La firma ed i documenti digitali

di Nicola Bortolotti

Chi assicura che un "modello di firma" (chiave pubblica) sia stato effettivamente generato dall'individuo che si dice essere? In parole tradizionali: chi fa le veci della "carta d'identità" e dell'autorità che la rilascia? E' questa la domanda che chiudeva l'articolo introduttivo sulla firma elettronica pubblicato nel numero precedente di "Nuova Antigone".

Una domanda fondamentale alla quale verrà data risposta facendo ricorso alla versione definitiva del DPR 10 novembre 1997, n. 513 ("Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59") pubblicato sulla Gazzetta Ufficiale n. 60 serie generale del 13/3/98 e che riportiamo in documentazione.

Prima di proseguire è però opportuno ricordare ed esemplificare i concetti presentati la volta scorsa, analizzandoli da un punto di vista diverso, più applicativo.

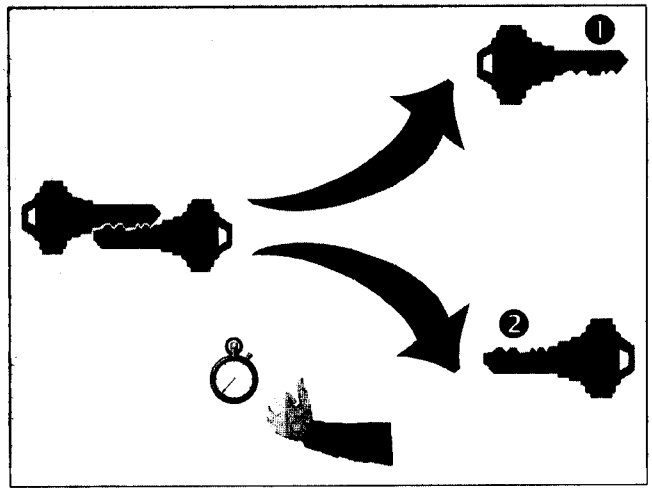

Figura 1 - Il processo di generazione di una coppia di chiavi per algoritmo di cifratura asimmetrica (si è indicato con 1 la chiave privata e con 2 la corrispondente chiave pubblica) è assai veloce utilizzando programmi dedicati come PGP.

Come firmare digitalmente

Forse nulla è più facilmente copiabile di una sequenza di bytes. Ecco perché il concetto di firma digitale deve essere radicalmente differente (senza che ciò implichi minor sicurezza) da quello della firma tradizionale: la firma apposta su carta è infatti legata alla calligrafia della persona che la appone ed è sicura nella misura in cui non possa essere "imitata" (copiata) da qualcun altro; copia che, nel caso informatico, è tuttavia banalmente fattibile in maniera del tutto indistinguibile dall'originale. Ecco quindi che *la firma digitale è associata allo scrivente non direttamente, ma attraverso il documento che si vuole firmare*. Ciò significa che *due diversi documenti "firmati" digitalmente dalla stessa persona avranno necessariamente due "firme" diverse.*

Assumere un'identità digitale

Se le firme sono diverse, come risalire allora all'identità di chi scrive? E, comunque, in che cosa consiste effettivamente "firmare digitalmente"? In realtà la firma digitale si realizza generando un copia "cifrata" del documento (o - meglio - di un'"impronta" di esso, ossia di una sorta di sommario generato automaticamente) mediante algoritmi crittografici a chiavi asimmetriche. "Chiavi asimmetriche" vuol dire che la chiave utilizzata per cifrare è diversa (seppure intimamente legata) da quella utilizzabile per decifrare. Il primo passo per poter firmare digitalmente un proprio documento è dunque quello di assumere un'identità digitale, il che consiste nella generazione di una coppia di chiavi (figura 1), una delle quali verrà denominata "privata" (la 1) mentre l'altra "pubblica" (la 2). Il destino di queste due chiavi sarà assai diverso: la "privata" andrà custodita gelosamente (figura 2) *in quanto il suo possesso equivale al possesso dell'identità dello scrivente*, ossia alla capacità virtuale di poter imitare perfettamente la sua firma. La "pubblica" dovrà essere invece resa disponibile, in quanto tramite essa sarà possibile determinare con certezza che un dato messaggio (corredato della sua cifratura) è stato generato da colui che detiene la corrispondente chiave privata.

Le garanzie offerte dal sistema

La sicurezza del sistema risiede nella enorme difficoltà computazionale insita nella ricostruzione della chiave privata a partire da quella pubblica (figura 3): un compito improbo in tempi ragionevoli anche unendo le forze dei più potenti calcolatori mondiali. E, quand'anche la potenza di calcolo aumentasse, sarebbe sufficiente aumentare la lunghezza delle chiavi per rimanere tranquilli (la complessità matematica di questi problemi è quanto meno esponenziale)

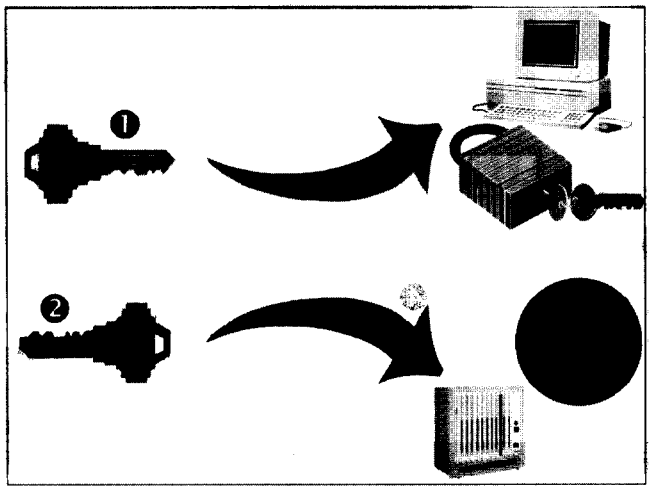

Figura 2 - Il destino delle due chiavi, una volta generate, è assai dissimile: la chiave privata andrà infatti gelosamente custodita (in quanto perderla significherebbe perdere la possibilità di "essere se stessi" dal punto di vista digitale, così come diffonderla consentirebbe ad altri di appropriarsi della nostra identità); la chiave pubblica (2) andrà invece certificata e registrata presso un certificatore, che sarà tenuto fra l'altro a renderla disponibile a chiunque per via telematica.

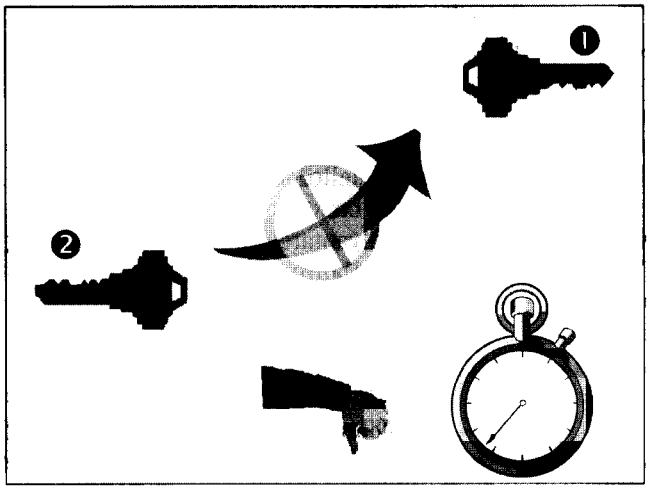

Figura 3 - La sicurezza intrinseca dell'algoritmo di cifratura asimmetrico è costituito dal fatto che, data una chiave pubblica di sufficiente lunghezza, è pressoché impossibile risalire da essa alla corrispondente chiave privata trattandosi di un problema matematico di elevata complessità computazionale.

L'autorità di certificazione

Essere sicuri che un certo documento (validato per mezzo di una certa chiave pubblica) sia stato generato da colui che detiene la chiave privata associata non è però sufficiente: chi assicura infatti la corrispondenza tra chiave e soggetto autore del messaggio? In altre parole: chi garantisce che una certa chiave pubblica identifichi effettivamente una certa persona? E' a questo punto che entra in campo il cosiddetto "certificatore" (artt. 1, 8 e 9 del DPR 513) al quale spetterà: "a) identificare con certezza la persona che fa richiesta della certificazione; b) rilasciare e rendere pubblico il certificato avente le caratteristiche fissate con il decreto di cui all'articolo 3; c) specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite; d) attenersi alle regole tecniche di cui all'articolo 3; e) informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi; f) attenersi alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675; g) non rendersi depositario di chiavi private; h) procedere tempestivamente alla revoca od alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni; i) dare immediata pubblicazione della revoca e della sospensione della coppia di chiavi asimmetriche; l) dare immediata comunicazione all'Autorità per l'informatica nella pubblica amministrazione ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività e della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento"

Gli obblighi del certificatore

E' dunque compito del certificatore (punto a) accertarsi preventivamente dell'effettiva identità di colui che deposita *la chiave*. Si noti il singolare: è infatti espressamente vietato per il certificatore (punto g) rendersi depositario di chiavi private in quanto ciò equivarrebbe alla possibilità, per il certificatore, di sostituirsi *in toto* all'effettivo proprietario dell'identità digitale. Sarà cura del certificatore custodire le chiavi *pubbliche* di cifratura "per un periodo non inferiore a dieci anni" e renderle

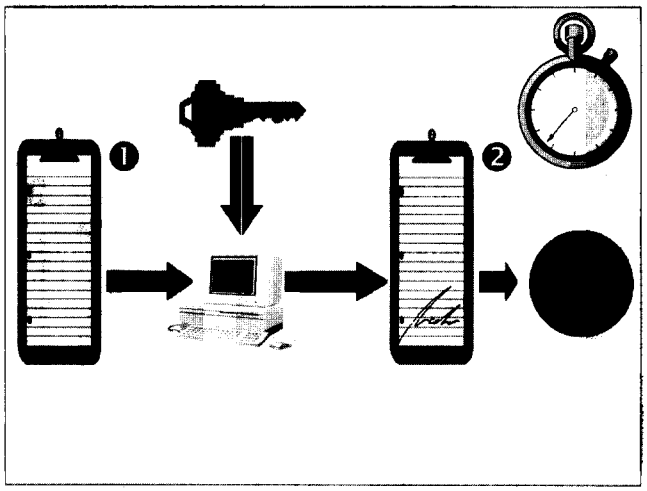

Figura 4 - Un primo esempio di "firma" digitale tramite crittografia asimmetrica prevede la cifratura del documento in chiaro (1) tramite la propria chiave privata e l'unione di esso in calce al testo (2). In tal modo chiunque, richiedendo la chiave pubblica associata, può essere in grado di verificare l'autenticità del documento in quanto il testo decifrato deve corrispondere a quello in chiaro.

"consultabili in forma telematica". Fra i requisiti richiesti ai certificatori, oltre ovviamente a quelli tecnici, nelle varie stesure del DPR ne è rimasto uno abbastanza criticato, in quanto esclude la gran parte degli Internet providers italiani: "forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati". Chi, fra i providers, può vantare 12.5 miliardi di capitale sociale? Uno solo, tra l'altro segnalatosi recentemente per reiterata inefficienza.

Va infine ricordato un ulteriore aspetto, come evidenziato da Mario Terranova dell'Autorità per l'Informatica nella Pubblica Amministrazione: "L'uso dell'autorità di certificazione consente di raggiungere, oltre la certezza dell'identità dell'autore di un messaggio, anche *l'impossibilità da parte di questi di ripudiare i messaggi da egli generati*; infatti, essendo l'unico detentore della chiave privata è anche l'unico soggetto in grado di generare firme verificabili con la corrispondente chiave pubblica".

Firmiamo, dunque...

Una volta certificata e registrata la propria chiave pubblica, si è dunque pronti per firmare digitalmente. Un primo semplice approccio, lento e ridondante, è illustrato in figura 4: in esso, al documento originale viene unita una copia cifrata mediante la propria chiave privata. Il destinatario potrà quindi verificare, decodificando la copia cifrata mediante la chiave pubblica del mittente e verificandone la rispondenza col testo in chiaro, che il testo è effettivamente "genuino". Nella pratica, tuttavia, quest'approccio non è mai seguito (la cifratura a chiave pubblica è estremamente pesante per un personal computer) ed è invece utilizzato quello di figura 5: dal documento in chiaro (fig. 5-1) viene automaticamente estratto un più breve "riassunto" (fig. 5-2) mediante un opportuno algoritmo detto di "hash". Sarà questo riassunto, detto "impronta", ad essere cifrato utilizzando la propria chiave *privata* (fig. 5-3); la cifratura dell'impronta sarà la "firma" del documento che sarà aggiunta in calce al testo stesso (fig. 5-4); quest'ultimo sarà quindi pronto per la diffusione.

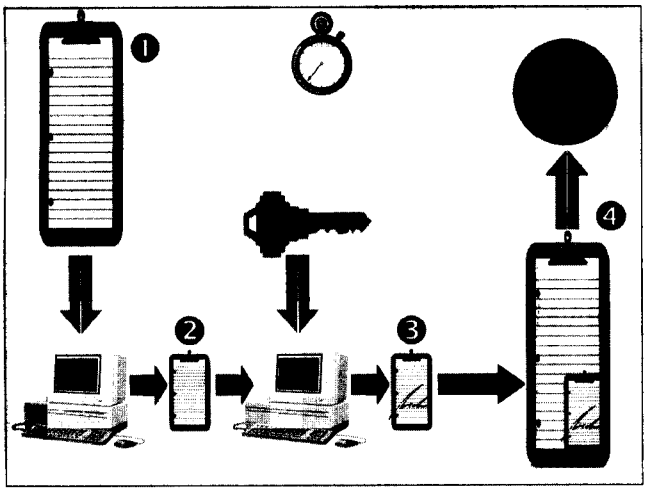

Figura 5 - Poiché la cifratura di un intero documento è assai pesante dal punto di vista elaborativo, viene sempre preferito un altro approccio (che consente anche un ulteriore vantaggio, ossia l'autenticazione del documento senza conoscerlo): a partire dal testo (1) viene automaticamente generato un "riassunto" o "impronta" (2) che viene cifrato tramite la chiave privata, diventando così la "firma" (3) del documento; tale firma viene aggiunta in calce al testo (4).

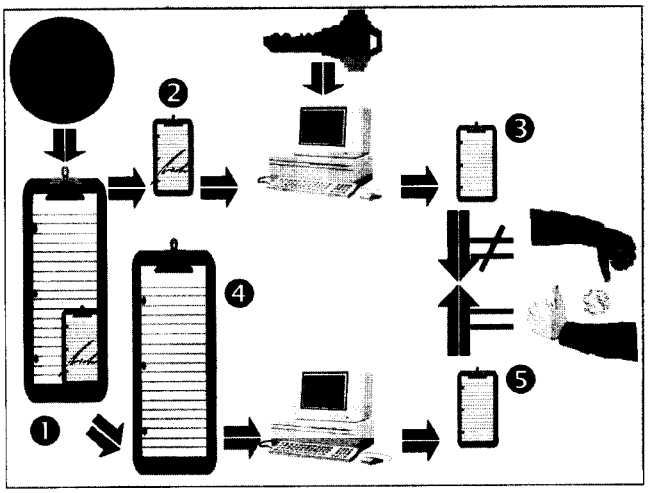

Figura 6 - La verifica di autenticità si opera decifrando la "firma" (2) mediante la corrispondente chiave pubblica e ottenendo dunque una impronta (3). In contemporanea, al documento (4) viene applicata la medesima funzione di generazione del "riassunto" che genererà un'"impronta di riferimento" (5). Se le due impronte saranno uguali, il documento potrà essere considerato autentico.

... e verifichiamo l'autenticità

Il destinatario che volesse verificare l'autenticità del documento, dovrà prima di tutto procurarsi la "carta d'identità digitale" (ossia la chiave *pubblica*) del mittente; per fare questo si rivolgerà al certificatore che è fra l'altro tenuto a renderla "consultabile per via telematica" (e il constatare che nei fine settimana il sito Internet dell'Autorità per l'Informatica nella Pubblica Amministrazione è inaccessibile fa davvero riflettere...). Verrà quindi applicata la procedura illustrata nella figura 6: dal documento (fig. 6-1) verrà estratta la "firma" (fig. 6-2) che sarà decifrata mediante la chiave pubblica ottenendo un'impronta (fig. 6-3). Parallelamente, al testo in chiaro (fig. 6-4) sarà stato applicato il medesimo algoritmo di "hash" utilizzato dal mittente, pervenendo anche in questo caso ad un'impronta (fig. 6-5). Il documento potrà ritenersi "genuino" qualora 6-3 e 6-5 coincidano; in caso contrario dovrà essere considerato contraffatto.

E' doveroso a questo punto osservare che tale sequenza di operazioni viene eseguita in maniera automatica (e sufficientemente agevole per l'utente) da appositi programmi; il più famoso di essi è PGP (Pretty Good Privacy), che sarà oggetto di trattazione nei prossimi numeri.