

Ugo Chirico

Programmazione delle Smart Card

Seconda Edizione

Copyright © 2002-2013 by Ugo Chirico 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.ugochirico.com>

ISBN: 978-1-291-45932-6

INDICE

INTRODUZIONE	10
1 LA SMART CARD	12
1.1 LA STORIA	13
1.2 ARCHITETTURA HW/SW	13
1.3 LA SMART CARD A SUPPORTO DELLA CRITTOGRAFIA	15
1.4 LA SMART CARD NELLE PROCEDURE DI AUTENTICAZIONE	15
1.5 LE APPLICAZIONI	16
1.6 GLI STANDARD	19
1.7 CASE STUDY	21
1.7.1 CORPORATE CARD	21
1.7.2 LA CARTA NAZIONALE SERVIZI	24
1.7.3 IL PROGETTO E-POLL	25
1.7.4 CARTA MULTISERVIZI DELLA DIFESA	26
2 FONDAMENTI TECNOLOGICI	29
2.1 LA SMART CARD	29
2.1.1 MEMORY CARD	30
2.1.2 MICROPROCESSOR CARD	31
2.1.3 SMART CARD CONTACT, CONTACTLESS E DUAL INTERFACE	32
2.1.4 TOKEN USB	34
2.2 ARCHITETTURA DEL MICROCHIP	34
2.3 PRODUZIONE DELLE SMART CARD	37
2.4 IL SISTEMA OPERATIVO	38
2.5 PROTEZIONE DEI DATI SULLA SMART CARD	38
2.6 QUALE SMART CARD ?	39
3 LE SPECIFICHE STANDARD ISO 7816	41
3.1 LE SPECIFICHE TECNICHE STANDARD	41
3.2 CARATTERISTICHE FISICHE ED ELETTRICHE	43

3.3 L'ATR	45
3.4 PROTOCOLLI DI TRASMISSIONE	46
3.4.1 PROTOCOLLO T = 0	47
3.4.2 PROTOCOLLO T = 1	47
3.4.3 PROTOCOLLO T = CL	47
3.5 STRUTTURA E FORMATO DEI DATI MEMORIZZATI NELLA EEPROM	48
3.5.1 FILE SYSTEM	48
3.5.2 TIPOLOGIA E FORMATO DEI FILE	49
3.5.3 PERMESSI DI ACCESSO AI FILE	51
3.5.4 SECURE MESSAGING	51
3.6 L'INSIEME DEI COMANDI	52
3.6.1 COMMAND APDU	52
3.6.2 RESPONSE APDU	53
3.6.3 TPDU	54
3.6.4 INSIEME DEI COMANDI BASE	55
3.6.4 INSIEME DEI COMANDI AVANZATI	58
3.7 EMULATORE DI SMART CARD	59
3.7.1 INSTALLAZIONE	61
3.7.2 LA SMART CARD VIRTUALE	62
3.7.3 CICLO DI VITA	62
3.7.4 INFORMAZIONI SUL MICROCHIP	63
3.7.5 FORMATTAZIONE DELLA SMART CARD	64
3.7.6 CREAZIONE DEL FILE SYSTEM	64
3.7.7 POPOLAMENTO DELLA SMART CARD	67
3.7.8 USO DELLA SMART CARD	68
4 MEMORY CARD	69
<hr/>	
4.1 TIPOLOGIE DI MEMORY CARD	70
4.1.2 ACCESSO LIBERO (I ² C)	70
4.1.3 COUNT-DOWN	71
4.1.4 COUNT-DOWN CON AUTENTICAZIONE	71
4.1.5 MEMORIA PROTETTA	72
4.2 INTEGRAZIONE DELLE SMART CARD A SOLA MEMORIA	74
PARTE 2 PROGRAMMAZIONE IN C/C++, C#, VB.NET E JAVA	75
<hr/>	
5 LE SPECIFICHE PC/SC	77

5.1 L'ARCHITETTURA PC/SC	77
5.1.1 INTEGRATED CIRCUIT CARD	78
5.1.2 INTERFACE DEVICE	79
5.1.3 L'INTERFACE DEVICE HANDLER	79
5.1.4 RESOURCE MANAGER	79
5.1.5 SERVICE PROVIDER	80
5.2 IL SERVIZIO RESOURCE MANAGER	81
5.3 L'API DEL RESOURCE MANAGER	82
5.4 C/C++	85
5.4.1 IMPORTARE LE FUNZIONI DELL'API	85
5.4.2 CONNESSIONE AL RESOURCE MANAGER	85
5.4.3 LISTA DEI LETTORI CONOSCIUTI DAL SISTEMA	86
5.4.4 CONNESSIONE ALLA SMART CARD	87
5.4.5 INVIO DI UNA APDU	88
5.4.6 LETTURA DI UN FILE PROTETTO DA PIN	90
5.4.7 SUGGERIMENTI	95
5.4.8 ESERCITAZIONI CON L'EMULATORE	95
5.5 IL SERVICE PROVIDER	96
5.6 VISUAL BASIC 6	97
5.6.1 LETTURA DI UN ELEMENTARY FILE CON IL SERVICE PROVIDER	98
5.6.2 CONNESSIONE ALLA CARTA	98
5.6.3 VERIFICA DEL PIN	99
5.6.4 LETTURA DI UN ELEMENTARY FILE	100
5.6.5 SCRITTURA IN UN ELEMENTARY FILE	101
5.6.6 CHIUSURA DELLA CONNESSIONE	102
5.6.7 GESTIONE DEGLI ERRORI	102
5.6.8 L'OGGETTO SCARDAUTH	104
5.6.9 LE API DEL RESOURCE MANAGER IN VISUAL BASIC 6	105
5.7 .NET SMART CARD API	107
5.7.1 INVIARE UN APDU ALLA SMART CARD	109
5.7.2 C#	109
5.7.3 VB.NET	111
6 OPENCARD FRAMEWORK	113
<hr/>	
6.1 ARCHITETTURA DI OPENCARD FRAMEWORK	114
6.1.1 CARDTERMINAL	116
6.1.2 CARDSERVICE	117
6.1.3 EVENTI CARDTERMINAL	118
6.2 APPLICAZIONE JAVA CON OCF	119

6.2.1	INSTALLAZIONE E CONFIGURAZIONE DI OCF	119
6.2.2	INVIO DI UNA COMMAND APDU	121
6.3	UN'APPLICAZIONE DI FIRMA DIGITALE CON OCF	124
6.3.1	INIZIALIZZAZIONE	126
6.3.2	GESTIONE DEGLI EVENTI	126
6.3.3	LETTURA DEL FILE "USERINFO"	128
6.3.4	GENERAZIONE DI UNA FIRMA DIGITALE	129
6.3.5	CHIUSURA DI OCF	131
7	JAVA SMART CARD I/O API	132
<hr/>		
7.1	INVIO DI INVIO DI UNA COMMAND APDU	133
8	GLOBALPLATFORM	137
<hr/>		
8.1	LE SPECIFICHE GLOBAL PLATFORM	138
8.1.2	DEFINIZIONI	139
8.1.3	CARD SPECIFICATION	139
8.1.4	DEVICE SPECIFICATION	140
8.1.3	SYSTEMS SPECIFICATION	140
8.2	ARCHITETTURA DELLA SMART CARD	140
8.2.1	SECURITY DOMAINS	142
8.2.2	GLOBAL SERVICES APPLICATIONS	143
8.2.3	RUNTIME ENVIRONMENT	143
8.2.4	TRUSTED FRAMEWORK	144
8.2.5	GLOBALPLATFORM ENVIRONMENT (OPEN)	144
8.2.6	GLOBALPLATFORM API	145
8.2.7	CARD CONTENT	145
8.2.8	CARD MANAGER	146
8.3	CICLO DI VITA DI UNA SMART CARD	147
8.3.1	CARD LIFE CYCLE STATES	148
8.4	EXECUTABLE LOAD FILE / EXECUTABLE MODULE LIFE CYCLE	150
8.4.1	EXECUTABLE LOAD FILE LIFE CYCLE	150
8.4.2	EXECUTABLE MODULE LIFE CYCLE	151
8.6	CARD CONTENT LOADING, INSTALLATION E MAKE SELECTABLE	153
8.7	CONTENT REMOVAL	155
8.8	COMMAND REFERENCE	156
9	JAVA CARD FRAMEWORK	158
<hr/>		

9.1 LA PIATTAFORMA JAVA CARD	158
9.2 JAVA CARD RUNTIME ENVIRONMENT	160
9.3 FUNZIONAMENTO DELLA JCRE	161
9.3.1 CARATTERISTICHE SPECIALI DEL JCRE	161
9.3.2 IL CICLO DI VITA DI UN'APPLET	162
9.4 JAVA CARD VIRTUAL MACHINE	163
9.4.1 JAVA CARD CONVERTER	163
9.4.2 JAVA CARD INSTALLER	165
9.4.3 JAVA CARD INTERPRETER	168
9.4.4 LINEE GUIDA PER LO SVILUPPO IN JAVA CARD	168
9.5 APPLETT JAVA CARD	169
9.5.1 IDENTIFICAZIONE DI UN'APPLET	169
9.5.2 COMUNICAZIONE CON UN'APPLET	170
9.6 IMPLEMENTAZIONE DI UN'APPLET	171
9.6.1 IL METODO <i>INSTALL</i>	172
9.6.2 CREAZIONE DI OGGETTI	175
9.6.3 IL METODO <i>SELECT</i>	175
9.6.4 IL METODO <i>DESELECT</i>	176
9.6.5 IL METODO <i>PROCESS</i>	176
9.7 CARATTERISTICHE E LIMITAZIONI IMPOSTE DAL FRAMEWORK	182
9.8 JAVA CARD DEVELOPMENT ENVIRONMENT	183
9.8.1 INSTALLAZIONE E CONFIGURAZIONE DEL DEVELOPMENT ENVIRONMENT	183
9.8.2 ECLIPSE JCDE	184
10 LE SPECIFICHE PKCS#11	195
<hr/>	
10.1 CRYPTOKI	195
10.1.1 ARCHITETTURA	196
10.1.2 STRUTTURA LOGICA DI UN <i>TOKEN</i>	197
10.1.3 INTERFACCIA DI PROGRAMMAZIONE	198
FUNZIONI DI CIFRATURA	200
FUNZIONI DI DECIFRATURA	200
FUNZIONI DI HASHING	200
FUNZIONI DI FIRMA DIGITALE	201
FUNZIONI DI VERIFICA DELLA FIRMA DIGITALE	201
FUNZIONI DI GESTIONE DELLE CHIAVI CRITTOGRAFICHE	202
FUNZIONI DI GENERAZIONE DI NUMERI CASUALI	202
FUNZIONI CRITTOGRAFICHE AVANZATI	202
10.2 PARADIGMA DI PROGRAMMAZIONE	203
10.2.1 INIZIALIZZAZIONE DEL <i>CRYPTOKI</i>	204

10.2.3 APERTURA DI UNA SESSIONE	206
10.2.4 LOGIN	208
10.2.5 CREAZIONE DEGLI OGGETTI SUL TOKEN	209
10.2.6 DATA	211
10.2.7 KEY	212
10.2.8 CERTIFICATE	215
10.2.9 OTTENERE UN RIFERIMENTO AD UN OGGETTO	216
10.2.10 LETTURA DEL CONTENUTO DI UN OGGETTO	218
10.2.11 FUNZIONI CRITTOGRAFICHE	219
10.3 .NET CRYPTOKI (C#, VB.NET)	222
10.3.1 NCryptoki	223
10.3 JAVA CRYPTOKI	232
<u>APPENDICE A: LA CARTA NAZIONALE SERVIZI (CNS)</u>	<u>241</u>
A.1 DETTAGLI TECNICI	242
A.2 LETTURA DEI DATI DALLA CNS	243
<u>APPENDICE B: EMV</u>	<u>247</u>
B.1 COS'È L'EMV?	248
B.2 EMV E APPLICAZIONI FINANZIARIE	249
B.3 EMV E SICUREZZA	250
B.4. AUTENTICAZIONE: SDA,CDA,DDA	250
B.5 GLI OBIETTIVI DELLE SPECIFICHE EMV	251
B.6 LA SITUAZIONE IN ITALIA	252
<u>APPENDICE C: LA SIM CARD</u>	<u>253</u>
C.1 LA SIM	253
C.2 GSM 11.11 / ETSI TS 102221	255
C.3 IL FILE SYSTEM DI UNA SIM	256
C.4 COMANDI DELLA SIM	259
C.5 LETTURA DELLA PROPRIA SIM	262
C.5.1 LETTURA DELL'ICCID	262
C.5.2 LETTURA DELLA RUBRICA DEGLI SMS	263
<u>APPENDICE D: IL SET DI COMANDI DELLA SMART CARD VIRTUALE</u>	<u>266</u>

ACTIVATE FILE	267
APPEND RECORD	267
CHANGE REFERENCE DATA	267
CREATE FILE	267
DEACTIVATE FILE	268
DELETE FILE	268
ERASE EEPROM	269
FORMAT	269
GENERATE KEY PAIR	269
GET DATA	270
INTERNAL AUTHENTICATE	270
PUT_DATA	270
READ BINARY	271
READ RECORD	271
RESET RETRY COUNTER	272
SELECT FILE	272
UPDATE BINARY	272
UPDATE RECORD	273
VERIFY PIN	273
APPENDICE E: CRITTOGRAFIA	274
E.1 TERMINOLOGIA	274
E.2 LA CRITTOGRAFIA	275
E.3 ALGORITMI A CHIAVE PRIVATA	277
E.4 ALGORITMI A CHIAVE PUBBLICA	278
E.5 LA TECNICA ADOTTATA NELLA PRATICA	280
E.6 LA FIRMA DIGITALE	280
E.7 GLI ALGORITMI DI HASHING	281
E.8 LA CERTIFICAZIONE	282
BIBLIOGRAFIA	284
RIFERIMENTI WEB	286

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 Grötrup. 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 capacità 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 di 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'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.

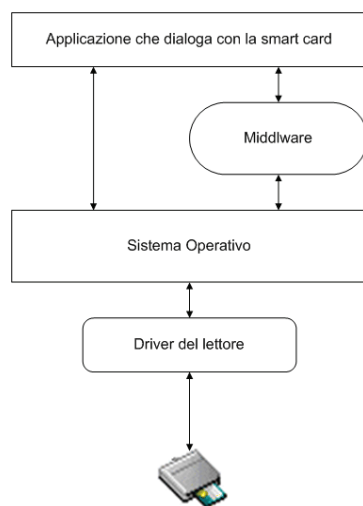


Figura 1.3 Architettura logica di un sistema con smart card

A partire dal basso, il lettore di smart card si interfaccia con il sistema operativo del computer attraverso un driver¹. Il sistema operativo mette a disposizione un insieme di funzioni a basso livello per comunicare con il lettore che possono essere usate direttamente dalle applicazioni o possono essere mappate in un insieme di funzioni ad alto livello, implementate in un *middleware*, 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 informazioni², 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>)