Vademecum minimo in tema di funzione notarile e firma digitale

giugno 2000

ugo bechini, ugo@altavista.net

---

cliccando sul richiamo delle note, queste appaiono del frame a fianco. Cliccare qui per una versione Microsoft Word (.doc), più adatta alla stampa

---

Facile, facilissimo. Apporre una firma digitale è quel che si dice un gioco da ragazzi. Si introduce una tessera, detta *smart card*, nell'apposita fessura, si digita una *password*, si premono pochi altri pulsanti ed è fatta. Non è più complicato di un prelievo Bancomat. Un utilizzo consapevole del mezzo, che tenga conto delle sue implicazioni tecniche e giuridiche (1), è evidentemente un altro discorso.

Dalla firma digitale si richiedono fondamentalmente due cose: l'attestazione della provenienza della dichiarazione, cui nella realtà cartacea provvede la sottoscrizione, e la non alterabilità del suo contenuto. La soluzione ormai standard a livello mondiale consiste nell'uso di un sistema crittografico, proposto nel 1975 da Witfield Diffie e Martin Hellman, e portato poi a maturità nel 1977 da Ronald Rivest, Adi Shamir e Leonard Adleman (2) con la tecnica detta, dalle loro iniziali, RSA: la crittografia a chiavi asimmetriche. Per comprendere il nesso che lega la crittografia asimmetrica alla sottoscrizione digitale converrà prendere le mosse dalla tradizionale crittografia a chiavi *simmetriche*.

La crittografia simmetrica è ben nota a tutti fin dai banchi delle scuole elementari. Pensiamo al "sistema" che utilizza come chiave la sostituzione di ogni lettera con quella che immediatamente la precede nell'ordine alfabetico: ad esempio "Ibm" diviene "Hal" (3). Ovviamente è possibile creare codici infinitamente più raffinati, come nel caso del sistema tedesco Enigma, impiegato durante la Seconda Guerra Mondiale, ma una caratteristica resta costante: chi possiede la chiave per decriptare un messaggio può creare a sua volta un messaggio nello stesso codice.

Nei sistemi a chiavi asimmetriche invece l'utilizzatore produce, avvalendosi di un software (4) di semplicissimo utilizzo (5), due chiavi, dette rispettivamente "chiave pubblica" e "chiave segreta": il perno dell'intero sistema consiste nel fatto che le due chiavi sono ben distinte ed è matematicamente impossibile ricavare l'una dall'altra (6). Un testo criptato con una qualunque chiave pubblica può essere letto soltanto se si possiede la corrispondente chiave segreta. La chiave segreta deve essere accuratamente custodita (7), quella pubblica può, ed anzi in un certo senso deve, essere diffusa il più possibile, senza alcuna precauzione: tipicamente, questa è depositata in archivi liberamente accessibili a chiunque via Internet.

L'utilizzo più ovvio è quello propriamente crittografico. Se Tizio desidera inviare a Caio un messaggio inviolabile per chiunque altro, gli è sufficiente criptare il messaggio utilizzando la chiave pubblica di Caio: solo quest'ultimo, che dispone della relativa chiave segreta, può leggerne il contenuto. Non occorre previo accordo tra Tizio e Caio, e neppure che i due si conoscano: la chiave pubblica di Caio è a disposizione di tutti. Ancora più importante: non c'è bisogno di alcun canale di comunicazione sicuro tra Tizio e Caio, perché essi non debbono condividere alcuna informazione riservata; la chiave segreta di Caio resta sulla *smart card* di Caio, e non deve essere comunicata a chicchessia.

La stessa tecnologia può essere impiegata per la sottoscrizione nel modo seguente. Il testo (8) da inviare resta in chiaro, leggibile per chiunque. Il medesimo testo viene pure criptato avvalendosi della chiave segreta del sottoscrivente; il messaggio in cifra che ne deriva è appunto la firma digitale, e viene acclusa al testo in chiaro (9). La firma digitale di ciascun soggetto varierà pertanto a seconda del

contenuto del messaggio: ciò ne impedisce l'uso fraudolento in calce ad un altro documento (10). Il destinatario, o qualunque soggetto comunque interessato, procuratasi la chiave pubblica del mittente, confronta messaggio e firma digitale. Se il confronto dà esito positivo, due cose sono accertate. In primo luogo, il messaggio proviene sicuramente da quel mittente: solo lui (o lei) possiede la chiave segreta che consente di produrre una firma riconoscibile dalla chiave pubblica corrispondente. In secondo luogo, il messaggio non è stato alterato: se così fosse, non vi sarebbe più corrispondenza tra messaggio e firma. Questo spiega perché un messaggio provvisto di firma digitale possa essere trasmesso anche attraverso reti intrinsecamente insicure (come Internet) (11), senza che ci si debba preoccupare della possibilità di intercettazioni od alterazioni: come si è visto la firma, anche se intercettata, non è riutilizzabile, e le manipolazioni emergerebbero in sede di controllo.

Nulla vieta, naturalmente, di eseguire entrambe le operazioni sul medesimo messaggio, che sarà quindi firmato digitalmente e leggibile solo dal destinatario (12).

I moderni softwares di posta elettronica fanno sì che la verifica della firma avvenga senza che l'utente debba preoccuparsi di premere neppure un tasto: il programma, constatata l'esistenza di una firma digitale su un messaggio in arrivo, si collega automaticamente con l'archivio delle chiavi pubbliche, verifica la firma, e fa apparire sul video un'icona: firma verificata (o non verificata, se del caso). L'operazione di firma o di criptazione è appena più complicata. La chiave segreta è contenuta sulla *smart card*, che ha le dimensioni di una carta di credito: questo sia per evitare di lasciare un dato così delicato all'interno di un computer, sia per consentirne l'uso (itinerante, per così dire) con qualunque computer attrezzato all'uopo. Si sceglie il file da firmare, si introduce il proprio PIN (come nel Bancomat), si clicca su "Firma" e l'operazione è conclusa.

Vi è in quanto fin qui descritto un evidente punto debole: come può il destinatario del messaggio essere certo che la chiave pubblica che egli adopera per la verifica appartenga veramente al mittente? Sotto un diverso angolo visuale: come può il destinatario dimostrare la riferibilità della chiave al mittente onde contrastare un eventuale tentativo da parte di quest'ultimo di disconoscere il documento od il suo contenuto?

Entra qui in campo la cosiddetta *Certification Authority*, ente pubblico o società provvista di requisiti analoghi a quelli richiesti per l'esercizio dell'attività bancaria. La sua funzione (13) è attestare a chi appartenga una determinata chiave pubblica: all'uopo deve procedere innanzitutto alla materiale identificazione dell'interessato, mantenendo le informazioni a disposizione di chiunque in un archivio *online*, da cui far emergere anche l'eventuale cessazione di validità della chiave, per avvenuta scadenza o revoca. Sulla base delle risultanze dell'archivio chiunque può dimostrare che un determinato documento è stato firmato con la chiave, valida e non scaduta, di Tizio (od almeno: della persona che la *Certification Authority* ha identificato come Tizio).

Il sistema pone evidentemente delicatissimi problemi di responsabilità, connessi all'accuratezza dell'identificazione ed all'efficiente (e tempestiva!) gestione dell'archivio. Ancora non del tutto risolti sono inoltre alcuni problemi legati alle speciali attribuzioni di firma che possono competere ad un determinato soggetto (14). L'analisi di tale problematica va ben al di là delle possibilità di questo brevissimo scritto; si consentirà pertanto di prescinderne, assumendo quale ipotesi di lavoro che i malfunzionamenti del sistema siano assolutamente trascurabili.

Resta un ulteriore passaggio: il fatto che la chiave pubblica appartenga a Tizio, non vuol dire che una determinata firma digitale sia stata apposta da Tizio. Può darsi che egli abbia affidato la propria *smart card* a qualcun altro, rivelandogli anche il relativo PIN; la firma così apposta è totalmente indistinguibile da quella realizzata direttamente dal titolare. Se Tizio è un imprenditore, possiamo metabolizzare una simile eventualità riconducendo i rischi di abusivo utilizzo della firma all'area del più generale rischio d'impresa; nel caso di un privato le cose si fanno evidentemente più delicate,

almeno da un punto di vista sociale. Se la firma corrisponde poi ad una funzione intrinsecamente indelegabile (quella di un giudice, di un notaio, di un pubblico funzionario) la semplice prospettiva di una delega de facto diviene difficilmente tollerabile (15).

La tecnologia si propone di risolvere anche questo problema. La *smart card* può incorporare alcuni dati biometrici del soggetto: l'impronta digitale, la forma della mano o del viso, la voce, l'immagine della retina o dell'iride. Il sistema può quindi essere impostato in modo da impedire l'apposizione della firma laddove il titolare non dimostri di essere presente appoggiando le dita su un lettore d'impronte digitali od avvicinando l'occhio ad una telecamera. Tali sistemi, già entrati nell'uso comune (16), pongono peraltro significativi problemi di sicurezza (17).

A rigore, non si può quindi affermare che la firma digitale assicuri in modo assoluto l'identificazione del sottoscrivente; per converso è del tutto ragionevole immaginare che nel complesso i rischi siano assolutamente accettabili, e non superiori a quelli connessi all'impiego di sistemi cartacei.

Occorre a questo punto porsi con franchezza una domanda. Quale significato può conservare, in un simile contesto, il ruolo del notaro?

Un dato deve essere messo a fuoco con assoluta chiarezza. L'identificazione delle parti è un passaggio ineliminabile ma ormai di secondaria importanza nell'ambito della funzione notarile. Il baricentro dell'attività notarile sta da tempo altrove: nell'attività di informazione e di assistenza dei contraenti, sul piano civilistico come su quello fiscale; nella ricerca delle soluzioni che meglio realizzano le intenzioni delle parti. La particolare autorevolezza del notaro, che gli deriva sia dalla sua specifica ed approfondita preparazione, sia dall'essere Pubblico Ufficiale al di sopra delle parti (e non al servizio di una parte), fa sì che la stragrande maggioranza delle operazioni possa essere conclusa col suo solo intervento, senza cioè che ciascuna delle parti debba sobbarcarsi il costo di un proprio consulente. Molte controversie vengono anche bonariamente composte con l'aiuto del notaro, prima che sfocino in vere e proprie cause. Il notaro svolge inoltre una funzione di pubblico interesse. In primo luogo limita, attraverso la sua opera preventiva (18), l'intasamento della giustizia: in Europa, ove con pochissime eccezioni operano notariati organizzati in modo molto simile a quello italiano, le controversie nelle materie di competenza notarile sono enormemente meno numerose rispetto a quanto accade, ad esempio, negli Stati Uniti, con costi globalmente molto inferiori per la collettività. Svariate norme di legge assegnano infine al notaro, oltre al tradizionale controllo di legalità degli atti, specifiche funzioni nell'ambito della repressione dell'abusivismo edilizio, dell'evasione fiscale, del riciclaggio di denaro sporco in attività economiche.

L'insieme di queste funzioni non rappresenta in alcun modo un retaggio del passato: la maggior parte dei compiti appena citati derivano anzi da legislazione recente, dell'ultimo quindicennio (19). Tale trend ha riscontro a livello mondiale: il notariato come noi lo conosciamo in Italia, il cosiddetto notariato latino, sta vivendo una fase di grande diffusione: al tradizionale nucleo storico (tra cui Italia, Francia, Germania e Spagna) si sono affiancate numerosissime altre realtà, a cominciare dal Giappone; i Paesi che nell'ultimo decennio si sono affacciati all'economia di mercato, soprattutto nell'Est Europeo, hanno aderito in massa al modello latino, ivi compresa la stessa Russia. Oltre settanta (20) Paesi sono oggi dotati di un'organizzazione notarile di tipo latino.

Non solo la firma digitale non potrà quindi sostituire la funzione notarile (21): è anzi probabilmente vero il contrario. Per averne riscontro, basta guardare a ciò che sta avvenendo negli Stati Uniti.

Il Public Notary americano è una figura di assai ridotta qualificazione professionale, il cui compito si limita all'identificazione del sottoscrittore (22). Ne discende, tra l'altro, che i documenti notarili americani sono accettati con difficoltà al di fuori degli Stati Uniti; ciò è già sufficientemente grave in un sistema basato su documenti cartacei, ma rischia di divenire esiziale nel mondo telematico, globale

per definizione. Una parte significativa del mondo giuridico statunitense guarda quindi da tempo all'istituzionalizzazione del sistema di firme elettroniche come ad una felice occasione per colmare una lacuna del proprio sistema. In questo contesto emerge la proposta, fatta propria dall'American Bar Association (23), di istituire negli USA una nuova figura professionale, denominata appunto *Cybernotary*, espressamente ispirata al notaro di tipo latino, cui affidare la produzione di documenti dotati di elevata credibilità sul piano internazionale (24). Il primo Stato dell'Unione a dotarsene è stato, nel maggio 1997, la Florida (25).

Con ciò si compie una duplice, incrociata nemesi storica: la miglior conferma della vitalità del modello latino proviene dall'area geografica che più flagrantemente ne aveva finora ignorato l'esistenza stessa, ed è maturata all'interno di un settore, quello dell'informatica e della telematica, che per mero pregiudizio viene talora inquadrato in termini di antagonismo od incompatibilità con il notariato stesso.

Nel frattempo, si sta per passare alla pratica. I notai italiani saranno certamente tra i primi ad avvalersi su larga scala della firma digitale, soprattutto nella trasmissione dei documenti tra loro e nei confronti della Pubblica Amministrazione. Anche degli atti originariamente creati in forma cartacea potranno essere prodotte copie in forma digitale (26), da trasmettere ad esempio via Rete ai pubblici uffici in modo economico e veloce per le formalità di registrazione, iscrizione, trascrizione e volturazione, per la maggior sicurezza di tutti.