Informatica

Firma digitale alla stretta conclusiva

di Nicola Bortolotti

Il 2002 non passerà alla storia solo per l'introduzione dell'euro. Un'altra piccola "rivoluzione copernicana" potrebbe derivare dal diffondersi della cosiddetta "firma digitale": un cambiamento di pratiche e abitudini assai più rilevante del cambio di valuta, con un impatto solo in una prima fase ristretto ad amministrazioni, società e professionisti; una modifica di prassi ormai cristallizzate nel tempo che - progressivamente - si estenderà alle società più piccole sino a raggiungere i privati cittadini.

Falsa partenza?

C'è tuttavia da sottolineare il fatto che - nelle previsioni dei legislatori - la firma elettronica avrebbe dovuto essere già a regime fin dall'inizio di quest'anno. Nella legge 24 novembre 2000, n. 340 pubblicata sulla G.U. n. 275 serie generale del 24 novembre 2000 si leggeva infatti, all'art. 31, comma 2: "Decorso un anno dalla data di entrata in vigore della presente legge, *le domande, le denunce e gli atti che le accompagnano presentate all'ufficio del registro delle imprese*, ad esclusione di quelle presentate dagli imprenditori individuali e dai soggetti iscritti nel repertorio delle notizie economiche e amministrative di cui all'articolo 9 del decreto del Presidente della Repubblica 7 dicembre 1995, n. 581, *sono inviate per via telematica ovvero presentate su supporto informatico ai sensi dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59*. Le modalità ed i tempi per l'assoggettamento al predetto obbligo degli imprenditori individuali e dei soggetti iscritti solo nel repertorio delle notizie economiche e amministrative sono stabilite con decreto del Ministro dell'industria, del commercio e dell'artigianato".

Figura 1

In altri termini, dal 10 dicembre 2001 le interazioni con il fondamentale registro delle imprese avrebbero dovuto essere totalmente digitalizzate, firma compresa, per una larga parte dei soggetti interessati. Ma la partenza è stata opportunamente differita nel tempo. Recita infatti il comma 13 dell'art.3 della Finanziaria 2002 approvata dal Senato il 22 dicembre scorso: "Al comma 2 dell'articolo 31 della legge 24 novembre 2000, n. 340, le parole: 'Decorso un anno' sono sostituite dalle seguenti: *'Decorsi due anni*'. (...) sono approvate le modalità per il pagamento dell'imposta di bollo (...) dovuta sulle domande, le denunce e gli atti che le accompagnano, presentate all'ufficio del registro delle imprese *per via telematica*, ai sensi dell'art. 31, comma 2, della legge 24 novembre 2000, n. 340, nonché la nuova tariffa dell'imposta di bollo dovuta su tali atti".

Si noti tuttavia che - nonostante lo slittamento dei termini di un anno per quanto concerne l'obbligo di apporre la firma digitale - l'orientamento generale delle Camere di Commercio è quello di imporre comunque, ai sensi dell'art. 4 del DPR 558/1999, il deposito delle domande *su supporto informatico* anche se non firmate elettronicamente.

Un po' di storia

Approfittando dell'obbligo rimandato di un anno, è il caso di fare il punto della situazione riguardante il cammino della firma digitale in Italia, cogliendo anche l'occasione per puntualizzare alcuni concetti che - giocoforza depurati quasi interamente della pur indispensabile base matematica - consentono di guardare alla firma smaterializzata con minore diffidenza di quanto non avvenga oggi.

Il sopra citato art. 15 della legge 15 marzo 1997, n. 59 rimandava al regolamento concernente il "documento informatico" ossia al successivo DPR 10 novembre 1997, n. 513 pubblicato nel marzo 1998 nel quale veniva definita la firma digitale come una procedura di "validazione basata su un sistema di chiavi asimmetriche" e la cui "*apposizione o associazione (...) al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo*" (art. 10 comma 2).


Figura 2

Fu tuttavia necessario attendere il DPCM 8 febbraio 1999, ossia il regola-

mento tecnico "per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del DPR 10 novembre 1997, n. 513" per cominciare ad intravedere il futuro della "digital signature".

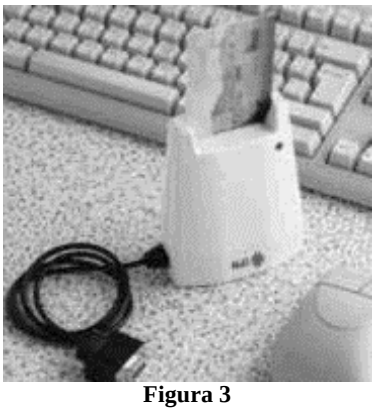

Figura 3

In questo fondamentale documento si poteva fra l'altro leggere per la prima volta chiaramente e inequivocabilmente che il "dispositivo di firma" doveva essere rigorosamente hardware, a diretto corollario alla definizione contenuta al comma d dell'articolo 1: "per 'dispositivo di firma', [si intende] *un apparato elettronico programmabile solo all'origine*, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private *e generare al suo interno firme digitali*".

Come si traduce in pratica quest'affermazione?

Con l'esclusione, dal novero delle soluzioni a norma di legge ipotizzabili per la firma digitale, di sistemi basati *unicamente* su uno (o più) computer, trattandosi di apparati programmabili *non* solo all'origine. Il computer rimane ovviamente un componente fondamentale, ma non può né generare né ospitare le chiavi.

Sono state dunque escluse le soluzioni totalmente software, come il giustamente celebrato programma PGP, peraltro utilizzato internamente da alcune grandi e piccole società per le proprie transazioni validate e/o protette, e sono rimaste valide solo grazie ad un apposito "salvagente" (l'art. 62 comma 3 del DPCM) procedure non conformi come il diffusissimo Entratel.

Inevitabile, dunque, far ricorso ad apparati esterni, ossia a una "smart card" (figura 1) o a una "chiave elettronica" (figura 2), che l'utente dovrà portare sempre con sé e custodire gelosamente, in grado di certificare la sua identità.

La soluzione "smart key" sviluppata soprattutto da Rainbow (www.rainbow.com/ikey/ikey2000.html) - sebbene allettante poiché non richiede l'adozione di un apposito lettore di card in quanto sfrutta le porte USB, presenti da alcuni anni in ogni computer - è partita con un netto svantaggio sulla smart card, più economica e diffusa.

Sia che si opti per "card" (e lettore, figura 3) o per "key" (che si sta affermando come mini hard disk trasportabile e crittabile), si tratta comunque di dispositivi a microchip assai sofisticati, anni luce distanti dalle originarie e insicure carte "Bancomat-like", in quanto devono essere in grado di generare al loro interno le firme digitali. Ma rimane fondamentale custodirli con la massima cura, in quanto chi dovesse impossessarsene unitamente al codice di attivazione non ruberebbe in un conto in banca, ruberebbe una vera e propria identità. A tale proposito il DPCM citato è assai chiaro, all'art. 8 comma 4: "Il titolare delle chiavi deve: a. conservare con la massima diligenza la chiave privata e il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza; b. conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave; c. richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi".

Un po' di teoria

Prima di proseguire è necessario chiarire cosa si intende per firma digitale. Il discorso è complesso e un modello esemplificativo - seppure non rigoroso - può aiutare. Innanzitutto la firma elettronica non è una "firma" in senso stretto, ossia sempre simile a se stessa, comunque lunga e/o complessa: non vi è infatti nulla che sia più facile, veloce ed economico del copiare un file, una sequenza di bit.

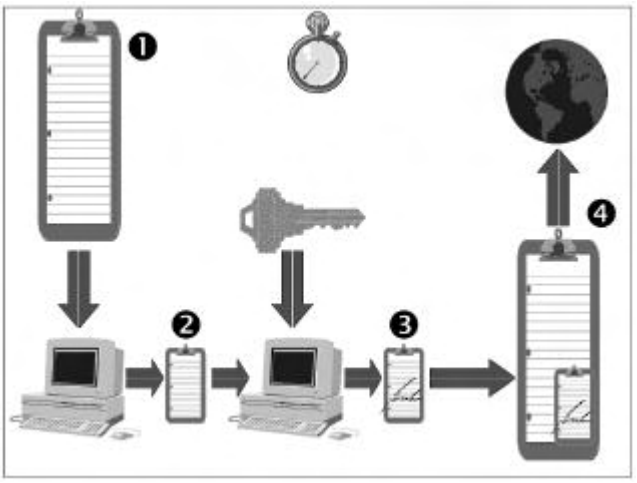

Figura 4

Si tratta invece - più propriamente - di una procedura, di una sequenza di operazioni che deve effettuare sia chi firma, sia chi vuole verificare l'autenticità del documento firmato.

Dal documento da firmare (figura 4-1) viene tratto una sorta di "riassunto" (figura 4-2) secondo regole ben precise e riproducibili. Questo rias-

sunto viene cifrato (figura 4-3) mediante una particolare chiave in possesso solo di colui che firma, la cosiddetta "chiave privata", e accodato al documento (figura 4-4) divenendone - in pratica - la firma.
Come primo punto importante si ha che, per decifrare il riassunto, *non bisogna utilizzare la chiave privata*, che rimane dunque segreta; per decifrare occorre invece una chiave particolare *diversa da quella privata*, detta chiave pubblica, che è stata generata contestualmente alla prima. Il secondo punto importante risiede nel fatto che il risalire alla chiave privata conoscendo quella pubblica è pressoché impossibile, in quanto impegnerebbe per centinaia di anni i più veloci computer disponibili. Il terzo punto importante, infine, è costituito dal fatto che, non potendo risalire alla chiave privata dalla conoscenza di quella pubblica, non è possibile contraffare la firma altrui poiché la cifratura richiede la conoscenza della privata.
Si noti che la "firma" (ma sarebbe meglio parlare di impronta firmata) del documento è dunque funzione sia del documento che della chiave privata e dunque *cambia al cambiare del documento*. In questo modo *non è possibile copiare la firma da un documento all'altro in quanto ogni firma è legata indissolubilmente al documento*.
Chi riceve il documento (figura 5-1) e vuole verificarne la paternità, come prima cosa ne ricava il riassunto seguendo le stesse regole di chi ha firmato (figura 5-5). Poi decifra il riassunto ricevuto (figura 5-2) mediante la chiave pubblica di chi ha firmato e - se il riassunto ricevuto e decodificato (figura 5-3) è identico a quello ricavato (figura 5-5) - il documento è originale. In caso contrario si è in presenza di una contraffazione.
Tutte queste operazioni sono ovviamente compiute con l'ausilio di un calcolatore elettronico e di un idoneo programma. A tal proposito il primo software autodichiaratosi conforme alla normativa italiana fu - il 9 giugno 1999 - DigitalSign della genovese CompEd Software Design (www.comped.it, nella figura 6 la pagina web con i prodotti attuali).

La certificazione
In questo quadro rimaneva aperto un fondamentale problema: ferma restando la robustezza del meccanismo di autenticazione digitale, chi è in grado di garantire che chi firma elettronicamente (e ricordiamo che questa operazione di firma può avvenire a distanza, per via telematica, senza che chi sottoscrive sia visibile ad alcuno) sia effettivamente chi afferma di essere?
Tale nodo è stato risolto dalla legge con l'introduzione della figura del certificatore, ossia una terza parte (soggetta a obblighi e responsabilità tutt'altro che trascurabili) in grado di dichiarare (o revocare) la corrispondenza tra una persona fisica e la propria chiave pubblica. Il paragone più naturale che si può fare è quello con la carta d'identità, che deve venire rilasciata da un'apposita autorità di certificazione (tipicamente il comune di residenza).
La Legge prevede che tali certificatori siano inclusi in un apposito albo che si può facilmente consultare collegandosi al sito dell'Autorità per l'Informatica nella Pubblica Amministrazione www.aipa.it e che conta in questo momento tredici società.

Lo stato di fatto
Infocamere, la società consortile di informatica delle Camere di Commercio, fin dalla sua inclusione nell'elenco dei certificatori il 6 aprile 2000, si è contraddistinta per intraprendenza, in ciò spronata dalla citata legge 24 novembre 2000, n. 340. Un dinamismo e una politica di diffusione (distribuzione gratuita del software di firma digitale, nonché delle smartcard e dei certificati ai rappresentanti legali delle imprese e - sembra - anche agli "sviluppatori di applicazioni") che le è valsa una denuncia (per ragioni più complesse di quelle esposte) all'Autorità Garante della Concorrenza e del Mercato da parte della prima citata CompEd.

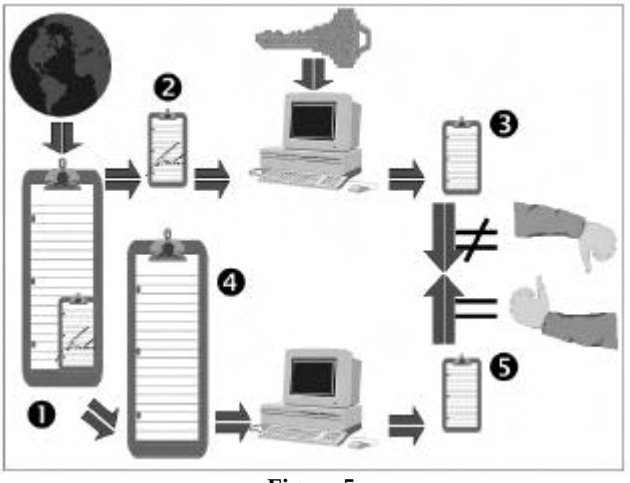

Figura 5

Molti studi, società e professionisti stanno quindi adottando come modello di riferimento quello di Infocamere, che prevede l'installazione di diversi software e drivers dotati di un buon livello di interoperabilità ma - inutile negarlo - di utilizzo non certo immediato.
Tanto che è ormai comune - in molte città - vedere il lettore di smart card timidamente appoggiato di fianco al monitor e correttamente collegato tra tastiera e computer, nonché alla porta seriale. Ma è

assai più raro vedere installato, ad esempio, il software GhostScript e il redirector RedMon della porta parallela che consente di generare un file PDF a partire da qualsiasi applicazione Windows.
La scelta del formato PDF è senza alcun dubbio vincente: in tal modo è possibile produrre documenti "portabili", che verranno cioè

Figura 6

stampati (mediante il diffuso Acrobat Reader, figura 7) indipendentemente dalla piattaforma sulla quale si lavora (Windows, Mac, Linux, stampanti ad aghi, a getto, laser...), in conformità a quanto voleva produrre il firmatario e indipendentemente dal possesso di un software "proprietario" come potrebbe essere Word o Excel.
Ma è lecito chiedersi perché ci si sia voluti basare su strumenti sì pregevoli e free come GhostScript - ma dall'installazione non immediata - piuttosto che su soluzioni "chiavi in mano" e pronte all'uso, già integrate in un unico pacchetto e autoconsistenti.

Molte potranno essere le resistenze alla firma digitale, in primis perché costringerà tutti ad una correttezza formale senza precedenti (la data e ora di apposizione della firma sono inalterabili, impossibile dunque riservare spazi vuoti nel registro del protocollo...) e spesso disagevole o addirittura incompatibile con altre branche della burocrazia.
L'unico modo per superare gli ostacoli, oltre all'obbligo legislativo, è quello di fornire strumenti semplici da installare, semplicissimi da configurare, rapidi da utilizzare.
La soluzione Infocamere, pur interessante e innovativa sotto molti aspetti, non sembra soddisfare tutti questi requisiti e diventa quasi problematica quando anche uno solo dei firmatari non sia dotato di smart card.
Il documento elettronico dovrebbe semplificare le procedure ma purtroppo - in ambito burocratico - diventa spesso e inevitabilmente un semplice surrogato del cartaceo, ereditandone i difetti e complicando le operazioni.

Figura 7