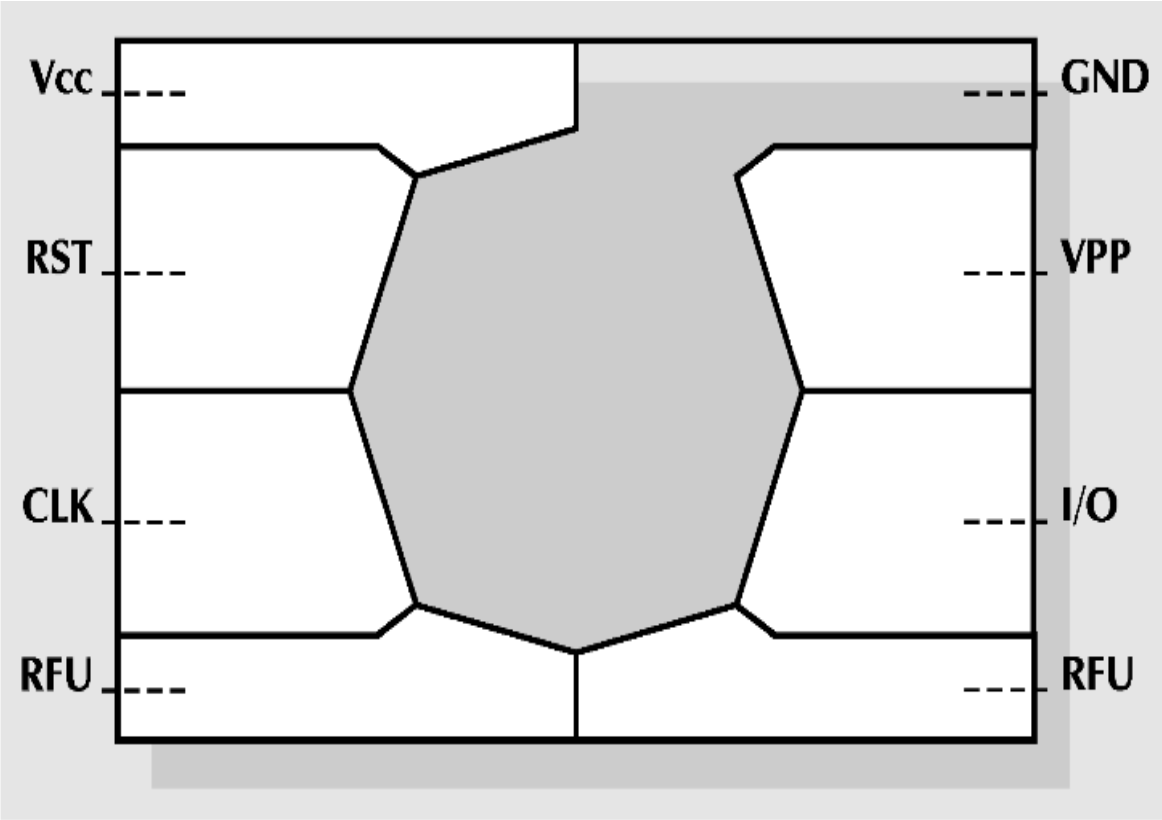
La tecnologia delle smart card.

Il nome smart card o carte intelligenti cattura l'immaginazione, comunque tale termine è ambiguo ed è usato in molti modi differenti. La ISO (Organizzazione per gli Standard Internazionali) usa il termine, Integrated Circuit Card (ICC) per comprendere tutti quei dispositivi dove un circuito integrato è contenuto in pezzo di plastica o carta di identificazione ISO ID1. La carta ha le dimensioni di 85.6mm x 53.98mm x0.76mm identiche alla diffusissima carta bancaria con la sua striscia magnetica usata come strumento di pagamento.

Le carte con circuito integrato sono di due tipi, con contatti e senza contatti. Il primo è facile da identificare a causa del suo piatto connettore di oro. Sebbene lo standard ISO definisca otto contatti , solo sei sono in realtà usati per comunicare con il mondo esterno. La carta senza contatti può contenere la propria batteria, particolarmente nel caso delle carte super intelligenti che hanno una tastiera integrata ed un display a cristalli liquidi.

In generale comunque la potenza è fornita alla elettronica della carta senza contatti mediante induzione magnetica usando radiazioni elettromagnetiche a bassa frequenza. Il segnale di comunicazione può essere trasmesso in una maniera similare o può fare uso di accoppiamento capacitivo o persino di connessione ottica.

La carta con contatti è la più comune ICC al momento soprattutto a causa del suo uso in Francia ed ora in altre parti d'Europa come carta telefonica. La maggior parte delle carte contiene un semplice circuito integrato sebbene vari esperimenti siano stati effettuati con due chip. Il chip stesso varia in modo considerevole tra differenti fabbricanti e fa le diverse applicazioni. Consideriamo prima lo scopo dei sei contatti usati dalla ICC .



La Vcc è la tensione di alimentazione che guida i chip ed è generalmente di 5 V . Si dovrebbe far notare comunque che in futuro è molto probabile che vedremo una tendenza verso i tre volt, avvantaggiandoci della tecnologia avanzata dei semiconduttori e permettendo livelli di corrente più bassi . La Vss è la tensione di riferimento di substrato o terra verso la quale è misurato il potenziale Vcc. Il reset è la linea di segnale che è usata per inizializzare lo stato dei circuiti integrati appena si alimenta la scheda. Il segnale di clock è usato per guidare la logica della carta

ed è usato in oltre come riferimento per la comunicazione seriale. Sono comunemente usate due velocità di clock, 3.5795 MHz e 4.9152 MHz. Ci si potrebbe chiedere perché siano state scelte frequenze così strane. La ragione sta nel disponibilità di cristalli economici usati nel mondo della televisione. Il connettore Vpp è usato per il segnale ad alta tensione necessario per programmare la memoria EPROM. In fine c'è il connettore per l'input-output seriale. Questo è la linea di segnale mediante la quale la carta riceve comandi e scambia dati con il mondo esterno.

Vediamo cosa contiene il chip. L'uso primario della carta è per l'immagazzinamento e il recupero di dati. Quindi il componente fondamentale della carta è un modulo di memoria. La lista seguente rappresenta i più comuni tipi di memoria :

- ROM Memoria a sola lettura
- PROM Memoria a sola lettura programmabile
- EPROM ROM programmabile cancellabile
- EEPROM Prom cancellabile elettricamente
- RAM Memoria ad accesso casuale.

Un particolare chip può contenere uno o più di questi tipi di memoria. Questi tipi di memorie hanno particolari caratteristiche che ne determinano la modalità d'uso. La memoria di tipo ROM è fissa e non può essere cambiata dopo essere stata realizzata da una fabbrica di semiconduttori. Questa è una memoria di basso costo, in quanto occupa uno spazio minimo su substrato di silicio . Ciò è utile perché si vuole ottenere quanto più possibile nel minore spazio possibile. Il problema sta nel fatto che essa non può essere cambiata e una fabbrica di semiconduttori impiega mesi per produrla. Per ottenere un basso costo occorre poi una quantità minima di ordine.

La PROM è programmabile dall'utente mediante l'uso di collegamenti con fusibile . Comunque sono necessarie un'alta tensione e corrente per il ciclo di programmazione e tali dispositivi non sono usati normalmente nelle carte a circuiti integrati. La EPROM è stata ampiamente usata nel passato. Mentre la memoria è cancellabile mediante l'uso di luce ultravioletta, la necessaria finestra di quarzo non è mai disponibile nella carta per cui la EPROM è usata in realtà come una memoria programmabile una

volta sola. La EEPROM può essere cancellata dall'utente e riscritta molte volte (dalle 10000 al milione di volte in una applicazione tipica). Tutte queste memorie sono non volatili. In altre parole esse conservano il proprio contenuto anche quando non c'è alimentazione. La memoria ad accesso casuale è invece una memoria volatile dalla quale si perdono i dati appena si toglie alimentazione.

Dobbiamo notare che il costo della carta alla saturazione (cioè quando sono stati recuperati i costi di sviluppo) è proporzionale all'area del silicio usato. Il connettore ISO è perciò disegnato per costringere l'ampiezza del silicio a circa 25mm x 2. Il punto più importante è più legato all'affidabilità poiché chiaramente un pezzo più ampio di silicio sarebbe più facilmente disposto a fratture meccaniche.

C'è un altro prodotto secondario che considereremo più avanti dove il costo del testing e della personalizzazione sono considerevolmente alterati dalla complessità del particolare chip. E' chiaro che comunque dovremmo tentare di minimizzare i contenuti

del chip sia dal punto di vista del costo che della affidabilità commisuratamente alla particolare applicazione.

Naturalmente non si può avere qualcosa per niente e sebbene una carta telefonica può operare con una piccola memoria Eeprom (128-512 byte) e la logica di controllo della memoria, più sofisticate applicazioni chiederanno alla Rom , Eeprom, RAM e CPU di raggiungere il necessario obiettivo. E' l'aggiunta della CPU o microcontrollore che realmente porta al termine "intelligente" sebbene il termine non sia rigoroso.

La logica di controllo non dovrebbe essere trascurata poiché è necessaria non solo per i protocolli di comunicazione ma anche per offrire qualche protezione alla memoria contro usi fraudolenti. La carta ICC è probabilmente il sogno della sicurezza dell'uomo perché a differenza della maggior parte degli apparecchi di immagazzinamento e trattamento elettronico dei dati essa ha la sicurezza intrinsecamente costruita dentro : La ICC realmente offre un dominio resistente che è difficile da eguagliare con i più ingombranti scatole di sicurezza che trattano processi crittografici.

Ora possiamo differenziare i differenti tipi di ICC dal loro contenuto,

- sole memorie
- memorie con logica di sicurezza
- memorie con CPU

La logica di sicurezza può essere usata per controllare l'accesso alla memoria per i soli usi autorizzati. Questo si ottiene usualmente mediante qualche forma di codice di accesso che può essere realmente lungo (64 bit o più). Chiaramente l'uso di memorie EEPROM deve essere strettamente controllato laddove autori di frodi possono ottenere un vantaggio economico mediante un uso non autorizzato della carta. Il vantaggio in termini di sicurezza delle carte con CPU è chiaramente più significativo poiché la CPU è capace di implementare algoritmi crittografici.

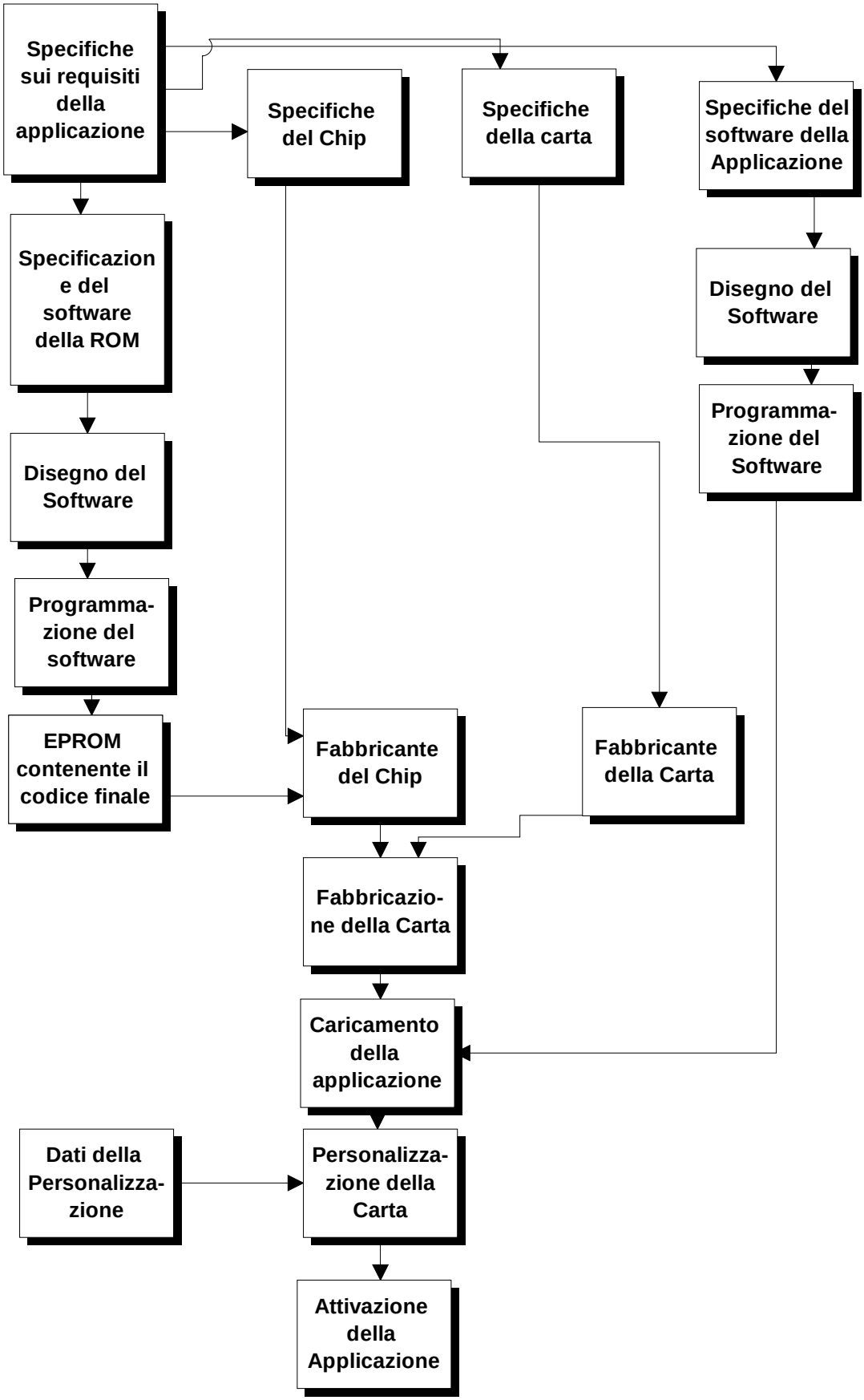
Nel mondo della smart card il termine applicazione è ampiamente usato per descrivere il software o programma che la ICC implementa. Nel caso più semplice la applicazione può essere soltanto un file manager per l'organizzazione

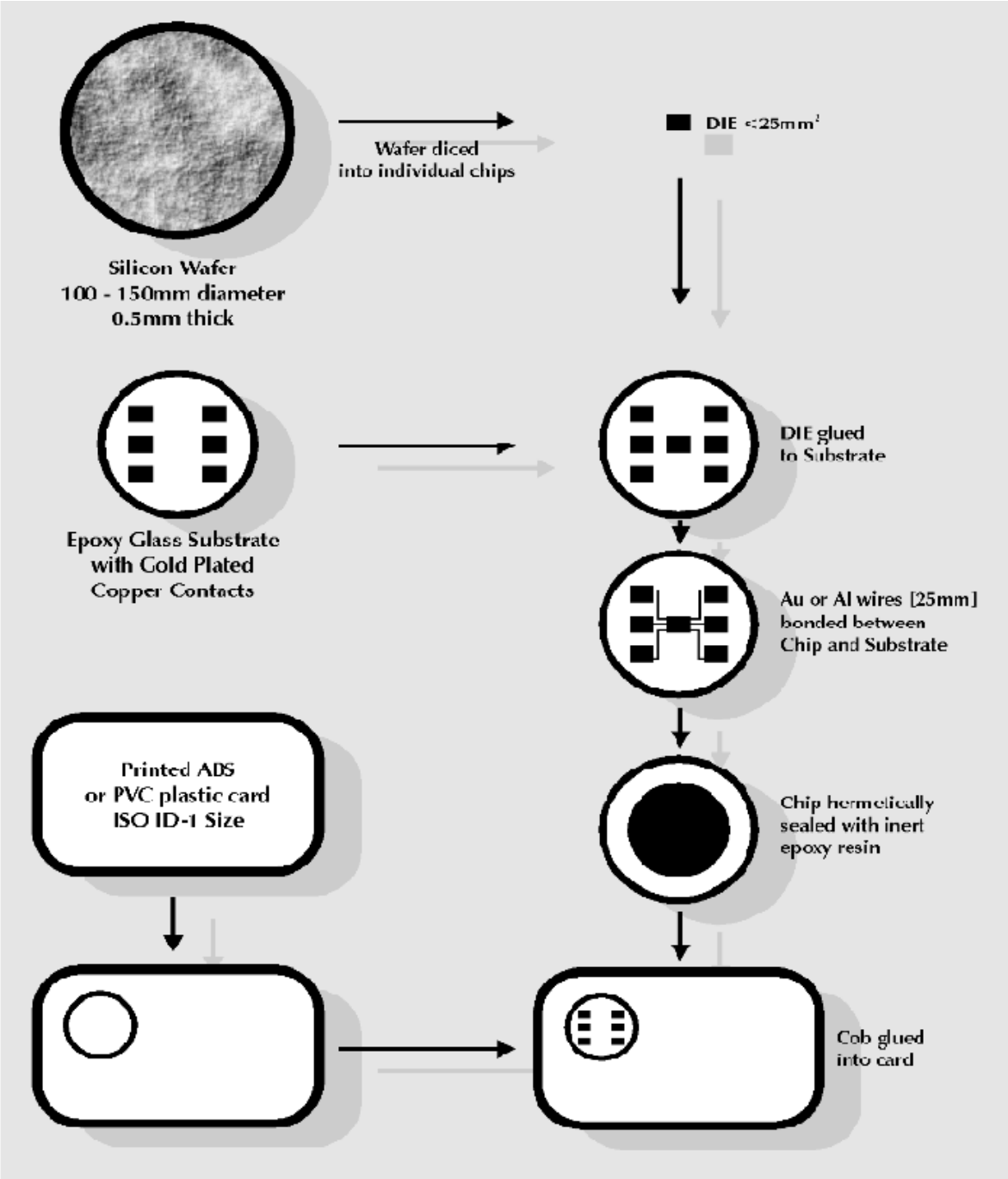
dell’immagazzinamento e il recupero dei dati. Una tale applicazione può essere completamente implementata nella logica del chip. In maniera similare il chip deve contenere la logica di comunicazione mediante la quale esso accetta comandi dall’apparecchiatura di accettazione della carta (CAD= card acceptance device) e attraverso la quale esso riceve e trasmette i dati dell’applicazione. La ICC che contiene una CPU può sostenere applicazioni più sofisticate e persino multiapplicazioni poiché la CPU è anche capace di processare i dati e prendere decisioni sulle varie azioni che vengono richieste.

Come è fatta la IC card.

La realizzazione di una smart card comporta un grande numero di processi dei quali l’inserimento del chip nella carta è il più critico al fine del raggiungimento di un prodotto di qualità complessiva. Si fa riferimento a quest’ultimo processo come fabbricazione della carta. L’intero processo inizia con le specificazioni delle richieste dell’applicazione. Dalle richieste individuali specifiche possono essere preparate per il chip, la carta, il software di maschera della

ROM e il software dell’applicazione. IL software della Rom viene fornito al fornitore del semiconduttore che realizza il chip. Il fabbricante della carta incastona il chip nella carta. Normalmente Il fabbricante carica il software di applicazione e i dati personalizzati. Ogni stadio della realizzazione della smart card è mostrato in fig. .


Specifiche sui requisiti della applicazione
Specifiche del Chip
Specifiche della carta
Specifiche del software della Applicazione
Specificazione del software della ROM
Disegno del Software
Programmazione del Software
Disegno del Software
Programmazione del software
EPROM contenente il codice finale
Fabbricante del Chip
Fabbricante della Carta
Fabbricazione della Carta
Caricamento della applicazione
Dati della Personalizzazione
Personalizzazione della Carta
Attivazione della Applicazione



Specifiche del chip

C’è un certo numero di fattori da decidere nella specificazione del circuito integrato per la smart card. Prendiamo ad esempio una carta

basata su CPU. I parametri chiave per la specificazione del chip sono i seguenti,

- tipo di microcontrollore
- ampiezza della ROM
- ampiezza della RAM
- tipo della memoria non volatile
- ampiezza della memoria non volatile
- velocità del clock (esterno e , opzionalmente interno)
- parametri elettrici (tensione e corrente)
- parametri di comunicazione (asincrona, sincrona, ecc)
- meccanismo di reset
- co-processore.

In pratica il fabbricante di semiconduttori ha una gamma di prodotti per i quali i parametri di qui sopra sono predefiniti. Il compito del disegnatore è quindi connesso con la scelta del prodotto appropriato per la particolare applicazione. La sicurezza può essere un aspetto importante e di conseguenza ci possono essere richieste extra sulla sicurezza fisica e logica offerta dal particolare chip.

Specifiche della carta.

La seguente lista elenca i principali parametri che dovrebbero essere definiti :

- dimensioni della carta
- posizione del chip
- materiale di cui è costituita la carta
- richieste di stampa
- striscia magnetica opzionale
- striscia per la firma
- ologramma o foto

Specifiche della ROM

La Rom contiene il sistema operativo della smart card. Esso è principalmente coinvolto nel trattamento dei file di dati ma può opzionalmente coinvolgere aspetti addizionali come algoritmi crittografici. Il codice sviluppato viene dato al fornitore che incorpora questi dati nel processo di fabbricazione del chip.

Specifiche del software dell'applicazione

Questa parte del processo di sviluppo della carta è chiaramente specifica della particolare applicazione. Il codice potrebbe essere designato come parte del codice della ROM ma l'approccio moderno è di disegnare il software di applicazione in modo che operi da una PROM non volatile. Questo permette una maggiore flessibilità di approccio poiché l'applicazione può essere caricata nel chip dopo la fabbricazione. La manifattura di un chip con il codice dell'utente nella ROM può richiedere tre mesi in media. Il codice dell'applicazione può essere caricato in una PROM in alcuni minuti senza avvalersi del produttore del chip.

Fabbricazione del chip.

La fabbricazione della carta coinvolge un certo numero di processi come mostrato in figura . Per prima cosa occorre fabbricare un substrato che contiene il chip. Questo viene spesso chiamato COB (chip on board) e consiste di un strato vetroso sul quale il chip viene collegato ai connettori. Vi sono tre tecnologie disponibili per questo processo. In ogni caso il wafer di semiconduttore realizzato dal

fornitore di semiconduttori viene diviso in chip individuali. Questo può essere fatto realizzando delle fessure mediante una punta di diamante e poi esercitando una pressione sul wafer in modo che si rompa lungo le fessure. Un foglio di mylar viene attaccato alla parte posteriore del wafer in modo che dopo la separazione i frammenti rimangano attaccati al foglio di mylar. Il legame a filo è la tecnica di uso più comune nella fabbricazione di carte. UN filo di oro o di alluminio di 25μm è collegato ai piedini del chip usando tecniche di saldatura a ultrasuoni o termocompressione. La saldatura a termocompressione richiede che il substrato venga mantenuto tra i 1500 e 2000 gradi centigradi . La temperatura sulla saldatura può raggiungere i 3500 gradi. Per alleviare questi problemi è spesso usata la saldatura termosonica che è una combinazione delle due tecniche precedenti ed opera a temperature inferiori.

Il montaggio dei vari frammenti e la saldatura dei fili comporta un gran numero di operazioni e sono perciò molto costosi. Poiché in generale soltanto 5 o 6 fili sono saldati per le applicazioni delle smart card questo approccio è accettabile.

Il substrato terminale viene ermeticamente sigillato con un materiale inerte come la resina epossidica. Il micromodulo completo viene poi incollato nella carta che contiene il buco di ampiezza appropriata.

Caricamento dell'applicazione

Assumendo che l'applicazione vada posta nella memoria PROM della carta il passo successivo è di caricare il codice nella memoria. Questo si ottiene usando i comandi di base contenuti nel sistema operativo della ROM. Questi comandi permettono la lettura e scrittura della PROM.

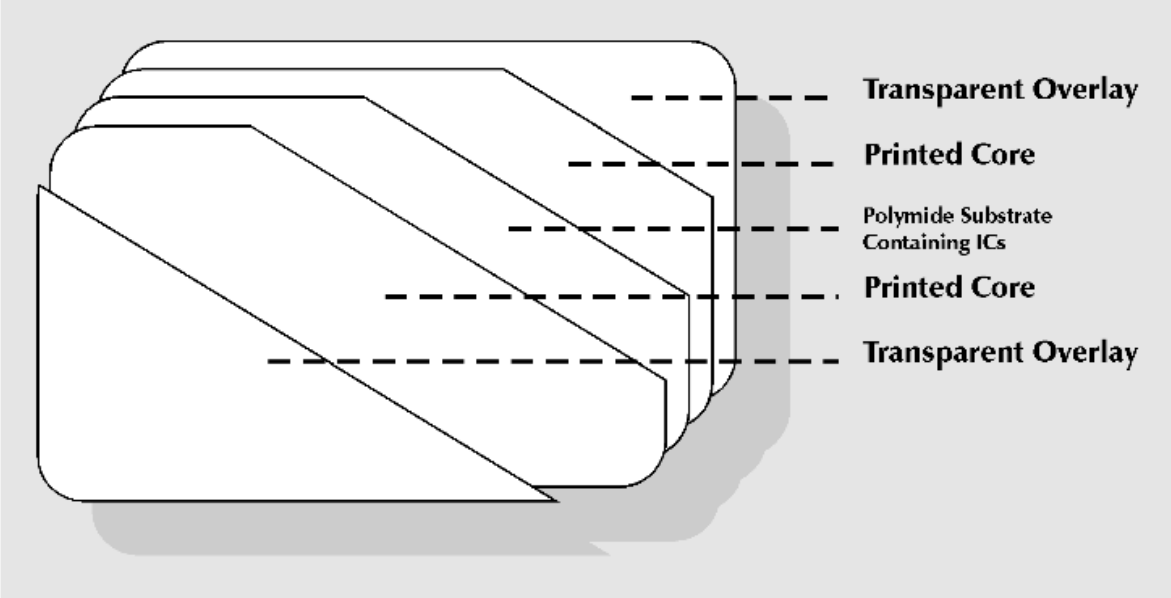
Personalizzazione della carta

La carta viene personalizzata per l'utente particolare caricando dati in file nella memoria PROM nello stesso modo in cui il codice dell'applicazione viene caricato nella memoria.

Attivazione dell'applicazione

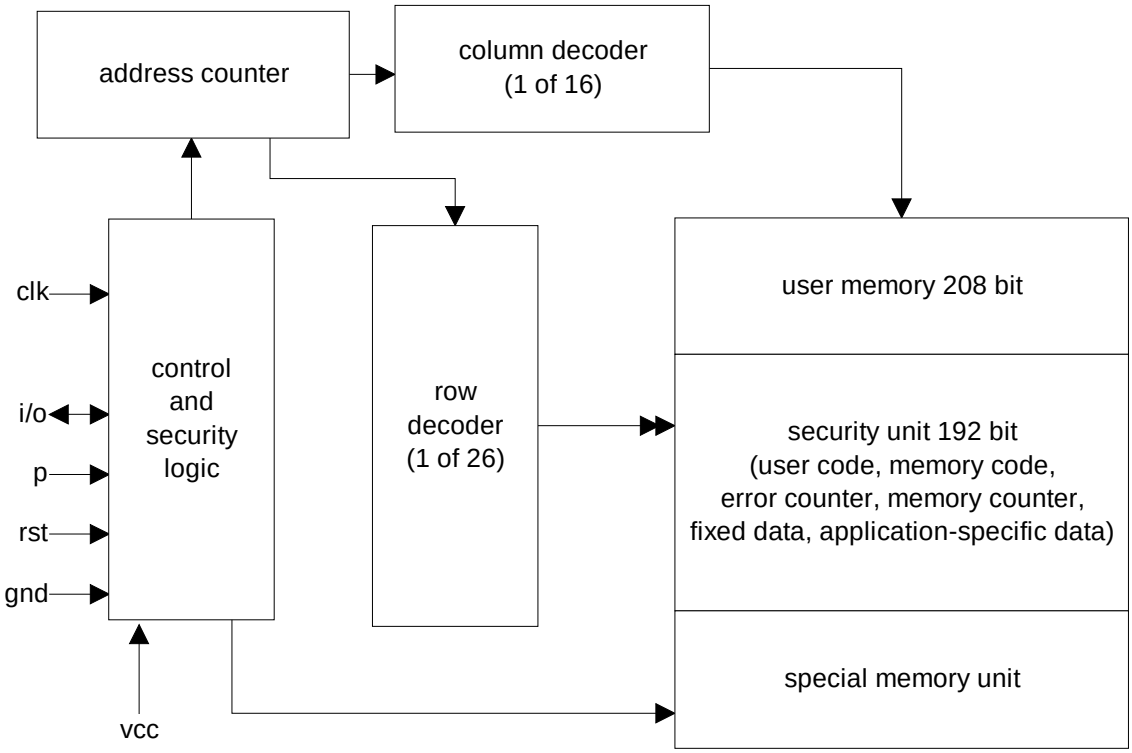
L'operazione finale nel processo di fabbricazione è l'abilitazione dell'applicazione. Questo comporta il settaggio di flags nella

memoria PROM che inibirà ogni ulteriore cambiamento nella memoria eccetto quelli sotto il diretto controllo dell'applicazione.



La chip card SLE4404 Siemens

IL nostro dispositivo di sorveglianza usa come chiave una chip card basata sull'integrato SLE4404 della Siemens il cui schema a blocchi appare in figura.



Di seguito abbiamo invece la organizzazione della memoria

blocco

MANIFACTURER CODE

indirizzo 0-15

numero bits 16

cancellazione

MAI

scrittura

MAI

lettura

SEMPRE

APPLICATION

ROM

indirizzo 16-63

numero bits 48

cancellazione MAI

scrittura mai

lettura SEMPRE

USER CODE

(BC)

indirizzo

64-79

numero bits

16

cancellazione

CON BC/FZ

scrittura

CON BC/FZ

lettura

(2)

ERROR

COUNTER

indirizzamento

80-83

numero bits

4

cancellazione

CON BC/FZ

scrittura

SEMPRE

lettura

SEMPRE

E2PROM-1

indirizzamento

84-95

numero bits

12

cancellazione

CON BC/FZ

scrittura

SEMPRE

lettura

SEMPRE

E2PROM-2

indirizzamento

96-111

numero bits

16

cancellazione

CON BC/FZ

scrittura

CON BC/FZ

lettura

SEMPRE

FRAME

MEMORY

indirizzamento

112-319

numero bits

208

cancellazione

CON BC/FZ/RC/RZ

scrittura

(1)

lettura

(1)

FRAME CODE

(RC)

indirizzamento

320-351

numero bits

32

cancellazione

(2)

scrittura

(2)

lettura

(2)

FRAME COUNTER

(RZ)

indirizzamento

352-415

numero bits

64

cancellazione

(2)

scrittura

SEMPRE

lettura

SEMPRE

La tabella mostra le possibili operazioni relative a ciascun blocco fermo restando la configurazione della frame memory con la seguente particolarità che i bit 112 e 113 configurano la Frame memory secondo le tabelle riportate nella pagina seguente. Nelle tabelle abbiamo usato le seguenti convenzioni :

- BC significa che per l'operazione è richiesto l'introduzione del User Code ; in questo caso FZ indica che all'introduzione del codice è associata la diminuzione di un bit dell'Error Counter.
- Il simbolo RC dice che l'operazione interessata richiede l'introduzione del Frame Code , e che comporta inevitabilmente l'aggiornamento del Frame Counter (RZ).

Ad esempio dalla tabella ricaviamo che possiamo scrivere e leggere dati dalla EEPROM 1senza che sia necessario introdurre alcun codice di accesso, indispensabile invece, per cancellarne il contenuto. Quest'ultima operazione richiede

FRAME

MEMORY

bit 112=1

bit 113=1

configurazione

PROM

scrittura

CON BC/FZ

lettura

SEMPRE

FRAME

MEMORY

BIT112=0

BIT113=1

configurazione

ROM

scrittura

MAI

lettura

SEMPRE

FRAME

MEMORY

BIT112=1

BIT113=0

configurazione

PROM SEGRETA

scrittura

CON BC/FZ

lettura

CON BC/FZ

FRAME

MEMORY

BIT 112=0

BIT113=0

configurazione

ROM SEGRETA

scrittura

MAI

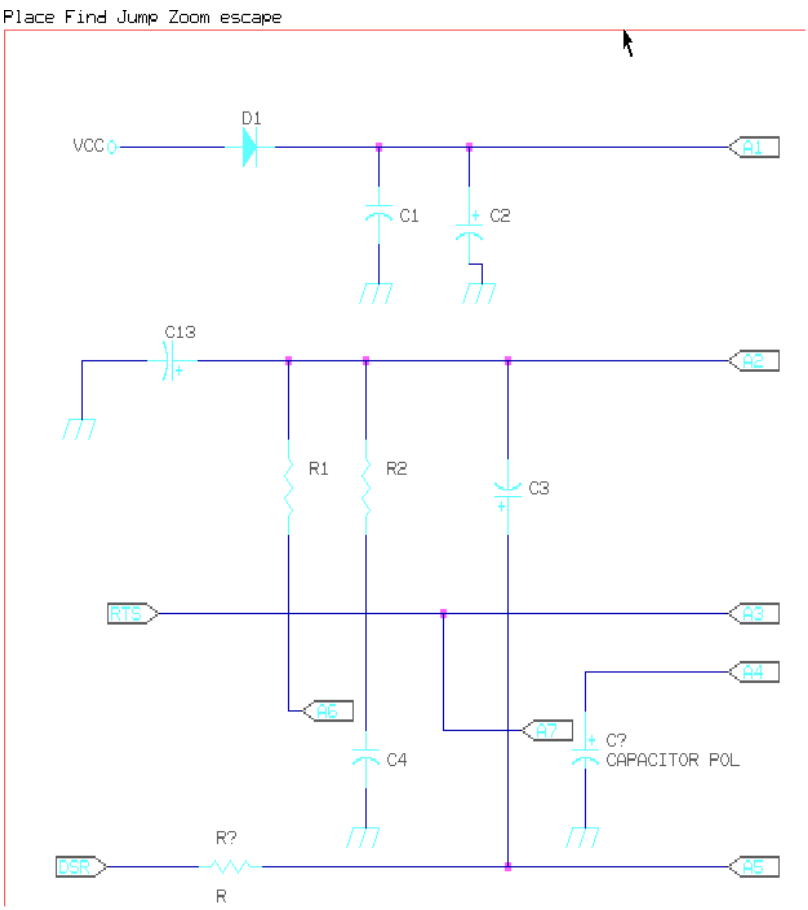
lettura

CON BC/FZ

l’introduzione ed il confronto dell’User Code e comporta il decremento dell’Error Counter .

Il Manifacturer Code è un codice dato dal fabbricante che, una volta scritto, non può più essere ritoccato, ma soltanto letto. In questa frazione di memoria che è una PROM il costruttore può inserire dati quali la scadenza della scheda, oppure può essere inserito il numero seriale, utile per identificare le varie chip card emesse da una fabbrica o da un istituto di credito. La parte di memoria riservata al Manifacturer Code corrisponde ai primi 16 bit (address 0-15). Il secondo pezzo della parte di memoria non scrivibile (ROM) è composto da 48 bit (indirizzi 16 -63) ed ospita l’Application ROM, cioè un secondo codice o comunque una ulteriore informazione sull’utilizzo la destinazione della chip card. Ad esempio l’application ROM può distinguere una partita di carte dall’altra : in pratica se un fornitore di servizi vuole distinguere quelle destinate

ad un uso da quelle fornite per una seconda applicazione può richiedere al fabbricante le carte, con lo stesso Manifacturer Code ma con differenti codici in Application ROM . Dall'indirizzo 64, ovvero dal sessantaquattresimo bit in poi,la memoria può essere letta e scritta a piacimento, in modo da poter introdurre dati di funzionamento, codici personali, valori da azzerare, ecc. La restante memoria (bit da 64 a 415) è organizzata, ovvero ripartita dalla logica di sicurezza, in 7 segmenti che analizziamo ora nei dettagli. Dall'indirizzo 64 al 79 abbiamo 16 bit utilizzabili per scrivere il cosiddetto User Code


Place Find Jump Zoom escape
D1
VCC
A1
C1
C2
C13
A2
R1
R2
C3
RTS
A3
A4
A6
A7
C?
CAPACITOR POL
C4
R?
DSR
A5
R