Firme digitali

Dall'Aprile del 1999 la "firma elettronica"[i] ha lo stesso valore giuridico di una firma manoscritta. Lo hanno deciso i ministri delle telecomunicazioni dell'Ue, riuniti a Lussemburgo, che hanno approvato all'unanimità la norma comunitaria che regola le transazioni nazionali e transnazionali via autostrade informatiche. All'approvazione della direttiva, già discussa lo scorso novembre dai ministri dell'Ue, mancava l'accordo su questo importante punto volto a garantire la sicurezza delle transazioni. Ora sarà possibile utilizzare le reti di telecomunicazione per ogni forma di "commercio elettronico" e anche per gli scambi delle amministrazioni pubbliche tra loro e con i cittadini e con operatori economici nel campo degli appalti pubblici, ad esempio, del fisco, della sicurezza sociale, della sanità e della giustizia. Ogni transazione su rete sarà ora autorizzata se si riusciranno a fornire le garanzie legali richieste dalla norma Ue. Le tecnologie che permetteranno di dare tali garanzie dipenderanno dai singoli paesi e vengono indicate nel documento approvato oggi che prevede una serie di sistemi di verifica dell'autenticità della 'firma. I fornitori di servizi possono competere liberamente tra loro purché offrano le dovute garanzie di fiducia, sicurezza e qualità.

Che cos'è il dispositivo di firma

L'articolo 1 del DPR 8 febbraio 1999 (le "Regole tecniche") stabilisce che si intende

per "dispositivo di firma", 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.

Non c'è una definizione del "sistema di validazione", ma è chiaro che si tratta dell'insieme hardware-software utilizzato di volta in volta o per la generazione delle chiavi o per la generazione (e la verifica) della firma digitale.
Il dispositivo di firma è un "apparato elettronico", quindi una "cosa", al cui interno sono presenti almeno la chiave privata del titolare e il software necessario alla generazione delle firme. Come vedremo tra poco, questi due elementi sono necessari, ma non sufficienti, al ciclo completo della firma digitale.
Ma, in pratica, come si presenta (o si presenterà) un dispositivo di firma? Nella sua forma più comune è costituito da una *smart card* (carta intelligente), cioè da un tesserino di plastica delle dimensioni standard di una carta di credito, provvisto di un microprocessore e di una certa quantità di memoria: insomma, un microscopico computer.

Non è difficile immaginare che il dispositivo di firma possa assumere un aspetto diverso, per esempio quello di una *cryptobox*, una scatola da collegare al computer e contenente altri sistemi di sicurezza.
Inoltre è ipotizzabile che possano essere utilizzate[ii] come dispositivo di firma anche carte a microprocessore la cui funzione principale è diversa, per esempio le future carte di identità digitali o quelle (già oggi diffusissime) dei telefoni cellulari.

La caratteristica fondamentale del dispositivo di firma consiste nel fatto che esso deve essere "programmabile solo all'origine"[1]. Questo significa che nel dispositivo di firma devono essere inserite, all'atto della fabbricazione o dell'inizializzazione, delle informazioni che non possono essere modificate successivamente.

L'indelebilità è ottenuta brutalmente con procedure fisiche, come la distruzione dei circuiti che consentono la scrittura in determinate aree di memoria, sicché non c'è nessun sistema per alterare i valori registrati nella fase di preparazione del dispositivo.

Questo è il primo e fondamentale meccanismo di sicurezza delle carte a microprocessore, che rende virtualmente impossibile la loro "clonazione": se ogni carta esce dalla fabbrica con inciso indelebilmente un numero di matricola, non sarà mai possibile avere due carte completamente uguali.

Se poi la correlazione tra il numero della carta e l'identità del titolare è asseverata dalla firma digitale dell'ente che emette la carta stessa, c'è anche la possibilità di verificare (attraverso la chiave pubblica dell'ente), la titolarità del dispositivo. Per inciso, questo è il principio della futura carta di identità digitale.

Infine è importante soffermarsi sull'indicazione che la chiave privata deve essere conservata "in modo protetto" nel dispositivo di firma. La protezione della chiave privata ha due aspetti differenti: il primo è che la chiave stessa non può essere attivata, per apporre una firma digitale, senza il superamento di un "blocco", costituito da una password o da un'altra procedura di identificazione del titolare; il

[1] prova2

secondo è che della chiave stessa non deve restare alcuna traccia all'interno del sistema di validazione usato per la firma.

L'importanza del dispositivo di firma

Il citato articolo 1 delle Regole tecniche indica la conservazione protetta della chiave privata e la procedura di firma come requisiti minimi del dispositivo. In realtà esso contiene anche altri componenti essenziali, elencati dall'articolo 26 (personalizzazione del dispositivo di firma):

- i dati identificativi del titolare presso il certificatore;
- il certificato rilasciato al titolare (che deve essere allegato alla firma)
- i certificati relativi alle chiavi di certificazione del certificatore.

Inoltre di solito il dispositivo contiene il software per la generazione della coppia di chiavi, che deve avvenire all'interno del dispositivo stesso nel caso che venga compiuta direttamente dal titolare. Se invece la generazione è compiuta da un altro soggetto (in linea di principio, il certificatore), essa può farsi anche al di fuori del dispositivo, ma in particolari condizioni di sicurezza.

In pratica ci sono due possibili schemi di generazione della coppia di chiavi:
1. il titolare si procura il dispositivo di firma, genera le chiavi e ne invia una (la chiave pubblica) al certificatore;

2. il certificatore genera le chiavi e consegna al titolare il dispositivo di firma contenente la chiave privata.

Il senso di tutte queste disposizioni è chiaro: la chiave privata deve essere protetta contro qualsiasi rischio di presa di conoscenza da parte di terzi, compreso lo stesso certificatore, sul cui sistema non deve restare la minima traccia della chiave stessa, nel caso in cui egli provveda alla generazione della coppia.

Il motivo che ha spinto il legislatore italiano a rendere obbligatorio l'uso del dispositivo di firma è chiaro: con la chiave privata del titolare stabilmente custodita all'interno di un qualsiasi PC, è abbastanza facile per un malintenzionato approfittare di un momento in cui il titolare si allontana dalla postazione e sostituirsi a lui per apporre firme apocrife, per di più difficilissime da identificare come tali. Questo rischio è particolarmente diffuso negli uffici pubblici, dove spesso i computer restano per lungo tempo accesi in assenza del titolare.
Invece, se il titolare può portare con sé la chiave, il livello di sicurezza del sistema è molto più alto. C'è anche un vantaggio pratico: con la chiave privata registrata su un dispositivo portatile, il titolare può sottoscrivere documenti dovunque vada (per esempio, nello studio di un notaio).

Va detto però che, almeno nelle soluzioni oggi disponibili, non è sufficiente inserire il dispositivo di firma nel lettore incorporato o collegato a un PC per attivare tutte le operazioni. Nella macchina deve infatti essere presente anche il software necessario

per il collegamento "protetto" con il certificatore, che poi è il "sistema di comunicazioni sicuro".

L'autenticazione in pratica

Dobbiamo ora cercare di immaginare come avverrà l'autenticazione della firma digitale.

L'interessato si recherà dal pubblico ufficiale (tipicamente un notaio) con il documento già predisposto su un dischetto o su un CD scrivibile, oppure sarà il pubblico ufficiale a scriverlo sul proprio PC. Quindi il comparente inserirà nell'apposito lettore il proprio dispositivo di firma e genererà la firma.
A questo punto il pubblico ufficiale, dopo aver compiuto i prescritti accertamenti sul documento, verificherà la chiave pubblica del firmatario collegandosi al certificatore, aggiungerà al documento l'attestazione di autenticità, inserirà il proprio dispositivo e quindi genererà la propria firma, la cui impronta sarà calcolata sull'insieme costituito dalla scrittura, dalla firma del sottoscrittore e dalla attestazione notarile di autenticità.

il documento informatico, di regola, è un documento "in chiaro", il cui contenuto è leggibile da chiunque, e non "criptato".Se mai la cifratura può farsi successivamente, nel caso in cui il documento contenga informazioni riservate, e in questo caso si utilizzerà la chiave pubblica del destinatario oppure un cifrario simmetrico.

Il progetto CAFE

Introduzione

CAFE (*Conditional Access For Europe*) è un progetto che si inserisce all'interno del programma ESPRIT della Comunità Europea.
Il suo obiettivo è quello di sviluppare sistemi innovativi per accesso condizionato, cioè sistemi digitali che amministrano alcuni diritti dei propri utenti. Tali diritti possono essere forme digitali di passaporto, accesso confidenziale a dati, ingresso in edifici, o, esempio importante, sistemi di pagamento digitali.

Dispositivi

Il dispositivo base per CAFE è il **borsellino elettronico**. Si tratta di un piccolo computer portatile, simile ad un calcolatore tascabile o ad un PDA (*Personal Digital Assistant*). È dotato di batterie, tastiera e display propri ed è in grado di comunicare con altri dispositivi, tramite canale ad **infrarossi**.
Ogni utente del sistema possiede e sfrutta il proprio borsello, che amministra i suoi diritti e garantisce la sua sicurezza.
La versione di lusso può combinare le funzioni CAFE con quelle di un PDA, di un telefono mobile o di un computer portatile. La versione base può semplicemente implementare le funzioni CAFE, e la tastiera contenere solo pochi tasti.

Funzionalità di base

Il sistema CAFE è un sistema di pagamento di tipo pre-paid o off-line(senza ricorrere ad una terza parte durante la transazione tra compratore e venditore). Il sistema base è fondamentalmente pensato per effettuare pagamenti dal borsello ad un terminale di un qualsiasi punto vendita. Il beneficiario del pagamento (cioè il venditore) deve depositare il denaro elettronico presso un acquirente, prima di poterlo usare per pagamenti propri.
Eventuali prelievi di denaro elettronico (cioè caricamento di denaro elettronico dentro il proprio borsello) rappresentano transazioni on-line (coinvolgendo un server di autenticazione e autorizzazione). Possono essere eseguiti da sportelli pubblici tipo ATM o da altri tipi di terminali base.

Tecniche

Questione molto importante è la seguente: come conciliare la sicurezza del fornitore di denaro elettronico e pagamenti off-line? Dopo tutto, il denaro elettronico è solo una stringa di bit. Dunque, anche se un sistema è sicuro nel senso che gli utenti non possono produrre nuovo denaro, cioè una nuova stringa di bit valida, chiunque abbia visto tale stringa potrà riprodurla nel tentativo di spendere la stessa moneta, anche più di una volta.

Il sistema CAFE propone la seguente soluzione:

- È impossibile spendere due volte lo stesso denaro finché un certo tipo di dispositivo anti-frode è funzionante.

- Anche nel caso in cui la protezione verso intrusioni sia superata, l'utente che spende lo stesso denaro elettronico più di una volta è identificato e la frode gli potrà essere contestata.
- Non è richiesto all'utente di riporre fiducia in tale dispositivo per garantire la propria sicurezza e la propria privacy. Il dispositivo, il cui interno è inaccessibile all'utente, è infatti distribuito dal fornitore di denaro elettronico e protegge la sicurezza del fornitore stesso.

Una soluzione standard: la firma digitale

Una misura di sicurezza standard che deve essere applicata è la **firma digitale**. Tale tecnica è indispensabile per sistemi con sicurezza multi-parte.

È importante notare che, in un sistema di pagamento, ogni messaggio con un qualche valore legale deve essere firmato per acquistare certezza legale. In particolare, il borsello deve inviare un ordine firmato per prelevare denaro dal fornitore, e chi riceve pagamenti deve possedere una ricevuta firmata per depositare denaro. Inoltre, l'inizializzazione del borsello deve garantire che i segreti utilizzati per creare la firma non siano noti a nessuna altra parte. La firma digitale è usata soprattutto per trasferimenti off-line. In questo caso l'autenticazione off-line non comporta alcun problema, dal momento che il venditore può facilmente verificare la firma del compratore (e può confrontare il certificato del compratore con una propria "lista nera" di certificati, se necessario). L'autorizzazione richiede comunque o una connessione in linea o la presenza di hardware affidabile presso il compratore.

Per i trasferimento off-line, oltre ad essere utilizzato nel sistema *CAFE*, è sfruttata anche nel *Express;*Mentre per i trasferimenti on-line è usata da Ecash, NetCash, CyberCash e SET.

[i] prova
[ii] prova