

## UTILIZZO DELLA FIRMA ELETTRONICA: QUALI GARANZIE?

MASSIMO LEONI

*IT e-business consultant, IBM Italia S.p.A.*

La legge 15 marzo 1997 n. 59, art. 15, comma 2, ha introdotto nella legislazione italiana il concetto di documento informatico che si è poi concretizzato nel DPR 513 del 10 novembre 1997 e nel relativo regolamento tecnico attuativo.

Il documento informatico è sicuramente una rivoluzione copernicana nel quadro legislativo italiano ed europeo. La legislazione italiana è stata infatti tra le poche a livello mondiale che si è spinta oltre i confini del commercio elettronico elevando ed equiparando il documento informatico al rango del documento cartaceo.

Questo concetto rivoluziona di fatto il modo di trattare e conservare documenti aventi significato giuridico con conseguenze estremamente rilevanti nel campo dell'archiviazione ottica, nei pagamenti, nelle scritture private e nei contratti.

La sfida del legislatore nella definizione delle regole che permettono ad un documento costituito da "bit" di equivalere ad uno di "atomi" è stata principalmente la trasposizione della firma autografa nel mondo virtuale.

Rispetto ad altri approcci legislativi<sup>[1]</sup> nei quali si parla in modo più generico di firma elettronica, senza alcuna preclusione sulla scelta delle tecnologie e delle soluzioni realizzative (es.: biometrica dinamica della firma, firma digitale, ...), il legislatore italiano ha invece definito rigorosamente la tecnologia da utilizzare per realizzare la firma di un documento informatico: la firma digitale con chiavi crittografiche asimmetriche<sup>[2]</sup>.

La scelta di questa tecnologia, già utilizzata per i pagamenti su Internet (ad esempio nel SET - *Secure Electronic Transactions*) per garantire il non ripudio della transazione finanziaria, comporta l'utilizzo di una chiave privata di cifratura per generazione della firma. La chiave privata di cifratura è associata in modo univoco e ad un'unica chiave pubblica che, a sua volta, viene utilizzata nell'operazione di verifica della firma.

Affinché ci sia la garanzia della veridicità della firma digitale generata per mezzo della crittografia a chiavi asimmetriche, devono trovare una soluzione i seguenti punti:

- Le chiavi di firma devono essere associate senza ambiguità al soggetto.
- Il documento deve essere visualizzato senza ambiguità al sottoscrittore all'atto della firma.
- La chiave di cifratura (chiave privata) deve essere custodita in un dispositivo (dispositivo di firma).

Questi tre punti riassumono l'essenza tecnologica del decreto e offrono spunto di riflessione sia per il tecnologo che per il semiologo. Vediamo ora nel breve seguito di scoprire le implicazioni ivi contenute.

Il *primo punto* riguarda l'**identificazione del soggetto**. Come nella realtà avviene che caratteristiche biometriche (es. altezza, firma autografa, ecc.) e sociali (nome, cognome, ecc.) vengono asserite da un'entità riconosciuta<sup>[3]</sup> così anche nel mondo digitale è necessario associare la chiave di verifica (chiave pubblica) a delle informazioni identificative del soggetto in modo certo. Questo compito è svolto dal soggetto certificatore (CA - *Certification Authority*) che, sempre utilizzando la firma digitale a chiavi asimmetriche, suggella le informazioni relative all'individuo e la sua chiave pubblica in un oggetto che prende il nome di **certificato digitale**. La sfida principale che questa infrastruttura di chiavi pubbliche (PKI - *Public Key Infrastructure*) deve affrontare è in prima istanza l'interoperabilità. Non è infatti conseguente che un certificato generato e gestito in una CA sia interoperabile con altre. Su questo fronte il comitato tecnologi-

[1] Si prenda ad esempio COM(1998)297 from European Commission "Proposal for a European Parliament and Council Directive on a common framework for electronic signatures".

[2] La crittografia a chiavi asimmetriche, detta anche a chiavi pubbliche, nasce dall'enunciazione teorica di Withfield Diffie e Martin Hellman nel 1976. Rivest, Shamir e Adelman perfezionarono il metodo inventando un nuovo algoritmo conosciuto come crittografia RSA, acronimo nato dalle iniziali dei suoi inventori. Un maggior approfondimento sulla materia lo si può avere visitando il sito internet <http://www.rsa.com>

[3] Ne è un classico esempio la Carta di Identità, dove informazioni sociali (nome, cognome, data di nascita e residenza) e biometriche (altezza, colore degli occhi, segni particolari, fotografia e firma autografa) vengono "certificate" dallo Stato Italiano attraverso la figura del Sindaco.

co di Internet, l'IETF <sup>[4]</sup>, supportato da fornitori di tecnologie come IBM ha definito uno standard di interoperabilità per una PKI su Internet, il PKIX. Questo standard ha come obiettivo la definizione di regole e l'implementazione di software comuni per garantire appunto la circolarità dei certificati. Un altro aspetto della certificazione è la garanzia del valore del certificato. Questo aspetto, più che alla tecnologia, affrisce alle procedure e ai processi che intervengono nella certificazione di un soggetto. E' necessario quindi che opportuni standard tecnologici (ISO e ITSEC) e di qualità (ISO 9002) vengano perseguiti e realizzati dal fornitore del servizio.

Il *secondo punto* è strettamente legato alla **semantica del documento**. Passando dal dominio del documento "cartaceo" a quello digitale vengono sollevate problematiche prima sconosciute o comunque già consolidate. Nel mondo digitale infatti, la visualizzazione del contenuto di un documento deve passare attraverso diversi strati di interpretazione il cui compito è quello di aggiungere "significato" al contenuto stesso. Per meglio capire questa problematica facciamo un esempio. Supponiamo di avere un documento in HTML <sup>[5]</sup>, se andiamo ad analizzarlo nella sua struttura esso è costituito da testo e da simboli di *markup* (metadati) che aggiungono significato alle parole o parti del testo (un chiaro esempio è la tabella, nella quale i simboli di *markup* - <TABLE>, <ROW>, ... - indicano la posizione e la struttura dei vari elementi al suo interno). Il software che visualizza il documento (il browser o un word processor) deve interpretare e "rendere" i vari *markup* secondo una propria logica e capacità che può essere differente da software a software o addirittura tra diverse versioni dello stesso software. Questo tipo di problema è stato già affrontato anche nel campo del documento cartaceo, ad esempio l'utilizzo dell'inchiostro nero o di un particolare tipo di carta nella stesura di documenti a valore legale sono una risposta a questa necessità.

Il *terzo punto* ed ultimo punto riguarda l'**utilizzo dei dispositivi di firma**. Sotto questa definizione possiamo facilmente identificare le c.d. *carte a microprocessore* o *SmartCard*. E' all'interno di questo dispositivo che viene custodita la chiave privata e realizzata l'operazione crittografica di firma digitale. In questo modo si evita che la chiave privata lasci il dispositivo e si esponga ad una sua intercettazione, garantendo così l'autenticità della firma e il non ripudio. Anche nel campo delle *SmartCard* come in quello delle PKI la sfida principale è l'interoperabilità tra diversi tipi di carta. Attualmente il mercato offre *SmartCard* per lo più incompatibili tra loro nonostante gli sforzi dei vari produttori per standardizzare i vari aspetti di questa tecnologia (sistema operativo, interfacce applicative,). Una soluzione a questo problema si intravede all'orizzonte ed è un nuovo tipo di carta denominata *JavaCard*. Queste carte dovrebbero permettere l'utilizzo delle loro funzioni e dati interni da qualsiasi applicazione autorizzata, in modo da garantire l'interoperabilità tra carte diverse e soluzioni applicative diverse sviluppate sulla stessa carta.

In conclusione si può affermare che la legislazione italiana sul documento informatico e il suo regolamento tecnico associato garantiscono con un buon livello di sicurezza la autenticità e il non ripudio della firma digitale. Rimane ancora aperto il problema di rendere questa opportunità pervasiva sul mercato, abilitando il singolo cittadino all'utilizzo della firma digitale. Gli ostacoli maggiori ad un tale obiettivo sono soprattutto l'affermarsi di standard riconosciuti ed adottati dal mercato nel campo della gestione dei certificati e delle *SmartCard*.

---

<sup>[4]</sup> IETF - Internet Engineering Task Force

<sup>[5]</sup> HTML - Hyper Text Markup Language