Il lungo cammino del "Testamento elettronico"

di Nicola Bortolotti

La strada del "documento elettronico", più che ad un bivio, è ormai chiaro che sia arrivata ad una "doppia corsia": da un lato - infatti - le tecnologie di firma digitale sono ampiamente utilizzate non solo dai privati (in primis banche ed aziende con chioschi di vendita su Internet) ma anche - ad esempio - dal Ministero delle Finanze che, per la trasmissione telematica delle dichiarazioni dei redditi varata quest'anno, ha predisposto un meccanismo di protezione e validazione a chiavi asimmetriche (decreto Min. Fin. 31/7/1998, pubblicato nella G.U. n. 187 del 12/08/1998).

Lenta rivoluzione

Sull'altro versante più propriamente "burocratico", invece, di "documenti elettronici" a norma di Legge non ne possiamo ancora vedere, e - verosimilmente - dovremo aspettare mesi perché la tanto attesa rivoluzione inizi il proprio cammino.
In altre parole, il "testamento telematico" - forse l'applicazione che assurge ad emblema dell'evoluzione tecnologica nell'immaginario collettivo - non sembra di prossima attuazione.
Come già previsto nei numeri 1/98, 2/98 e 3/98 di "Nuova Antigone", il DPR 10 Novembre 1997 pubblicato sulla Gazzetta Ufficiale n.60 Serie Generale del 13/3/1998 (e riprodotto nella sezione dedicata alla documentazione del numero 2/98), non poteva che essere considerato unicamente un punto di partenza - seppure assai meditato - per il presumibilmente lungo (e fulgido) cammino del documento elettronico "firmato" (si veda al proposito il fascicolo 3/98).

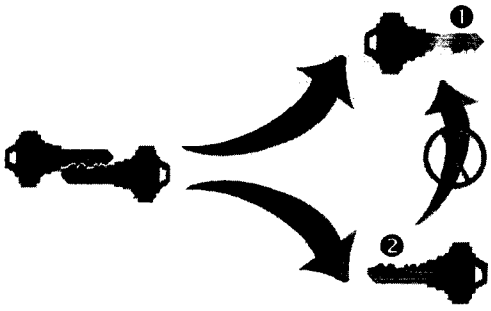

Figura 1 - Per comprendere - per lo meno a grandi linee - il senso del DPCM 8/2/1999 citato nell'articolo e di carattere prettamente tecnico, può essere utile un riepilogo per immagini della tecnica di validazione dei documenti a chiave asimmetrica. Nella figura si assiste alla fase di generazione della coppia di chiavi. Con (1) si è indicata la chiave privata (da conservare gelosamente) e con (2) la chiave pubblica. E' fondamentale osservare che l'ottenere la (1) a partire dalla (2), sebbene non impossibile dal punto di vista teorico, è - di fatto - impraticabile.

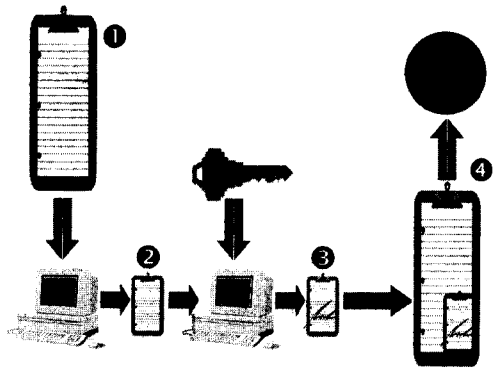

Figura 2 - Il meccanismo di validazione prevede la generazione automatica - mediante un algoritmo di "hash" - di un'impronta del documento (2) che viene poi cifrata mediante la chiave privata diventando così una "firma" (3) apposta in calce. Si noti che la firma non dipende solo dall'identità di chi scrive ma anche dal documento. Si assiste cioè alla validazione non del supporto (come accade in una firma tradizionale - pressoché sempre uguale - apposta su un foglio di carta indipendentemente da ciò che vi è scritto) ma del contenuto stesso.

Firma elettronica "a due velocità"

Oggi - all'indomani della pubblicazione sulla G.U. n. 87 Serie Generale parte prima del 15/4/1999 dell'atteso DPCM 8/2/1999, ossia del regolamento 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 Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513" che si riproduce in documentazione - la sensazione di assistere impotenti ad uno dei tanti "scollamenti" fra mondo "reale" e "burocratico" si rafforza ulteriormente, pur riconoscendo il fatto che non vi possa essere alcuna alternativa percorribile.

Il punto è la certificazione...

Ferme restando le solide basi matematiche della crittografia a chiavi asimmetriche, già ampiamente presentate e discusse nei numeri citati di Nuova Antigone, il punto basilare della questione rimane infatti uno ed uno solo: chi "certifica" (e garantisce, a fronte di possibili conseguenze civili e penali di potenziale enorme entità) che il possessore di una

determinata coppia di chiavi sia effettivamente colui che afferma di essere?

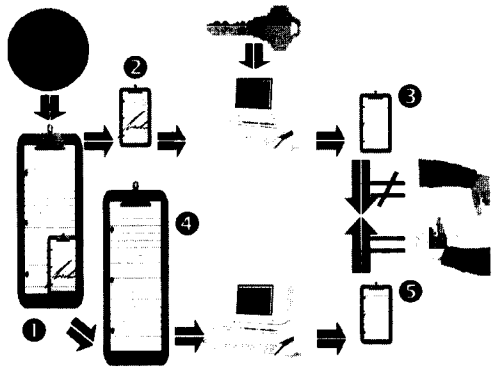

Figura 3 - Il processo complementare - di verifica di autenticità del documento - prevede di decifrare la firma (2) mediante la corrispondente chiave pubblica e ottenere un'impronta (3) che dev'essere uguale a quella prodotta (5) applicando l'algoritmo di hash, prima citato, al documento (4).
Se le due "impronte" differiscono, il documento è contraffatto.
Il mettere a disposizione le chiavi pubbliche - nonché l'assicurare il fatto che a una determinata chiave pubblica corrisponda una ben precisa ed accertata identità - è compito del certificatore.
In realtà il meccanismo previsto dalla legge è più complesso: alla firma deve essere infatti associato anche un certificato della firma, ossia un apposito documento ("firmato" dal certificatore) che contiene una sorta di identikit dettagliato del firmatario.

...ma a non tutti interessa

Questo aspetto può essere parzialmente trascurato per gran parte delle transazioni commerciali.
Si pensi, ad esempio, ad un personaggio che si qualifica come "XY" che decida di acquistare un bene la cui vendita non sia in alcun modo sottoposta a restrizioni: una volta che il suo ordine sia validato, il prodotto recapitato ad un certo indirizzo e la somma "coperta", il fatto che il personaggio sia effettivamente "XY" non è di grande interesse.
Inoltre, anche in caso di contenzioso, l'indirizzo "fisico" di recapito e la ricostruzione della provenienza dei messaggi che hanno costruito la transazione dovrebbero consentire una composizione della controversia abbastanza rapida (tacendo tuttavia delle possibili implicazioni di diritto internazionale).

...nemmeno alle banche (apparentemente)

Per i servizi di "home banking" il discorso è concettualmente diverso ma le conclusioni analoghe: l'apertura di un contratto di banca telematica, infatti, avviene secondo modalità tradizionali, con firma autografa apposta su carta dopo accertamento dell'identità dello scrivente - presente "in persona" - mediante metodiche assolutamente "classiche". Solo allora viene assegnata la coppia di chiavi (e spesso il software proprietario) che consente poi di dialogare con la propria banca via Personal Computer con un elevato grado di sicurezza. Si noti che ciò comunque avviene limitatamente alle transazioni bancarie con la propria banca; inoltre, la fase cruciale di "certificazione" avviene in modo tutt'altro che elettronico.

... e così trionfa un approccio "disinvolto"

Questo è il motivo principale per cui la "firma digitale" su Internet e nelle banche è utilizzata quotidianamente con grande disinvoltura (conseguendo notevoli risultati ed efficienza), al di là di quanto stabilito da qualsivoglia DPR o DPCM: al di là dunque di regole, di vincoli, di norme di attuazione et similia.
E questa è anche la ragione per cui sistemi di certificazione non a norma di legge italiana (intendendo con ciò: non "fuori" legge bensì non riconosciuti da essa!) vengono correntemente e proficuamente utilizzati per validare lo scambio di messaggi e programmi; e questo è infine il motivo per cui programmi eccezionali come il giustamente celebrato PGP (illustrato nel numero 3/98) - la cui sostanziale "anarchia" non ne consentirà l'uso in ossequio alla legislazione italiana - rimarrà pur sempre uno "standard di mercato" per quanto concerne lo scambio di messaggistica protetta e validata non solo all'interno della comunità telematica ma anche e soprattutto in contesti aziendali nazionali e internazionali che ne hanno fatto il loro software "ufficiale".
E lo stesso avverrà per le estensioni "sicure" di Microsoft Outlook e Outlook Express, per citare due prodotti commerciali...

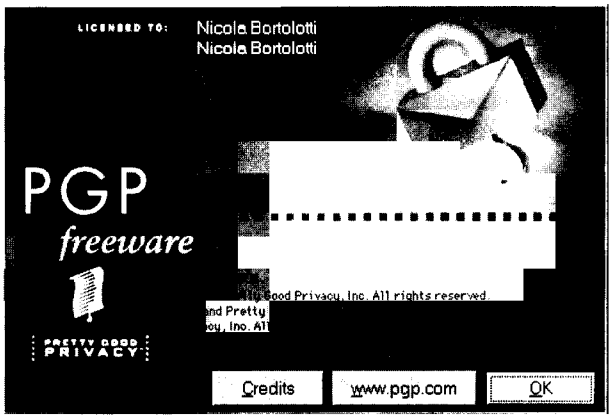

Figura 4 - La legge parla esplicitamente di un "dispositivo di firma" definendolo "un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali".
Qualsiasi software, come il giustamente celebre PGP, non sarà dunque adeguato a "firmare" digitalmente documenti che aspirino ad essere validi "per legge"; il "dispositivo di firma", infatti, è un apparato hardware che deve contenere al suo interno almeno un numero di serie univoco e non modificabile, una sorta di "smart card" dedicata alla firma elettronica.

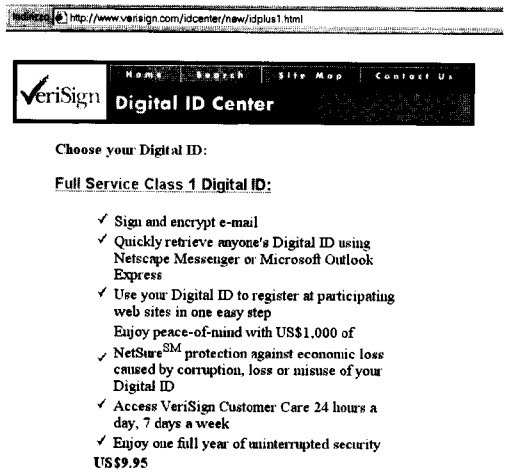

Figura 5 - Lontane dal meccanismo previsto dalla legge italiana anche le "Certification Autorithy" internazionali, tra le quali una delle più note è Verisign. La inidoneità, tuttavia, non si limita al "dispositivo di firma" ma anche ai requisiti assai stringenti richiesti alle società aspiranti all'attività di certificatori.

La prospettiva realmente rivoluzionaria è quella burocratico-legale

Il problema è dunque nella diversa ottica nella quale vedere il problema.
E, da ciò, discende quanto sia diversa ma non - come potrebbe apparire - di retroguardia la visione del legislatore.
L'approccio formale burocratico-legale è - paradossalmente - quello in realtà rivoluzionario, in quanto porta alla "smaterializzazione" della propria identità: non più legata alla carta bensì al messaggio stesso; non più legata alla presenza fisica bensì intimamente legata alla produzione di documenti elettronici, immateriali, diretta emanazione del proprio pensiero...

Il discorso porterebbe lontano, in termini del resto già abusati anche da "guru" come Nicholas Negroponte: è tuttavia incontestabile che così diverse premesse conducano ad aspetti regolamentativi inevitabilmente delicati e complessi.

Vademecum per certificatori

Ecco quindi il DPCM 8/2/1999 diventare un autentico vademecum per "aspiranti certificatori", soffermandosi su normative tecniche internazionali semplicemente citate e non allegate (in quanto coperte da copyright, il che porta ad una situazione ambigua di una legge non pubblicabile nella sua interezza) sin dal Titolo I (Regole tecniche di base).
I "Titoli" più interessanti sono tuttavia i successivi, dove viene esplicitato nel dettaglio il "sistema qualità e sicurezza" richiesto tassativamente ai certificatori, non bastasse il capitale sociale non inferiore a quello richiesto per l'attività bancaria a restringere la rosa dei pretendenti...
Dettagliato e tecnicamente ineccepibile anche il capitolo dedicato alla validazione temporale.
Requisiti stringenti - tuttavia necessari per le notevoli responsabilità connesse all'attività di certificatori - che fanno sì che, alla data di redazione dell'articolo, non ve ne sia nessuno attivo né in Italia né all'estero; in aggiunta: il dispositivo di firma dovrà essere rigorosamente hardware e dunque nessun software gratuitamente disponibile sarà adeguato allo scopo.
E' comunque sperabile che tale imponente "corpus" di adempimenti non finisca per "ingessare" lo sviluppo di un sistema - sulla carta - rivoluzionario.

Perché non una "autocertificazione" digitale?

Non sarebbe stato tuttavia opportuno prevedere anche una modalità di certificazione "leggera", una sorta di equivalente digitale dell'autocertificazione?

I risultati sarebbero stati comunque di assoluto rilievo: non dimentichiamo infatti che - in palese disprezzo di ogni considerazione tecnica - per questioni di opportunità è stato dato - nell'immediato passato - valore legale ad un sistema di trasmissione quanto mai inaffidabile e falsificabile come il fax.
E rimane intatta una considerazione di fondo: molti notai, avvocati e dipendenti della pubblica amministrazione inevitabilmente freneranno lo sviluppo di un sistema intrinsecamente complesso che "non capiscono" (così come fanno fatica a comprenderlo appieno anche alcuni addetti ai lavori!) e di cui - dunque - non si fidano affatto.

Resistenze difficili da superare

Gli esempi di miopia - a livello peraltro assai inferiore - non mancano: in occasione dei recenti bandi di concorso riguardanti la scuola, a dispetto di ogni pretesa di semplificazione, era impossibile effettuare la domanda via web o posta elettronica.

Non solo: alcune sovrintendenze suggerivano - pena esclusione - di evitare i moduli agevolmente "scaricabili" e stampabili via Internet in quanto su quattro diversi fogli "A4" e non recanti l'intestazione "Gazzetta Ufficiale" assieme al relativo numero di pagina.

Meglio dunque una sgualcita fotocopia fronte/retro in formato A3, sempre in attesa della firma digitale...