BERGAMO ECONOMICA
N° 1 - 2000

Certezza tecnica e giuridica si scontrano con la semplificazione dei rapporti tra privati

Francesco Lanorte

Un soggetto che volesse gestire tutti i legami con la Pubblica amministrazione attraverso documenti digitali dovrebbe munirsi di una coppia di chiavi per ciascun ente. Senza contare la complessità della gestione organizzativa di un "portachiavi" affollato, oltre al rischio che deriva dall'impossibilità di ricordare a memoria tutte le password corrispondenti. Ma non solo...

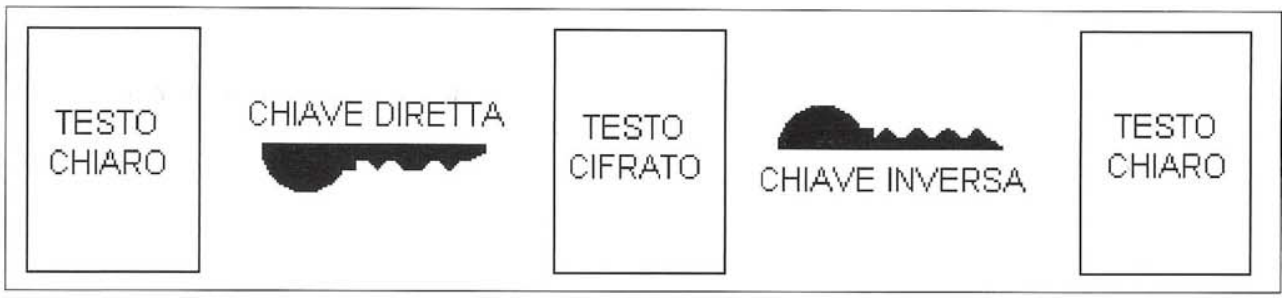
La diffusione degli strumenti informatici e la parallela crescita della comunicazione attraverso le reti di calcolatori hanno posto il problema della sostituzione del tradizionale documento cartaceo con un equivalente strumento informatico. Il meccanismo universalmente adottato per costruire tale strumento è la firma digitale basata sulla crittografia a chiavi pubbliche.

La firma digitale è una informazione che viene aggiunta ad un documento informatico al fine di garantirne integrità e provenienza. In ultima analisi altro non è che un codice numerico. Sebbene l'uso per la sottoscrizione dei documenti formati su supporti informatici sia quello più naturale, essa può essere utilizzata per autenticare una qualunque sequenza di simboli binari, indipendentemente dal loro significato.

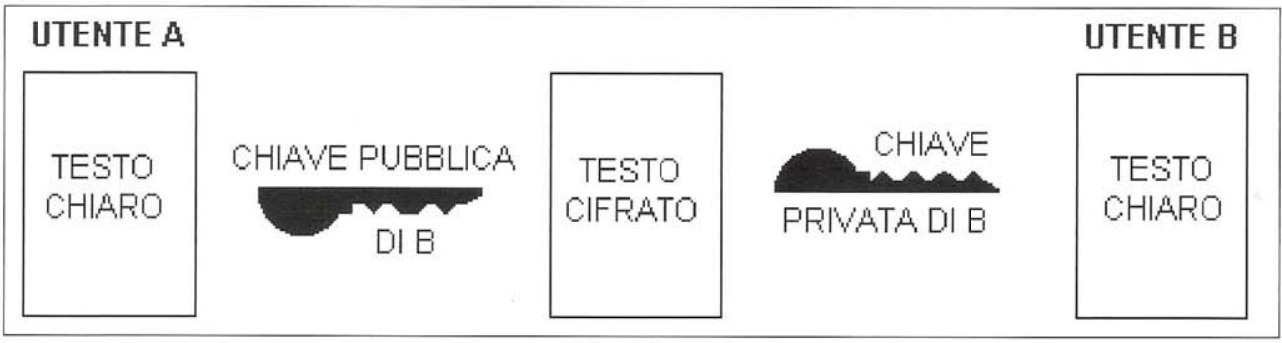
Un esempio sempre più comune di questo uso generalizzato è l'aggiunta di firme digitali ai file contenuti nella memoria di massa di un sistema di elaborazione onde contrastare gli attacchi dei virus e degli hackers.

La principale differenza tra firma autografa e firma digitale sta nel fatto che la prima è direttamente riconducibile all'identità di colui che la appone, poiché la calligrafia è un elemento identificativo della persona, mentre la seconda non pos-

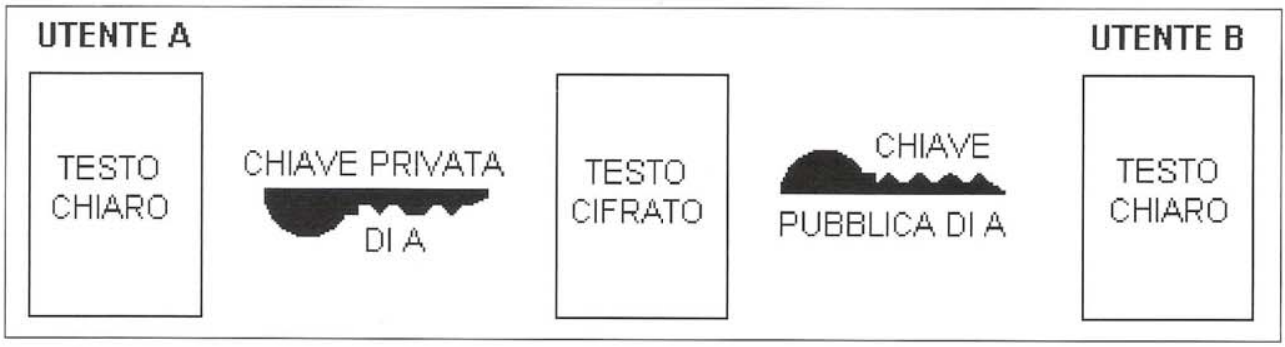
Cifrario simmetrico. In questo caso la stessa chiave serve per cifrare e decifrare il testo.



Cifrario asimmetrico. Cifratura e decifratura di un documento con un cifrario a chiave asimmetrica.



Messaggio cifrato con sistema asimmetrico. Il mittente cifra il testo con la chiave pubblica del destinatario, questi lo decifra con la propria chiave privata.



Testo cifrato con la chiave privata del mittente. Se B riesce a decifrare il messaggio con la chiave pubblica di A, questi è certamente l'autore del testo.

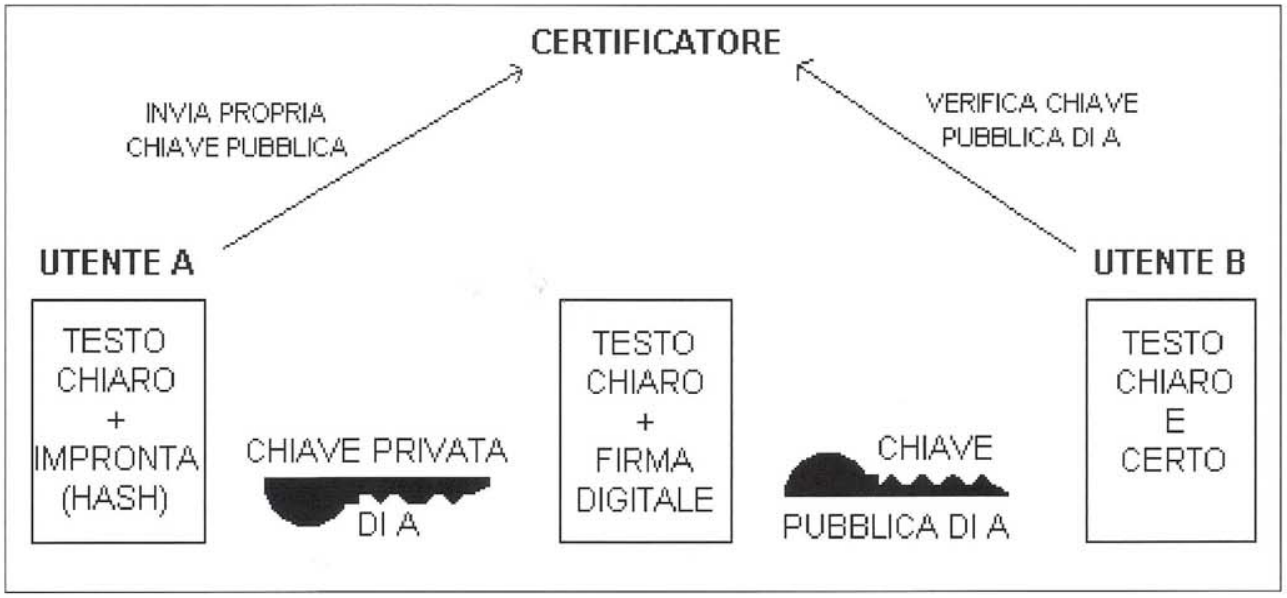
siede questa proprietà. Per coprire questa deficienza si ricorre all'autorità di certificazione, il cui compito è quello di stabilire, garantire e pubblicare l'associazione tra firma digitale e soggetto sottoscrittore.

Per contro, mentre l'associazione tra testo di un documento e la firma autografa è ottenuta esclusivamente attraverso il supporto cartaceo, la firma digitale è intrinsecamente legata al testo a cui è apposta, tanto che i due oggetti possono essere fisicamente separati senza che per questo venga meno il legame esistente tra loro. Conseguenza di ciò è l'unicità della firma digitale, nel senso che a testi diversi corrispondono firme diverse e quindi, nonostante la sua perfetta replicabilità, è impossibile trasferirla da un documento ad un altro.

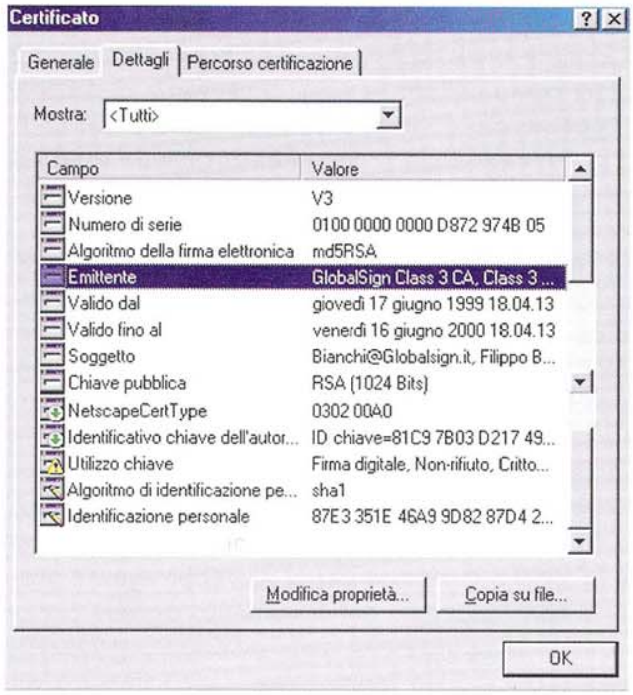
Nella legislazione italiana il riconoscimento della firma digitale e del documento informatico avviene con l'art. 15, comma 2, della Legge 15 marzo 1997, n. 59, la cosiddetta "Bassanini-uno" nella quale si stabilisce che "*gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi a tutti gli effetti di legge*".

Il successivo regolamento attuativo, DPR 153/97, raccoglie i criteri e le modalità di applicazione in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici: in esso è presente una visione complessiva molto avanzata, che si riassume nella formulazione dell'articolo 2: "*Il documento informatico da chiunque formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge se conformi alle*

disposizioni del presente regolamento".
In esso vengono definite le norme generali per la validità della firma digitale rimandando, con l'articolo 3, la definizione dei dettagli operativi a un ulteriore regolamento tecnico.
Si tratta appunto delle "*Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione 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*".
E' un testo estremamente delicato, prima di tutto per quanto riguarda la quantità e la complessità degli adempimenti richiesti; poi perché traccia un solco tra l'impiego del documento digitale nella Pubblica amministrazione e le applicazioni private, in primo luogo il commercio elettronico.
A prima vista sembra addirittura che ci sia una contraddizione tra il regolamento generale e le norme tecniche. Infatti il DPR 513/97, articolo 17, stabilisce che "*le pubbliche amministrazioni provvedono autonomamente, con riferimento al proprio ordinamento, alla generazione, alla conservazione, alla certificazione ed all'utilizzo delle chiavi pubbliche di competenza*", ma l'articolo II.7 delle regole tecniche introduce una norma che appare in contrasto con la validità e rilevanza della firma digitale "a tutti gli effetti di legge": "*E' consentito ai certificatori definire accordi di certificazione mutua*".
Dunque la firma certificata da una pubblica amministrazione può non valere per un'altra, se tra le due non c'è un accordo di mutuo riconoscimento. In pratica, se il ministero delle Finanze certifica una firma per gli adempimenti fiscali, questa può non essere valida per un altro ministero, o per il Comune o per la Asl, anche se la certificazione è stata compiuta con la piena osservanza di tutte le regole. E ciò contrasta con l'articolo 2 del DPR 513/97, che vuole il documento digitale valido e rilevante ad ogni effetto di legge, se formato secondo le norme generali e specifiche.
In conseguenza di questa disposizione, un soggetto che volesse gestire tutti i rapporti con la Pubblica amministrazione attraverso documenti digitali (e la cosa dovrebbe essere possibile nel giro di pochi anni, secondo il DPR 513/97) dovrebbe munirsi di una coppia di chiavi per ciascun ente con il quale volesse o dovesse trattare. Il che significherebbe anche il doversi recare di persona presso tutti gli uffici interessati, con il dispendio di tempo e lo spreco di risorse che si vorrebbe evitare proprio con l'adozione del documento digitale. Senza contare la complessità della gestione organizzativa e tecnica di un "portachiavi" tanto affollato, oltre al rischio che deriva dall'impossibilità di ricordare a memoria le password corrispondenti alle diverse chiavi.
A tutto questo si aggiunge un'altra complicazione. L'articolo V.1 delle regole tecniche stabilisce che "*Le Pubbliche amministrazioni, anche in forma associata, possono istituire, con riferimento al proprio ordinamento, un servizio di certificazione delle chiavi pubbliche dei dipendenti e dei cittadini, utilizzate ai soli fini amministrativi, senza l'iscrizione dell'elenco pubblico di cui all'art. 8, comma 3, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513*".
Insomma, il cittadino che vorrà assumere una "identità digitale" a tutti gli effetti, dovrà rivolgersi a un



Generazione e verifica della firma digitale. La firma digitale si genera applicando la propria chiave privata all'impronta del testo.



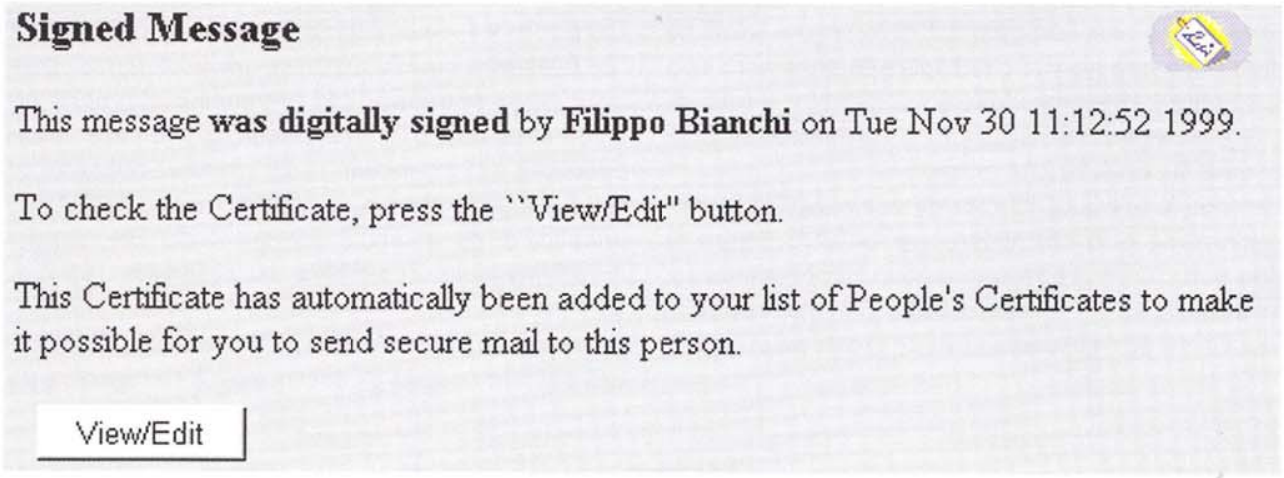
Certificato della chiave pubblica. Ecco come appare un certificato della GlobalSign in Explorer.

certificatore iscritto all'albo, mentre i certificati rilasciati da una Pubblica amministrazione avranno un'efficacia limitata a quella singola amministrazione e, eventualmente, alle altre che abbiano stipulato accordi di mutuo riconoscimento con la prima.

E' difficile capire il senso di questo complesso di norme. Che le Pubbliche amministrazioni possano certificare, per il solo uso interno, le firme dei propri dipendenti, appare naturale. Un po' meno naturale è la facoltà del mutuo riconoscimento, invece dell'obbligo.

Ma perché estendere la potestà certificatoria delle amministrazioni a soggetti esterni, se questi certificati non possono avere gli effetti previsti dall'articolo 2 del regolamento generale?

Al di là di questo problema, che però non diminuisce il valore innovativo dell'introduzione del documento digitale, resta la complessità e la rigidità delle regole tecniche per la certificazione, che forse sono necessarie per conciliare la certezza tecnica e la certezza giuridica del documento digita-



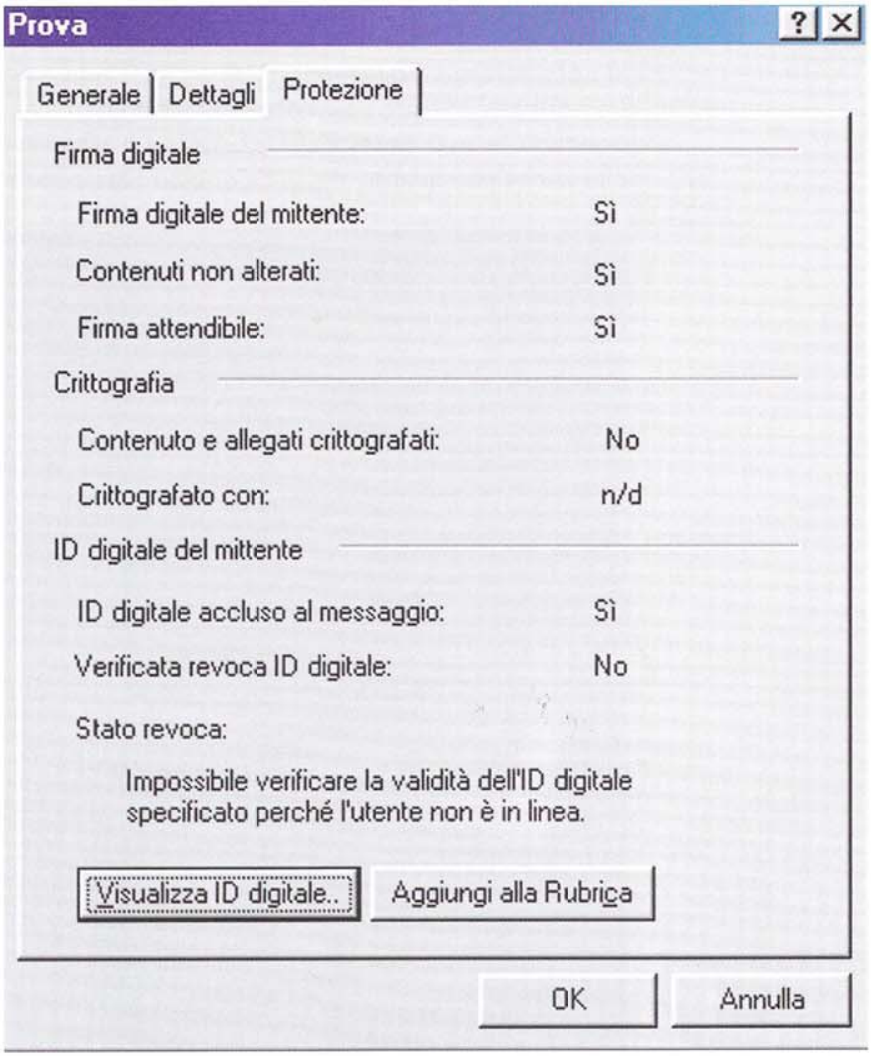
La firma digitale "rivelata". Così Netscape ci dice "chi è" il firmatario del messaggio.

L'essenziale del certificato. Lo stesso certificato visualizzato in Netscape.

Controllo del certificato. In questo modo Netscape ci informa che il certificato è valido.

le nell'ottica della Pubblica amministrazione e degli atti pubblici in particolare, ma si scontrano con le esigenze di rapidità e di semplificazione nei rapporti tra privati e soprattutto nel commercio elettronico.
Le prime positive esperienze in questo settore dimostrano che non sono necessarie tante formalità e tante precauzioni per la sicurezza delle transazioni telematiche, anche in considerazione del loro valore, generalmente esiguo. Quindi è facile prevedere che i soggetti interessati al commercio elettronico continueranno sulla strada, già intrapresa con buoni risultati, dell'autenticazione diretta degli utenti attraverso i controlli sulle carte di credito e altre precauzioni relativamente semplici. Infatti le estenuanti procedure della firma digitale "valida e rilevante ad ogni effetto di legge" finirebbero col frenare, invece che favorire, la diffusione delle transazioni telematiche.
Dunque quella che si profila non è la convergenza, ma la "divergenza" tra lo sviluppo del commercio elettronico e l'evoluzione telematica della Pubblica amministrazione. Tutto ciò offusca in parte la prospettiva della nascita dei "cittadini telematici" che le prime norme sul documento informatico avevano fatto sognare.
Da ultimo una semplice domanda: come si applicherà il bollo ai documenti informatici, nei casi in cui l'attuale ordinamento lo prevede (per esempio, sulle ricevute dell'affitto di un appartamento)? Si potrebbero escogitare diversi espedienti tecnici per un bollo "virtuale", ma poi come si farebbe a controllare l'assolvimento dell'obbligo? Forse autorizzando la Guardia di Finanza a curiosare in tutti i pc dei cittadini o a intercettare "a campione" i messaggi posta elettronica?
In ultima analisi la risposta è semplice come la domanda: esonerando dall'imposta di bollo i documenti digitali considerando i consistenti risparmi nei costi amministrativi che possono essere determinati dalla diminuzione dell'uso della carta. Ma la norma è scomparsa dalla versione definitiva del provvedimento. E non perché l'Autorità abbia cambiato idea, ma probabilmente perché per l'abolizione del bollo occorre una legge. Il primo testo era appunto un disegno di legge, che quindi avrebbe potuto dettare una norma ad hoc, ma poi è diventato un regolamento, che non può modificare una legge.
E' dunque opportuno che si intervenga con una disposizione di buon senso, che non costa nulla.

Francesco Lanorte



Verifica dell'autenticità. La finestra con il riassunto delle informazioni sul documento informatico (Explorer).