

TECNOLOGIA E SICUREZZA DELLE SMART CARD

I DATI IN TASCA

È difficile oggi trovare un portafoglio che non contenga almeno una scheda telefonica e un paio di carte di credito, e magari la carta di fidelizzazione del supermercato preferito, la scheda per la raccolta punti del distributore di benzina, una Viacard, ... Sia pure con tecnologie diverse, tutte queste schede hanno la funzione di contenere dati che all'occasione possono essere letti o modificati. Si tratta ancora, in genere, di pochi dati elementari, ma sul piano tecnologico è già possibile fornire schede in grado di contenere una quantità di dati enormemente più alta, fino all'intera storia clinica, corredata di radiografie o tracciati elettrocardiografici, di un paziente a rischio. Se poi la carta non è un semplice supporto di memorizzazione, ma è dotata di capacità di elaborazione proprie (in questo caso si parla di "carte intelligenti", o "smart card"), le prospettive di utilizzo che si aprono diventano ancora più interessanti. Tra non molto potremmo quindi circolare portandoci in tasca tutti i dati relativi al nostro status di cittadini (carta di identità elettronica), alla nostra situazione economica (carte bancarie), alla nostra salute (carte sanitarie). Questi dati possono poi essere letti, modificati, trasmessi a distanza attraverso le reti telematiche, o elaborati direttamente sulla carta se questa ha le capacità per farlo.

Si possono facilmente immaginare, ed in parte si possono già vedere in atto, i profondi cambiamenti, la vera e propria rivoluzione, che verranno prodotti dall'uso generalizzato di questi strumenti soprattutto nei settori bancario, commerciale, delle comunicazioni e della salute. Ad esempio, diciotto milioni di tedeschi hanno ricevuto una smart card che riporta i dati amministrativi relativi alla assistenza sanitaria. In Francia, i pazienti in dialisi possono viaggiare per piacere o per lavoro grazie alla standardizzazione del software dei centri di dialisi e all'uso di smart cards.

DALLE SCHEDE MAGNETICHE ALLE "CARTE INTELLIGENTI": LE POSSIBILI SCELTE TECNOLOGICHE

La tecnologia oggi prevalente è ancora quella della banda magnetica, ma ci si sta rapidamente spostando verso carte a microprocessore, più costose ma che offrono diversi vantaggi. In ogni caso, la scelta della tecnologia dipende dal tipo di applicazione che si vuole sviluppare. In particolare, i punti da tener presenti nella scelta sono i seguenti:

1. Quanta memoria occorre ?
2. Che livello di sicurezza occorre garantire ?
3. Con che frequenza è necessario aggiornare i dati ?
4. Tutti i dati devono essere residenti sulla carta o si vuole mantenere un database centralizzato ?

Vediamo allora le principali scelte tecnologiche disponibili.

a) Schede a banda magnetica

Sono rettangoli di plastica su cui è posta una sottile striscia di materiale magnetizzabile. La diffusione delle schede a banda magnetica è dovuta essenzialmente alla loro semplicità di uso e al basso costo sia della scheda che dei lettori. Hanno però forti limitazioni per quanto riguarda la capacità di memorizzazione (che non supera in genere i 75 caratteri) e la sicurezza e protezione dei dati, poichè sono facilmente leggibili e falsificabili da persone non autorizzate, ed inoltre i dati in esse contenuti possono essere facilmente danneggiati o resi illeggibili anche semplicemente dalla chiusura magnetica di una borsetta. Naturalmente, le schede magnetiche non possono elaborare i dati, ma possono attivare un collegamento con un elaboratore remoto su cui risiede un database centralizzato. Anche se per alcune applicazioni (identificazione, controllo degli accessi, schede telefoniche) la scheda magnetica può essere tuttora una scelta adeguata, per applicazioni più complesse ha evidenziato problemi che

impongono il passaggio a tecnologie più avanzate. In particolare, per le carte di credito a banda magnetica è difficile limitare le frodi, data l'intrinseca carenza di sicurezza; inoltre, questa tecnologia non è in grado di soddisfare richieste di multifunzionalità e di interoperabilità tra applicazioni simili in diverse nazioni o tra applicazioni diverse.

b) Schede a chip di memoria

In questo caso il supporto di memoria è costituito da un circuito integrato (chip) che non ha però capacità di elaborazione, ma è semplicemente una "memoria programmabile non volatile cancellabile elettricamente" (EEPROM). La capacità di memoria può andare dai 1024 bit ai 65536 bit, e vi è la possibilità di modificare i dati fino a 10000 volte. Il chip è dotato di connessioni fisiche per il collegamento al lettore e, attraverso di esso, ad un computer esterno. L'ISO (International Standards Organization) ha definito uno standard preciso per la posizione e le funzioni delle connessioni, che tutti i produttori devono rispettare.

Pur essendo più difficile da falsificare rispetto alla banda magnetica, il chip di memoria non garantisce la confidenzialità dei dati, che possono essere letti anche da estranei. Esistono però versioni, leggermente più costose, in cui il chip contiene un campo codificato in hardware e non modificabile che permette di usare una password per controllare l'accesso. Attualmente l'uso di queste schede si sta diffondendo per tutte quelle applicazioni che richiedono di memorizzare una certa quantità di dati direttamente sulla scheda, senza che sia necessario mantenere un database centrale: schede telefoniche prepagate, programmi di manutenzione di autovetture, programmi di fidelizzazione di supermercati o compagnie petrolifere, ma anche registrazione della carriera scolastica di uno studente.

c) Carte ottiche

Si tratta di schede su cui è possibile memorizzare grandi quantità di informazioni attraverso l'uso di un laser, come per i compact disk. Il loro punto di forza è la capacità di memorizzazione, che può arrivare a parecchi milioni di caratteri, equivalenti a un libro di qualche migliaio di pagine, o ad una ottantina di immagini mediche (radiografie, TAC, risonanza magnetica). Anche dal punto di vista della sicurezza dei dati la carta ottica offre numerosi vantaggi. La sua memoria è non cancellabile e non volati-

le, non è danneggiata da campi magnetici o elettrostatici, può resistere anche a temperature piuttosto alte. Inoltre, ha spazio sufficiente per memorizzare codici personali di identificazione (PIN), dati biografici, fotografia, firma, impronte digitali e vocali del titolare, rendendo pressochè impossibile l'uso non autorizzato. Nonostante questi aspetti positivi, l'uso delle carte ottiche è limitato dall'alto costo soprattutto dei lettori, dalla necessità di mantenere sempre assolutamente pulita la superficie ottica e dal fatto che le informazioni non vengono mai cancellate fisicamente dal supporto, per cui non si prestano ad applicazioni in cui l'aggiornamento dei dati è molto frequente.

d) Carte intelligenti a contatto

Una "carta intelligente" è una scheda che rispetta il formato standard definito dalla ISO e contiene un microprocessore (CPU, Central Processing Unit) che ha capacità di elaborazione propria e può interagire, inviando o ricevendo dati, con un altro processore (lettore o host). Inoltre, il chip contiene tre diversi tipi di memoria:

- ROM, memoria di sola lettura, che viene programmata durante la produzione della carta e non può essere alterata; di solito contiene il sistema operativo che controlla la CPU.
- RAM, memoria volatile, che si cancella quando la scheda è estratta dal lettore.
- EEPROM, non volatile e riscrivibile fino a 10000 volte.

Sia pure in piccolo, si tratta di un vero e proprio calcolatore, della dimensione e dello spessore di una carta di credito, che può eseguire ad esempio algoritmi crittografici. Il livello di sicurezza è quindi molto più alto che nei casi precedenti, anche perchè il microprocessore è difficile, se non impossibile, da copiare, e inoltre la scheda può avere in memoria codici identificativi senza la cui conoscenza è impossibile usarla.

I parametri che caratterizzano le CPU usate per le carte intelligenti sono gli stessi dei microprocessori per i personal computer: la lunghezza delle parole (attualmente in genere 8 o 16 bit) e la dimensione dei vari tipi di memoria. L'applicazione di maggiore importanza è per ora quella dei servizi GSM per la telefonia cellulare, ma alcune carte di credito stanno adottando questa tecnologia.

e. Carte intelligenti senza contatto

Anche le carte intelligenti senza contatto, come le precedenti, sono dotate di un microprocessore con memorie di diverso tipo, ma non richiedono di essere fisicamente inserite in un lettore per scambiare dati con l'esterno: lo scambio avviene attraverso onde elettromagnetiche. L'assenza di contatti metallici rende la carta molto più robusta e longeva rispetto alle carte a contatto. È ideale per applicazioni come il pagamento del biglietto dell'autobus o del parcheggio, in cui si richiede una esecuzione molto rapida delle transazioni.

f. La Java card

L'allargarsi del ventaglio di possibili applicazioni delle carte intelligenti, dalla telefonia GSM ai servizi di credito/debito, al borsellino elettronico, alla carta sanitaria e così via, ha portato in primo piano l'opportunità di disporre su un'unica carta di diverse applicazioni. Java Card è una architettura che si propone di andare in questa direzione.

Java è un linguaggio di programmazione sviluppato da Sun Microsystems che si sta imponendo come standard per le applicazioni di rete. I suoi punti di forza sono la indipendenza dalla piattaforma hardware, per cui programmi sviluppati in Java possono essere eseguiti su qualunque tipo di hardware, e la facilità di integrazione con i browser www, cioè con i programmi che servono per navigare in Internet.

L'elemento chiave per eseguire i programmi Java è la Java Virtual Machine, un interprete che risiede sulla macchina che esegue i programmi, che possono però essere scaricati via rete. Alcuni produttori di smart cards si sono raggruppati nel Java Card Forum, con l'obiettivo di definire gli standard per una Applications Programming Interface (API), cioè una libreria di routines Java, per schede a microprocessore. Le applicazioni sviluppate in Java secondo questi standard sono indipendenti dal particolare microprocessore o dal particolare sistema operativo, e possono quindi essere utilizzate anche su carte di produttori diversi, dotate di una Java Virtual Machine. Visa ha intuito il potenziale innovativo di questa soluzione, ed è andata oltre, proponendo una Open Platform Specification per le Java Card che tiene conto delle esigenze di sicurezza delle applicazioni finanziarie.

Dopo tre anni di lavoro, le Java Card stanno ormai entrando sul mercato e rappresenteranno sicuramente una ulteriore spinta per l'uso generalizzato delle

carte a microprocessore in diversi settori.

IL PROBLEMA DELLA SICUREZZA E DELLA PROTEZIONE DEI DATI

Uno dei principali problemi legati all'uso delle schede, qualunque sia la tecnologia usata o l'applicazione specifica, riguarda la protezione dei dati e delle transazioni dal punto di vista della confidenzialità, della integrità e della sicurezza.

Infatti i dati sono di proprietà del possessore della carta, ed è fondamentale garantire che la carta non possa essere usata da un altro soggetto, per leggere o modificare i dati o per eseguire transazioni di qualsiasi tipo, senza la sua autorizzazione. D'altro lato, nelle applicazioni di maggior rilievo la carta viene usata dal possessore per interagire con il sistema informativo di un terzo soggetto (banca, sistema sanitario e così via), ed occorre per quanto possibile eliminare la possibilità di frodi. Il problema è ancor più complesso quando sulla carta risiedono diverse applicazioni, o quando vi sono frequenti trasferimenti o modifiche di dati.

La prima forma di protezione consiste nella introduzione di una password o di un codice personale che deve essere inserito per abilitare le operazioni della carta. Nel caso in cui la carta supporti più applicazioni, è possibile con le smart card più recenti inserire password diverse per le diverse applicazioni. Per evitare che la password possa essere scoperta per prove ed errori, dopo alcuni tentativi errati la carta viene trattenuta dal lettore.

Forme di protezione più sofisticate passano attraverso l'uso di complessi algoritmi crittografici che codificano tutte le informazioni in un formato che non può essere letto senza conoscere la chiave di lettura. Questi algoritmi possono essere usati anche la verifica, da parte del sistema centrale o del lettore, che la carta non sia stata falsificata (autenticazione della carta). Inoltre, garantiscono la confidenzialità dei dati che, anche qualora fossero letti da estranei a seguito ad esempio del furto o dello smarrimento della carta, non potrebbero essere decifrati.

