

LE SMART CARD DALLE ORIGINI AL FUTURO

Giancarlo Mauri

I pionieri

Chi è il padre, l'inventore della carta a microprocessore? Ogni nuova invenzione ha bisogno, per essere sviluppata, di alcuni elementi: l'idea, la tecnologia, l'esigenza socio-economica (e quindi i finanziamenti), gli uomini in grado di mettere insieme questi elementi e di portare avanti il progetto.

Nel caso della carta a microprocessore, l'esigenza nasce in Francia, nel 1975, quando i dirigenti del circuito bancario Carte Bleu incontrano numerosi problemi nella penetrazione di mercato del loro prodotto, soprattutto a causa della bassa sicurezza delle transazioni. Si mettono quindi alla ricerca di un sistema di pagamento sicuro, in grado di autoverificarsi.

Un sistema simile è descritto nel 1968 nel romanzo "La notte dei tempi" di Renè Barjavel, che parla della civiltà perduta di Gondawa, in cui ciascuno "riceveva ogni anno una uguale quantità di crediti, calcolata sulla produzione totale delle fabbriche. Questi crediti erano gestiti da un computer centrale, ed erano ampiamente sufficienti a garantirgli di vivere serenamente, sfruttando pienamente tutto ciò che la società poteva offrirgli. Ogni volta che un Gonda desiderava qualcosa di nuovo, vestiti, oggetti, un viaggio, pagava con il suo anello-chiave. Gli bastava piegare l'anello, inserire la chiave in una fessura, e il suo conto nel computer centrale veniva immediatamente ridotto dell'importo della merce o dei servizi acquistati".

Forse a questo romanzo si è ispirato Roland Moreno, che nel 1974 aveva presentato per il brevetto un "processo e un dispositivo per il controllo elettronico" dell'identità degli individui, poi proposto ai banchieri come soluzione al loro pro-

blema. In effetti, la prima proposta di Moreno si basava su un anello, e solo in un secondo tempo, dopo aver raccolto le osservazioni e le obiezioni delle banche, l'anello fu sostituito dal rettangolino di plastica che si sarebbe poi diffuso.

A quel punto, si trattava di trovare la tecnologia adatta per concretizzare il progetto, attraverso lo sviluppo di un chip con una memoria sufficiente a contenere le informazioni richieste, e il suo inserimento nella carta senza danneggiarlo. Moreno si rivolse a diverse aziende, tra cui la Honeywell-Bull, che aveva sviluppato la tecnologia TAB (Tape Automated Bonding). Il processo consentiva di trasferire automaticamente i chip su un nastro da 35 mm simile a una pellicola cinematografica, e fu adattato alla produzione di carte a microchip: nasceva così la smart card, e Roland Moreno è passato alla storia come il suo inventore.

In realtà, Moreno rimase legato ad una concezione tecnologica piuttosto arretrata, e pensava al chip esclusivamente come una memoria realizzata con la tecnologia bipolare prevalente a quell'epoca. Michel Ugon, l'ingegnere della Bull che collaborava con lui, pensava invece che il livello di sicurezza richiesto per una carta bancaria potesse essere raggiunto solo dotando il chip di capacità di elaborazione che solo le più avanzate tecnologie unipolari della famiglia MOS potevano consentire. Questa differenza di vedute provocò una forte tensione tra i due e una divaricazione tra la Innovatron, società fondata da Moreno per portare avanti il progetto, e la Bull. Il punto centrale, che permette anche di stabilire il "grado di paternità" della smart card come la conosciamo oggi, sta proprio nella scelta della tecnologia. Secondo Moreno, è fondamentale che le carte siano estremamente robuste e poco care. Già il



primo punto da solo implica che si debbano scartare le tecnologie unipolari (essenzialmente N-MOS, P-MOS e C-MOS) che, per almeno altri cinque anni, saranno caratterizzate da una estrema vulnerabilità. La posizione intransigente di Moreno è ancora più chiara quando dichiara che “qualunque utilizzo di un microprocessore o di un microcontrollore in una carta deve essere scartato, fino almeno al 1985”. Nel 1980, Ugon presentava la prima carta dotata di un microprocessore, smentendo clamorosamente Moreno: da questo primo prototipo derivano i chip usati attualmente.

L'esplosione della potenza

Come si è visto, la scelta della tecnologia MOS per la fabbricazione dei circuiti integrati, dovuta soprattutto a Michel Ugon, è stata fondamentale per il passaggio dalle carte a memoria tipo scheda telefonica a carte che somigliano sempre più a computer in miniatura, con crescenti capacità di calcolo in grado di garantire alti livelli di sicurezza e di prestazioni, oltre alla integrazione di funzioni diverse.

Il primo “Self-Programming One-Chip Microcomputer”, CP8, presentato nel 1980, conteneva due chip: una memoria da pochi byte e un microprocessore da 8 bit.

Da allora il mercato delle carte a microprocessore è andato continuamente crescendo, così come la loro potenza. Le smart card odierne possono essere tranquillamente confrontate con i PC degli anni 80; inoltre, secondo Marc Lassus, top manager di Gemplus, la potenza di calcolo complessiva installata nelle smart card, valutata in 34.000 Mdhrystone nel 2000, ha sorpassato nel 1997 quella dei sistemi mainframe (ferma nel 2000 a 5.400 Mdhrystone) e subito dopo quella dei PC (20.000 Mdhrystone).

Nel 1981 il prototipo CP8 era già un prodotto commerciale con un circuito da 19,5 mm², 42000 transistor, 36 bytes di RAM, 1024 byte di EPROM e 1,6 kbyte di ROM per il sistema operativo, una porta seriale da 9,6 Kb/s, e una unità di elaborazione da 8 bit in tecnologia CISC con funzioni di sicurezza che nessun PC aveva.

Vent'anni dopo, il progetto europeo MEDEA-MASSC ha realizzato un chip prototipale da 25 mm², con memoria di lavoro da 4 Kb (100 volte quella di vent'anni prima), una ROM da 96 Kb, una EEPROM da 64 kb e una CPU a 32 bit in tecnologia RISC, con una potenza di calcolo di 35 MIPS. Se si pensa che l'Intel 486 DX66 aveva una poten-

za di 20 MIPS e il primo Pentium raggiungeva a stento i 100 MIPS, con un circuito di dimensioni ben maggiori, ci si rende conto degli enormi progressi delle smart card negli ultimi venti anni. Si tratta ormai di veri e propri computer, sia pure senza tastiera e schermo.

