Parte seconda

Titoli Elettronici caratteristiche e vantaggi

di Gianni Becattini > g.becattini@aep-italia.it

Microprocessori, chiavi e moduli SAM: principi di funzionamento degli elementi su cui è basata la bigliettazione elettronica.

Concludiamo l'analisi delle caratteristiche e dei vantaggi dei titoli elettronici che, come abbiamo più volte sostenuto, rappresentano il futuro del Trasporto Pubblico Locale. Analizziamo in questo numero le funzioni dei sistemi a microprocessore ed indichiamo gli standard generali a cui fare riferimento; passeremo poi ad un'illustrazione dei moduli SAM e dei sistemi di protezione basati sulle chiavi di criptazione.

Il microprocessore

L'introduzione del microprocessore, alla fine degli anni '70, ha avviato una rivoluzione nel campo dell'elettronica e delle sue applicazioni la cui "onda lunga" si estende fino ai nostri giorni.

Prima di esso, i circuiti elettronici venivano "costruiti" e "cablati" per adempiere a determinate funzioni. Ogni modifica funzionale richiedeva necessariamente la modifica fisica dei circuiti stessi.

Con il microprocessore tutto cambia: la logica di funzionamento del circuito non è più fornita dal circuito, ma da una entità immateriale detta ***programma***, ossia della codifica in istruzioni elementari di algoritmi astratti che descrivono il comportamento desiderato del sistema.

Questo ha una importante implicazione: il comportamento del sistema non è più vincolato alla complessità del circuito ma può diventare virtualmente sempre più evoluto semplicemente scrivendo programmi più complessi. Ed è da qui che parte quella impressionante evoluzione dei circuiti digitali alla quale ancora facciamo fatica ad abituarci.

Il microprocessore ha costituito, fra l'altro, la base ideale per la progettazione dei personal computer e dello sviluppo del software che tutti conosciamo.

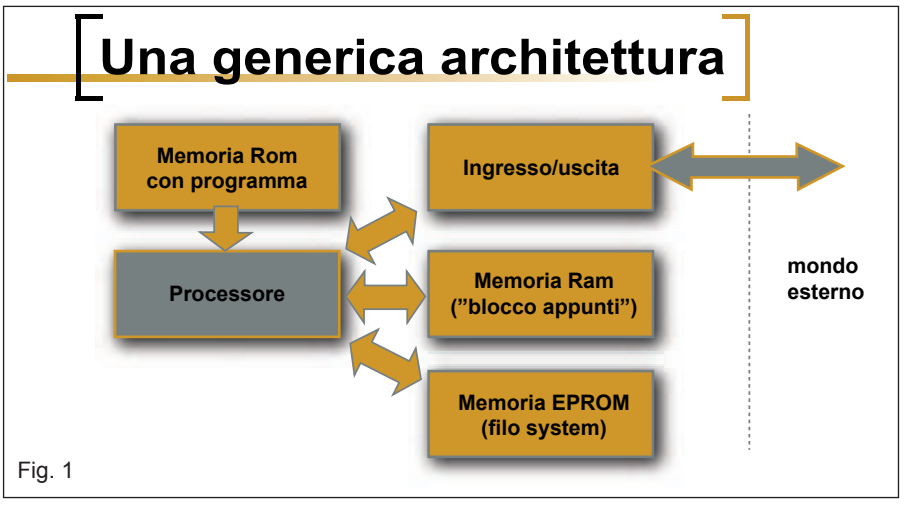


Fig. 1

Le smart card a memoria sono ancora circuiti con "logica cablata"; le smart card a microprocessore sono invece, a tutti gli effetti, logicamente simili a dei computer ed il loro comportamento dipende in massima parte dal programma in esse contenuto.

La **figura 1** mostra lo schema a blocchi di un generico sistema a microprocessore. In esso sono riconoscibili:

- ***il microprocessore***, ossia l'unità "intelligente" che decodifica ed esegue le istruzioni del programma, codificate in forma numerica. Esso è in grado di eseguire operazioni aritmetiche (es. 2+2) o logiche (es. "se A è maggiore di B fai questo, se no fai quello").
- ***la memoria*** contenente il programma;
- ***la memoria contenente dati temporanei*** (ad esempio i risultati parziali di certe elaborazioni);
- ***la memoria contenente i dati archiviati;***
- ***i dispositivi di comunicazione*** o di generica interazione con il mondo esterno.

La memoria

In verità, quasi tutti i moderni microprocessori (ma non tutti) seguono il cosiddetto schema di Von Neumann in cui la memoria è concettualmente unica anche se contiene entità logicamente diverse come il programma ed i dati. Esistono però dei validi motivi per separare fisicamente le varie aree di memoria, in modo da poter usare per esse tecnologie differenti.

La memoria ideale dovrebbe possedere caratteristiche quali tempo di accesso bassissimo, consumo di energia minimo, dimensioni fisiche minime, ritenzione dei dati per un tempo infinito e costo minimo.

Purtroppo questo tipo di memoria non è ancora stato realizzato, ragione per la quale si utilizzano, a seconda delle necessità, più memorie costruite con tecnologia diversa. In particolare:

- ***memoria RAM*** – memoria in lettura/scrittura, veloce, riscrivibile un numero

virtualmente illimitato di volte. Purtroppo è volatile: togliendo alimentazione, perde il suo contenuto e, all'accensione successiva, presenta contenuti casuali. Nel caso in esame è buona per la conservazione dei dati temporanei.

- memoria ROM – memoria in sola lettura, abbastanza veloce. Non potendo essere scritta se non in fase di fabbricazione torna utile per dati "fissi", ad esempio per la conservazione del programma.

- memoria EEPROM – memoria in lettura/scrittura, piuttosto lenta ma non volatile. E' l'ideale per ottenere un comportamento simile ad un hard disk. In essa si registrano i dati dell'utente, i contratti, i crediti, le ultime transazioni eseguite ecc.

Un suggerimento: in fase di scelta del tipo di smart card valutare soltanto le specifiche funzionali e le dimensioni della memoria EEPROM della smart card. Processore, dimensioni di ROM e RAM sono ininfluenti ai fini delle performance, una volta definite le specifiche funzionali. E' consigliabile non inserirli nei capitolati per non limitare inutilmente l'offerta di eventuali prodotti che siano capaci di centrare gli stessi obiettivi con tecniche più evolute.

Le unità di I/O

Se un sistema a microprocessore disponesse solo di quanto fin qui esaminato sarebbe del tutto inutile, in quanto ancora privo della capacità di colloquiare o interagire con il mondo esterno. A questo scopo sono deputate le cosiddette "unità di ingresso/uscita" (I/O, ossia "input/output"). Nel caso generale, esse potrebbero essere costituite, ad esempio, da relè, ingressi per sensori ecc. Nel caso delle smart card, è presente un'unica unità di I/O che viene usata per comunicare con il terminale attraverso il contatto o la radio frequenza. La comunicazione è di tipo seriale, una specie di "codice Morse", un bit dietro l'altro.

Il software

Una carta, similmente ad un PC, non è in grado di compiere alcuna operazione utile finché non venga dotata di un programma. Il produttore delle carte crea il programma che, risiedendo sulla carta, ne determina le caratteristiche funzionali. Una volta messo a punto, il programma viene passato al costruttore dei chip e trasformato in una maschera per la fabbricazione della ROM. I chip, sulla base della stessa, verranno prodotti già con il programma all'interno, pronti per essere incorporati nella struttura plastica della scheda. Esistono oggi soluzioni alternative alla costruzione della ROM con il codice già all'interno; ad esempio esistono memorie dette OTP (One Time Programming) che consentono di inserire il programma dopo la fabbricazione del chip o addirittura della carta intera. Per motivi di abitudine, tuttavia, molti continuano a chiamare "maschera" il software della carta (il cui nome corretto sarebbe "firmware"), ma il programma contenuto nel chip viene chiamato anche "sistema operativo".

Standard di riferimento

L'International Standards Organization (ISO) ha emesso una serie di standard per definire univocamente le smart card in termini di caratteristiche fisiche, elettriche e di comunicazione; si è creato così uno standard internazionale che dovrebbe garantire l'interoperabilità delle carte, anche se prodotte da diversi produttori, nei vari circuiti di utilizzo.

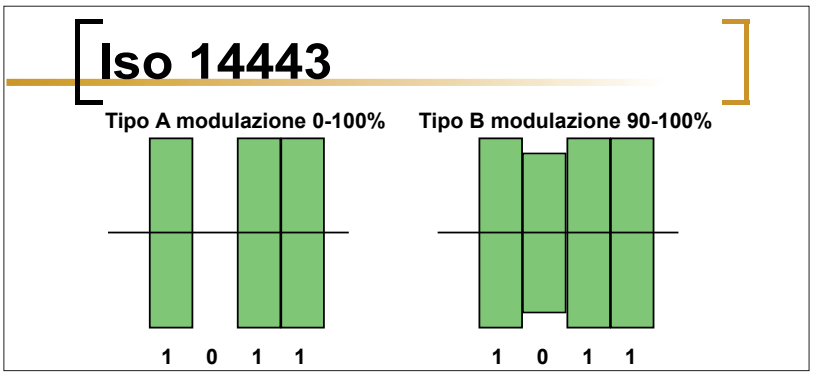
Gli standard più significativi per le applicazioni di TPL sono i seguenti:	
ISO 7816 parte 1°	Caratteristiche meccaniche
ISO 7816 parte 2°	Posizionamento ed uso dei contatti
ISO 7816 parte 3°	Protocollo di trasmissione
ISO 7816 parte 4°	Organizzazione dell'area dati e struttura dei comandi
ISO 14443 parte 1°	Caratteristiche fisiche
ISO 14443 parte 2°	Alimentazione radio e modulazione
ISO 14443 parte 3°	Inizializzazione ed anticollisione
ISO 14443 parte 4°	Protocollo di trasmissione

ISO 14443°

Questo standard è quello previsto per la comunicazione a radio frequenza dalle carte contactless MIFARE, un prodotto della Philips che ha trovato larghissima applicazione nel settore dei trasporti. A livello mondiale, la diffusione delle carte MIFARE supera di gran lunga quella di tutte le altre messe assieme. Si noti che la sola comunicazione in aderenza al 14443A non garantisce la compatibilità con le carte MIFARE. E' possibile cioè avere un terminale che processa carte di tipo A ma non carte MIFARE.

ISO 14443B

Si è detto che la comunicazione con le carte avviene con una tecnica in qualche modo simile al codice Morse. La modulazione della radio frequenza utilizzata nello standard di tipo A è di tipo 0/1, ossia si trasmette la portante per significare un "1" logico (linea Morse) e la si interrompe per lo "0" (punto Morse).



Questo determina un trasferimento di energia ridotto: quando si trasmette uno "zero" il trasferimento di energia è nullo. L'energia trasferita non risulta adeguata, in genere, al funzionamento delle carte a microprocessore. Per questo motivo è stato ideato lo standard del tipo B che ovvia a questo inconveniente.

Diversamente dallo standard 14443A, nato sulla

base di prodotti già esistenti, la variante B non è derivata da alcun prodotto. La maggior parte delle carte contactless a microprocessore usano questo standard per la sua flessibilità nel consentire alti flussi di dati (fino a 847 Kbs) e il 100% di disponibilità durante la transazione del segnale di clock, che è critico per alcune CPU. Molte delle nuove smart card presenti sul mercato supportano ora lo standard ISO 14443B.
Va osservato che la tecnologia avanza a grandi passi e che allo stato attuale sarebbe magari possibile realizzare carte a microprocessore di tipo A. Resta comunque il fatto che, in parallelo, diviene possibile, con il tipo B, l'impiego di carte di tipo ancora più evoluto.

ISO 15693

Un ulteriore standard da citare è l'ISO 15693, il cosiddetto standard per le operazioni di "vicinità". Le carte aderenti a questo standard possono essere lette a distanza maggiore, fino a quasi un metro, usando antenne di grandi dimensioni, molto simili a quelle che si impiegano nei varchi di uscita dei supermercati con finalità antifurto.
Questo standard assicura però una bassa velocità di comunicazione, inadeguata alle esigenze di un Sistema di Bigliettazione Elettronica. Anche l'affidabilità della transazione è imperfetta, per cui viene di solito relegato al rilevamento dei flussi di passeggeri.

ENV 1545

La norma ENV 1545 descrive la struttura dati raccomandata per le carte usate nelle applicazioni di trasporto pubblico. E' molto esteso e spesso ne viene usato solo un sotto assieme. E' raccomandabile adottarlo, almeno parzialmente.

Calypso

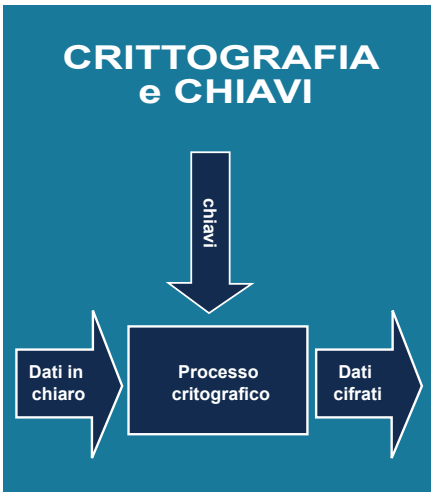
La società RATP di Parigi, che gestisce i trasporti pubblici della Ile de France (4000 bus, 420 stazioni di metropolitana), ha da molti anni effettuato cospicui investimenti per la definizione di una tecnologia per la bigliettazione elettronica.
La tecnologia Calypso, sviluppata per iniziativa di RATP, propone uno standard interoperabile di bigliettazione che è stato accettato anche in altre parti d'Europa e sta divenendo uno degli standard accettati per sistemi di pagamento con carte a microprocessore di tipo contactless.
La tecnologia Calypso, che è in continua evoluzione, è stata progettata congiuntamente agli operatori di trasporto di Bruxelles, Costanza, Lisbona, Parigi e Venezia ed è stata adottata dalle città di 9 paesi inclusi Parigi, Lisbona, Venezia, Lione, Skopje, Glasgow, Amiens, Avignone, Metz, Nizza.

	Layer	Standard internazionali	Calypso
7	Gestione Sicurezza e architettura		Calypso Security Architecture
6	Software del terminale		Calypso API
5	Modello dati		Calypso Data Model
4	Meccanismi di sicurezza della carta e della SAM		Calypso Card Application
3	Struttura dati della carta	CEN ENV 1545	
2	S.o. della carta, comandi e struttura file	ISO 7816-4	
1	Interfaccia contact e contactless	ISO 7816 1-3 ISO 14443 B 1-4	

Gli scopi di Calypso sono di definire delle specifiche di riferimento per le carte e assicurare l'interoperabilità tra gli operatori per i terminali.
Calypso è basato sugli standard internazionali già indicati (ISO 14443, ISO 7816, ENV1545), in alcuni casi ha costituito la base stessa sulla quale è stato sviluppato lo standard e promuove la standardizzazione di altri elementi. Al momento gli standard internazionali non sono abbastanza completi da garantire la reale interoperabilità dei prodotti di bigliettazione. Così Calypso, anticipando gli standard, propone specifiche che cercano di definire completamente una comunicazione carta-terminale interoperabile per la bigliettazione.
La tabella sopra indica le correnti relazioni tra gli standard internazionali e Calypso:
Le scelte Calypso sono le seguenti:
- ISO 7816 (parti da 1 a 4) per le applicazioni smart card. Questo è uno standard ben stabilito che è stato completato da Calypso per l'applicazione alla bigliettazione contactless (linea 4 nella tabella).
- ISO 14443B per il collegamento contactless.
- ENV 14445 per il dizionario dati della bigliettazione per il trasporto, che definisce i dati come supporto delle informazioni, eventi di pagamento ecc.
In aggiunta Calypso specifica con precisione i meccanismi di sicurezza per la carta e per la SAM.
Gli svantaggi della tecnologia Calypso sono nella sua complessità e nel maggior costo delle apparecchiature e delle carte. Pur trattandosi in molti casi di standard, è necessario corrispondere infatti un premio di licenza per utilizzarla, anche se questi costi sono inferiori a quelli che si dovrebbero sostenere per sviluppare da zero un sistema contraddistinto da equivalenti caratteristiche. I costi delle licenze si applicano solo ai costruttori e non alle società di trasporto, ma è evidente che è comunque l'utente finale che, indirettamente, li sostiene.

Sicurezza e chiavi

La creazione di falsi documenti di viaggio, se sufficientemente semplice, è un'attività criminale potenzialmente alquanto lucrosa. E' indispensabile quindi prevedere adeguate contromisure. Molte possono essere le tecniche impiegabili per garantire la sicurezza della transazione di un TDVE.

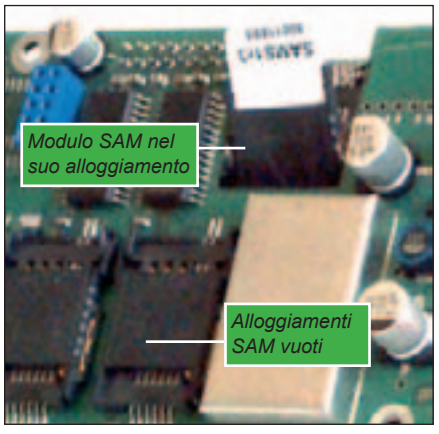


La scienza della crittografia è antica e, negli ultimi anni, ha fatto notevoli progressi, non solo per ragioni militari o strategiche ma anche perché indispensabile in ambito bancario.
Oggi si ritiene ormai accertato che non è opportuno basare la sicurezza sull'impiego di algoritmi segreti: essi prima o poi ven-

gono conosciuti, esponendo il sistema a probabili effrazioni. Si tende invece ad utilizzare algoritmi crittografici pubblici, come ad esempio il DES e il triplo DES, basando l'operazione di codifica su numeri segreti detti chiavi.
Attraverso un adeguato impiego di tecniche crittografiche è possibile assicurarsi contro l'impiego di carte non autorizzate o, viceversa, impedire che un terminale non legittimato possa sottrarre credito da carte autentiche.

I moduli SAM

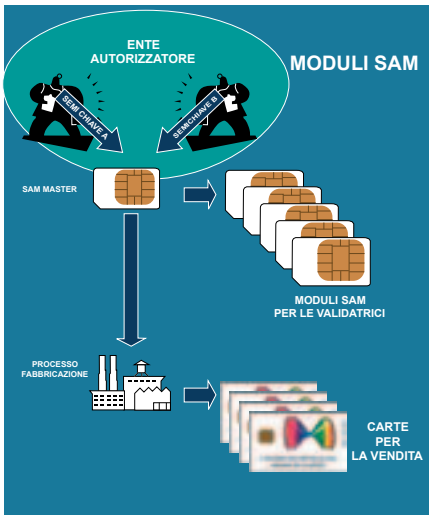
Una volta costruito un sistema basato sui principi ora esposti, il problema diventa quello di garantire la segretezza delle chiavi crittografiche.
Una soluzione, ormai di impiego generalizzato, è quella di utilizzare nei terminali una seconda smart card, detta SAM (Security Access Module). Essa viene, di solito, fisicamente "tagliata" per ridurne l'ingombro ed assume quindi l'aspetto esteriore delle classiche SIM impiegate per la telefonia cellulare.
Gli scopi del modulo SAM possono essere molteplici e differire a seconda dello schema di sicurezza adottato. I moduli SAM possono ad esempio essere usati per contenere le chiavi crittografiche, eseguire operazioni di crittografia, conservare una copia delle transazioni effettuate e generare una firma elettronica che garantisca l'autenticità delle transazioni.



Grazie ai moduli SAM è possibile scindere la fornitura dei terminali, che può essere affidata virtualmente "a chiunque" e avere al contempo nella stessa Comunità tariffaria (formata da Compagnie servite da fornitori diversi) apparati di marca e modello diversi.
I terminali, in questo caso, dovranno ovviamente risultare dotati di uno o più alloggiamenti ove inserire i diversi moduli SAM ed essere in grado di processarli.
Le chiavi, la SAM master e tutti i diritti relativi ad essa devono essere di esclusiva proprietà dell'Ente responsabile della Compagnia o della Comunità Tariffaria, l'unico autorizzato, come una Zecca dello Stato, alla "tiratura" delle carte e dei relativi contenitori di chiavi, i moduli SAM.

SAM come custodia per le chiavi

E' evidente che non è opportuno conservare le chiavi crittografiche nel software della validatrice, a portata di un qualunque addetto "infedele". E' anzi opportuno che nessuno le conosca nella loro interezza. Esse vengono invece generate, con una complessa e collaudata procedura, da due "semichiavi", in possesso di due persone diverse, ciascuna delle quali ignora l'altra semichiave. In base a questa procedura viene costruito un modulo, detto "SAM master" che è la "matrice" dalla quale possono essere generate, in modo automatico e sicuro, tanto le smart card di produzione, che saranno poi poste in vendita agli utenti, quanto i "moduli SAM", che hanno lo scopo di costituire il contenitore inviolabile in cui si trovano le chiavi all'interno delle validatrici e che risultano indispensabili per processare le carte prodotte con lo stesso



insieme di chiavi.
Al momento della transazione, la validatrice, con un complesso procedimento, verifica, tra l'altro, che la smart card presentata dall'utente sia capace di eseguire le operazioni crittografiche previste; questo è possibile solo se la carta presentata è stata costruita con le stesse chiavi contenute nella SAM; viceversa fa la smart card, per controllare che la validatrice sia effettivamente in possesso della chiave corretta (mutua autenticazione).
Quindi se le chiavi con cui sono state costruite le carte non collimano con quelle contenute nel modulo SAM della validatrice, nessuna operazione da eseguirsi "in sicurezza" è possibile.

Altri impieghi dei moduli SAM

Alcuni moduli SAM possiedono una memoria riscrivibile sufficientemente grande da poter contenere un certo numero di transazioni. In caso di guasti al terminale, essi possono essere impiegati per il recupero dei dati relativi alle operazioni effettuate.
In certi casi è possibile utilizzare il modulo SAM anche per garantire la trasmissione dei dati verso il centro di controllo. Tramite il SAM viene generata una firma digitale da apporre in coda alla transazione. Il sistema centrale esegue una verifica e controlla che la firma sia corretta, permettendo così di individuare eventuali transazioni false.

Chiavi differenziate

Un modulo SAM può contenere o meno più chiavi per l'accesso a zone differenti della carta o per differenti operazioni. Si possono ad esempio avere SAM con le sole chiavi per il solo "consumo" (transazione di fruizione) o contenenti anche le chiavi per eseguire la ricarica del credito.
Si osservi che, per evidenti ragioni di sicurezza, è opportuno controllare e limitare la diffusione di moduli SAM con chiavi che consentano solo le operazioni effettivamente necessarie.

Conclusione

Chi ha avuto la pazienza di seguire fino a questo punto, si aspetterebbe probabilmente che si procedesse adesso ad una elencazione delle tipologie di carte più comuni e delle loro caratteristiche, ma questo è un argomento che merita uno spazio più ampio. MobilityLab si impegna a tornare sull'argomento con una specie di "prova comparativa" per le carte più conosciute e diffuse tanto in Italia quanto all'estero.

Autore

Gianni Becattini
è uno dei pionieri dell'informatica italiana. Nel 1975 progetta uno dei primi personal computer italiani e fonda la General Processor, i cui prodotti sono oggi esposti al Museo dell'Informatica di Pisa. Titolare di uno studio di consulenza e progettazione, ha operato in numerosi settori dell'automazione industriale. Dal 1999 dirige AEP, di cui oggi è Amministratore Delegato, uno dei principali operatori italiani nel settore del pagamento elettronico dei servizi di Trasporto Pubblico Locale (www.aep-italia.it).