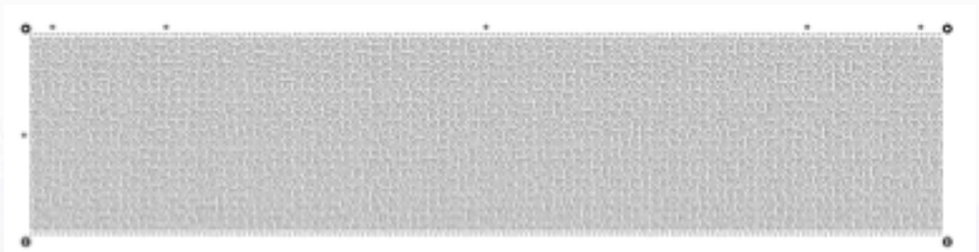
Timbro digitale: esempi

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Area Vasta Romagna

Programma di Patologia Clinica
e
Medicina Trasfusionale

Pag. 2 / 2
Doc. n. 4993717 prodotto il 17/05/2010 Ore: 11:09 Routine
Richiesta: **10472712 13/05/2010** Ore: 09:18
10070 11-ESTERNI LABORATORIO
Sig.ra **PAZIENTE DI PROVA**
Data Nascita: 04/12/1990 Età: 19 Anni Sesso: F
Id. Paz.: 15002896

Esame	*Esito*	*U.M.*	*Intervalli Riferimento*
[51] S-Ferro *(Cobas C)*	**75**	ug/dl	37 - 145
[51] S-Ferritina *(Modular E)*	**28**	ug/L	15 - 150



Referto analisi cliniche

Pergamena di laurea

Applicazione pratica

La firma digitale è uno dei mattoni fondanti dei documenti informatici ed ha quindi un ruolo protagonista dell'Agenda Digitale.

Anche nella prima edizione (D.L. Crescita 2.0), pur criticata per una portata inferiore alle aspettative, i riferimenti a PA Digitale, Sanità digitale, Giustizia Digitale implicano un crescente impiego di questa tecnologia.

Applicazione pratica

Usare la firma digitale in luogo della firma tradizionale su carta consente la dematerializzazione:

il documento firmato è puramente digitale e può essere prodotto, trattato, acquisito, replicato, conservato digitalmente, liberandosi del costo e della complicazione del trattamento (basti pensare all'archiviazione a tempo indeterminato) della carta.

Applicazione pratica

- A tal proposito si consideri ad esempio il settore della Sanità, nel quale la dematerializzazione è già molto avanzata: le cartelle cliniche, i referti, tutto quello che reca una firma di un medico è già digitale.
- Ma il **consenso informato**, firmato dal paziente, fino ad oggi è stato inesorabilmente cartaceo, costringendo ad una archiviazione tradizionale. Questa tecnologia consente di abbattere anche questo ultimo diaframma di resistenza sul cammino della dematerializzazione.

Applicazione pratica

- Inoltre la verifica dell'**autenticità** di una firma digitale e dell'**identità** del sottoscrittore è un processo automatico, istantaneo, molto affidabile.
- Basta pensare ad un documento firmato su carta per comprendere la differenza: solo se conosciamo personalmente il sottoscrittore e il suo modo di firmare possiamo capire a prima vista se la firma autografa è autentica o meno.
- Le falsificazioni poi possono essere scoperte solo da un perito calligrafo.

Considerazioni

Nel discorso della dematerializzazione e della firma digitale il vero problema sta nella ***legislazione*** che regolamenta i vari ambiti normativi in tema di documentazione; e va ricercato nella UNIFORMITA' OPERATIVA e nell'UTILIZZO DI UNO STANDARD anch'esso uniforme per la digitalizzazione dei documenti.

Considerazioni

Prendiamo l'esempio degli ospedali italiani, tipico ambiente dove si producono documenti in quantità industriale.

Purtroppo non esistono ***protocolli operativi condivisi*** e uniformi su tutto il territorio nazionale: ogni ospedale crea i propri moduli e gestisce i dati in essi contenuti in modo differente!

Considerazioni

Viene da sé che anche catalizzare i dati in un sistema informativo unico risulta un'impresa faraonica.

Senza contare che queste discrepanze generano difficoltà in fase di analisi dei dati (ad esempio per le statistiche, o per analisi dei costi precise).

Qui ci dovrebbe mettere le mani lo Stato e ordinare il modus operandi secondo regole ben precise e utilizzando esclusivamente modulistica digitale e software IDENTICI per quanto riguarda l'ambito pubblico.

La dematerializzazione completa dei documenti

Grazie per l'attenzione

Prof. Crescenzio Gallo
c.gallo@unifg.it