Ugo Chirico

Programmazione delle Smart Card

Seconda Edizione

Listati, esempi di codice e aggiornamenti al testo sono disponibili sul sito dell'autore all'indirizzo: http://www.ugochirico.com

ISBN: 978-1-291-45932-6

INDICE

Introduzione

Negli ultimi vent'anni le tecnologie basate su smart card sono state ampiamente sfruttate sia dal mondo dell'informatica sia nell'ambito delle telecomunicazioni, in un panorama tecnologico che vede internet e gli smartphone come potentissimi e ormai indispensabili strumenti di comunicazione.

Oggi tali tecnologie sono ormai mature ed affidabili e hanno stimolato una sostanziale rivoluzione dei modelli di comportamento inerenti l'accesso, l'uso e la gestione delle informazioni, rivoluzione che oggi si sta attuando attraverso la completa riformulazione dei paradigmi di sicurezza preposti alla protezione delle informazioni riservate, alla protezione della privacy, all'autenticazione sicura dei soggetti e, più in generale, alla sicurezza dei sistemi informatici.

Il valore aggiunto offerto dalle smart card, che corrisponde altresì al loro principale pregio, sta sostanzialmente nella possibilità di:

1) memorizzare informazioni riservate in maniera estremamente sicura in un dispositivo elettronico che può essere facilmente tenuto nel portafogli come se fosse una normale carta di credito;

2) eseguire all'interno del microchip i principali algoritmi crittografici preposti all'identificazione e all'autenticazione degli individui titolari delle smart card e alla protezione di informazioni riservate.

Tali caratteristiche hanno consentito di realizzare svariate applicazioni sia nell'ambito della sicurezza informatica ed in particolare nell'identificazione automatica e certificata degli individui, sia in altri ambiti quali telecomunicazioni mobili, sistemi di pagamento, *PayTV*, commercio elettronico, sistemi bancari, ecc. Basti pensare alle SIM card (in ambito GSM/UMTS), alle Carte di credito a microchip, alla Carta d'Identità Elettronica, alla Carta Nazionale Servizi, ai vari badge aziendali, alle carte prepagate e di raccolta punti, ecc. Queste sono solo alcune

delle possibili applicazioni realizzate con la smart card che è ormai diventando un oggetto di uso comune indispensabile nella vita quotidiana.

Sebbene la tecnologia sia ormai consolidata, le numerose esigenze emerse dai vari campi di applicazione nei quali le smart card sono state utilizzate e le differenti caratteristiche dei sistemi e delle piattaforme di elaborazione, hanno portato alla definizione di numerosi standard e/o specifiche tecniche che mirano a definire una piattaforma comune che consenta l'interoperabilità tra applicazioni e smart card di diverso tipo e fabbricazione. In un panorama tecnologico così ricco di specifiche tecniche e di paradigmi di programmazione pressoché equivalenti, risulta difficile capire le differenze, quasi filosofiche, tra le varie proposte ed è quindi molto faticoso orientarsi verso la scelta dello standard o dell'insieme di specifiche tecniche che meglio soddisfano le esigenze di una particolare applicazione.

Lo scopo di questo libro è offrire una guida chiara, ma allo stesso tempo completa ed esauriente, a tutte le tecnologie, gli standard e le specifiche tecniche legate alle smart card, che dia in primo luogo una visione generale ad alto livello dello scenario tecnologico e proponga, in secondo luogo, un approfondimento tecnico sulle architetture, i paradigmi di programmazione e le API relative a ciascuno standard e/o specifica tecnica, rivolto principalmente ai programmatori, agli analisti e ai progettisti.

La prima parte del libro introduce la tecnologia legata alle smart card, i concetti generali ed alcuni *case study* ed è rivolta anche ai lettori che pur non avendo una preparazione spiccatamente tecnica vogliono conoscere, capire e sapersi orientare nel mondo delle smart card.

La seconda parte, invece, si propone come una guida alle diverse specifiche tecniche e paradigmi di programmazione proposti in ambito smart card. Ciascun capitolo della seconda parte tratta nei primi paragrafi le concezioni generali della tecnologia in esame, ed è quindi accessibile anche ai lettori non tipicamente tecnici, mentre nei restanti paragrafi approfondisce gli aspetti spiccatamente tecnici relativi alla programmazione e alla realizzazione di applicazioni con smart card e, pertanto, richiede una minima conoscenza delle basi della programmazione ed in particolare di C/C++, C# e Visual Basic .NET per i capitoli relativi alle specifiche PC/SC e PKCS#11, Java per i capitoli dedicati alla piattaforma JavaCard e all'*OpenCard Framework* e infine Visual Basic 6 per alcuni paragrafi del capitolo relativo alle specifiche PC/SC

1

La Smart Card

Bisogna avere in sé il caos per partorire una stella che danza.
Nietzsche

La smart card è un dispositivo hardware delle dimensioni di una carta di credito capace di memorizzare ed elaborare informazioni mediante un circuito integrato incapsulato in un supporto di plastica (**Figura 1.1**)

Grazie alle dimensioni ridotte, la smart card può essere facilmente portata con sé da un individuo (tipicamente nel portafogli). Considerando anche la sua capacità di memorizzare informazioni in maniera estremamente sicura e inviolabile e la possibilità di elaborare dati al suo interno, la smart card si propone in primo luogo come strumento informatico di identificazione sicura e certificata degli individui; in secondo luogo come dispositivo di elaborazione a supporto della crittografia in grado di memorizzare e proteggere le chiavi crittografiche private e di eseguire i principali algoritmi crittografici; infine, come dispositivo multi-applicazione e/o multi-servizio che può quindi ospitare al suo interno i dati relativi ad applicazioni e servizi di diverso tipo.

Figura 1.1. Alcune smart card in commercio

1.1 La storia

L'idea di incapsulare un circuito integrato in un supporto di plastica fu introdotta nel 1968 da due inventori tedeschi: Jürgen Dethloff e Helmut Grötrupp. Negli anni '70 furono registrati i primi brevetti da parte di diverse aziende e gruppi di ricerca, ma solo alle soglie degli anni '80 Bull (allora CII-Honeywell-Bull) mise in commercio il primo prototipo di smart card e introdusse le smart card a microprocessore.

Le prime applicazioni con smart card furono realizzate in Francia e Germania all'inizio degli anni '80, dove le smart card furono adoperate come carte telefoniche prepagate e come carte bancarie di credito/debito ad alta sicurezza. Tali applicazioni mostrarono la grande capacita di resistenza ad attacchi e la considerevole flessibilità delle smart card e traghettarono la nuova e vincente tecnologia verso i recenti sviluppi in ambito GSM e Web.

Negli ultimi anni le nuove tecniche di miniaturizzazione, mediante le quali è stato possibile produrre microchip sempre più piccoli a costi sempre più bassi, hanno consentito di realizzare smart card più potenti dotate di coprocessore crittografico e di buone capacità di memoria a costi accessibili. Tale disponibilità ha avviato una fase di notevole e sorprendente sviluppo che è partita dall'implementazione delle SIM card in ambito GSM fino ad arrivare alla realizzazione della Carta d'Identità Elettronica e delle carte di credito "intelligenti".

1.2 Architettura HW/SW

La **Figura 1.2** mostra l'architettura hardware di un generico sistema di elaborazione che consente l'uso di smart card. Oltre a tastiera e mouse, al personal computer è collegato un terminale di lettura (a destra nella figura) detto tipicamente "lettore di smart card" che consente di comunicare con la smart card. La maggior parte dei lettori in commercio può essere collegata al PC tramite porta seriale o USB. Per i computer portatili sono anche

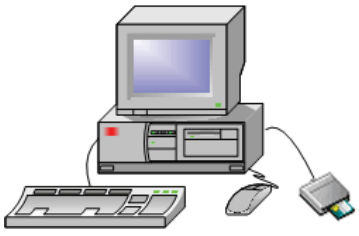

Figura 1.2 Sistema con lettore di smart card

disponibili lettori PCMCIA (solitamente più costosi). Esistono inoltre (ma sono meno diffusi) lettori collegati alla tastiera, o montati su floppy disk.

Le funzionalità tipiche di un lettore si smart card sono: fornire l'alimentazione e il segnale di clock al microchip della smart card e gestire il canale di I/O mediante il quale sono scambiati i dati digitali da e per la smart card.

Un'applicazione software con smart card consiste in un una applicazione in esecuzione sul computer che interagisce con la smart card mediante le funzionalità offerte dal circuito integrato. La **Figura 1.3** mostra l'architettura logica di un sistema software che dialoga con la smart card.

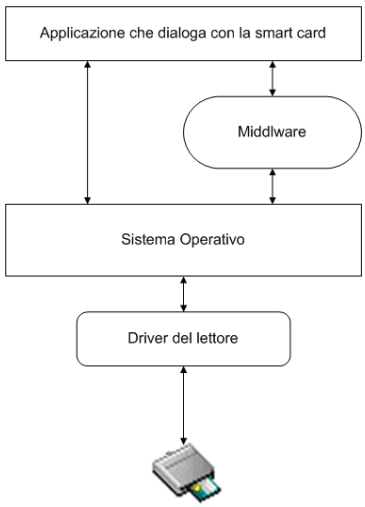

Figura 1.3 Architettura logica di un sistema con smart card

A partire dal basso, il lettore di smart card si interfaccia con il sistema operativo del computer attraverso un driver[1]. Il sistema operativo mette a disposizione un insieme di funzioni a basso livello per comunicare con il lettore che possono essere usate direttamente della applicazioni o possono essere mappate in un insieme di funzioni ad alto livello, implementate in un *middlware*, che fornisce pertanto un interfaccia di programmazione più semplice e flessibile per scrivere applicazioni.

---

[1] Per maggiori informazioni sull'installazione di un lettore di smart card su piattaforma Windows di veda: "*Step-by-Step Guide to Installing and Using a Smart Card Reader*", http://www.microsoft.com/WINDOWS2000/library/planning/security/smartcard.asp

1.3 La smart card a supporto della crittografia

La crittografia, sebbene fornisca delle tecniche estremamente eleganti e potenti per assicurare l'integrità e la riservatezza delle informazioni[2], presenta un punto debole che sta nella difficoltà di proteggere in maniera adeguata le chiavi private. Difatti, se una chiave privata adottata per cifrare un insieme di informazioni non è adeguatamente protetta (ad esempio è memorizzata sull'hard disk di un PC), un individuo malintenzionato potrebbe impossessarsene e quindi decifrare tutte le informazioni vanificando gli sforzi crittografici compiuti.

La smart card a microprocessore, grazie alle caratteristiche di protezione dei dati intrinseche del microchip e alla presenza di un coprocessore crittografico che gli consente di eseguire le principali funzioni crittografiche on-board, (senza quindi la necessità di esporre le chiavi private all'ambiente operativo delle applicazioni, nel quale potrebbero essere attaccate da programmi ostili) si propone come il mezzo adeguato a proteggere le chiavi private rilanciando la crittografia come supporto tecnologico di base per lo sviluppo di sistemi informatici sicuri e riproponendo, in maniera decisa, la firma digitale come un sicuro e insostituibile strumento per l'autenticazione e l'identificazione degli individui, per la verifica dell'integrità di insiemi di dati e per il non ripudio delle transazioni.

1.4 La smart card nelle procedure di autenticazione

Per le sue peculiarità, la smart card è fortemente usata nelle procedure di *Strong Authentication* come dispositivo di memorizzazione sicura delle credenziali utente. Tipicamente, tali credenziali sono rappresentate dalla coppia *username-password*, o, nei sistemi più avanzati basati su firma digitale, dalla coppia *chiave privata-certificato digitale*.

L'accesso alle credenziali è subordinato alla verifica di un PIN (*Personal Identification Number*) che il titolare della smart card è tenuto a conservare con cura e digitare durante la procedura di autenticazione quando richiesto. In seguito alla verifica positiva del PIN da parte della smart card, le credenziali utente vengono lette dalla procedura e usate per eseguire l'autenticazione. Nel primo caso la coppia *username-password* viene inviata al sistema che richiede l'autenticazione. Nel secondo

---

[2] Per un approfondimento sulla crittografia si veda: U. Chirico, *"La Crittografia*, MokaByte, Giugno '99, n. 31 (http://www.mokabyte.it/1999/06/crittografia.htm)