



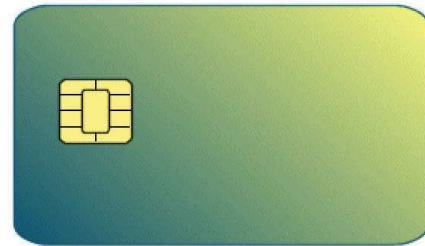
Programmazione delle SmartCard

Parte 1 - I Fondamenti:

Nozioni di base

Le Specifiche ISO 7816

Esempi d'uso con smart card virtuale



Ugo Chirico

Cryptware
advanced software

Ugo Chirico

Programmazione delle Smart Card

Parte 1 - I Fondamenti

Copyright © 2003-2009 by Ugo Chirico – <http://www.ugosweb.com>
All rights Reserved

Nessuna parte di questo libro può essere riprodotta o trasmessa in qualsiasi forma senza il consenso scritto dell'autore.

Tutti i diritti di traduzione, di riproduzione, di memorizzazione elettronica e di adattamento totale o parziale con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche, CD, siti internet) sono riservati per tutti i paesi.

I nomi e i marchi citati nel testo sono depositati o registrati dalle rispettive case produttrici.

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

Note sull'autore:



Ugo Chirico è laureato in Fisica Cibernetica all'Università di Napoli "Federico II" e attualmente ricopre il ruolo di Direttore della divisione Mobile Development di KeyVision (<http://www.key-vision.com>) ed è il titolare di Cryptware (<http://www.cryptware.it>).

Ha scritto numerosi articoli per le riviste "Computer Programming", "Dev" e "Mokabyte" ed è esperto di progettazione e sviluppo software in C/C++, C#, Java, VB, Prolog e LISP su piattaforme .NET, Windows, Linux, J2ME, Symbian,

Windows Mobile, iPhone e sistemi embedded. E' inoltre appassionato di Intelligenza Artificiale.

Il suo sito web personale è: <http://www.ugosweb.com>

INTRODUZIONE.....	4
LA SMART CARD.....	5
1.1 LA STORIA.....	5
1.2 ARCHITETTURA HW/SW DI UN SISTEMA BASATO SU SMART CARD.....	6
1.3 LA SMART CARD A SUPPORTO DELLA CRITTOGRAFIA	7
1.4 LA SMART CARD NELLE PROCEDURE DI AUTENTICAZIONE	7
1.5 LE APPLICAZIONI.....	8
1.6 GLI STANDARD	9
1.7 CASE STUDY	10
1.7.1 <i>Corporate Card</i>	10
1.7.2 <i>Il progetto E-Poll</i>	12
1.7.3 <i>Carta Multiservizi della Difesa</i>	12
FONDAMENTI TECNOLOGICI.....	14
2.1 LA SMART CARD	14
2.1.1 <i>Memory Card</i>	14
2.1.2 <i>Microprocessor Card</i>	15
2.1.3 <i>Smart Card Contact, Contactless e Dual Interface</i>	15
2.1.4 <i>Token USB</i>	16
2.2 ARCHITETTURA DEL MICROCHIP	16
2.3 PRODUZIONE DELLE SMART CARD.....	18
2.4 IL SISTEMA OPERATIVO	18
2.5 PROTEZIONE DEI DATI SULLA SMART CARD.....	18
2.6 QUALE SMART CARD ?	19
LO STANDARD ISO 7816.....	20
3.1 LE SPECIFICHE TECNICHE STANDARD	20
3.2 CARATTERISTICHE FISICHE ED ELETTRICHE	21
3.3 L'ATR.....	22
3.4 PROTOCOLLI DI TRASMISSIONE	22
3.4.1 <i>Protocollo T = 0</i>	23
3.4.2 <i>Protocollo T = 1</i>	23
3.5 STRUTTURA E FORMATO DEI DATI MEMORIZZATI NELLA EEPROM.....	23
3.5.1 <i>File System</i>	23
3.5.2 <i>Tipologia e formato dei file</i>	24
3.5.3 <i>Permessi di accesso ai file</i>	25
3.5.4 <i>Secure Messaging</i>	25
3.6 L'INSIEME DEI COMANDI.....	26
3.6.1 <i>Command APDU</i>	26
3.6.2 <i>Response APDU</i>	26
3.6.3 <i>TPDU</i>	26
3.6.4 <i>Insieme dei Comandi base</i>	28
3.6.4 <i>Insieme dei Comandi avanzati</i>	29
3.7 EMULATORE DI SMART CARD	29
3.7.1 <i>Installazione</i>	30
3.7.2 <i>La smart card virtuale</i>	30
3.7.3 <i>Ciclo di vita</i>	31
3.7.4 <i>Informazioni sul microchip</i>	32
3.7.5 <i>Formattazione della smart card</i>	32
3.7.6 <i>Creazione del File System</i>	32
3.7.7 <i>Popolamento della smart card</i>	35
3.7.8 <i>Uso della smart card</i>	35
APPENDICE A.....	36

Introduzione

Nell'ultima decade le tecnologie basate su smart card hanno ricevuto grande attenzione sia nel mondo dell'informatica sia nel campo delle telecomunicazioni, in un panorama tecnologico che vede internet come un potentissimo strumento di comunicazione pur tuttavia non in grado di proporre un mezzo di identificazione certificata degli interlocutori, di assicurare un adeguato livello di privacy e di fornire un sistema di protezione delle informazioni trasmesse.

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 si sta attuando attraverso la completa riformulazione dei paradigmi di sicurezza preposti alla protezione delle informazioni riservate, alla protezione della privacy e, più in generale, alla sicurezza dei sistemi informatici.

La novità offerta 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 portato 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, 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 sta ormai diventando uno strumento indispensabile nella vita quotidiana.

Sebbene la tecnologia sia ormai consolidata, le numerose esigenze scaturite 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 smart card di diversa 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 e quindi è 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 leggera, 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, rivolto principalmente al programmatore, sulle architetture, i paradigmi di programmazione e le API relative a ciascuno standard e/o specifica tecnica.

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 un 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.