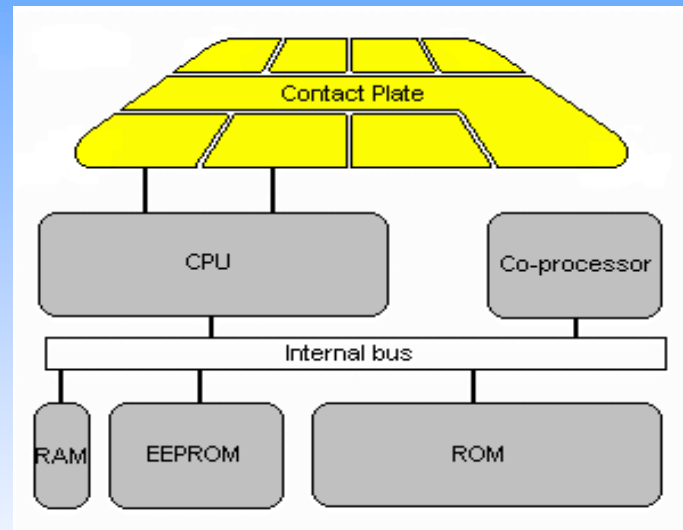


L'architettura generale



Le componenti delle smart cards (1/4)

- La parte plastica (resistente, elastica, economica).
- Materiali più usati: PVC, ABS, Melinex, ecc.
- Il processore è di tipo CISC con clock a 5 Mhz (tipico).
- Le Java card portano verso architetture a 32 bit.

Le componenti delle smart cards (2/4)

- ROM: Read Only Memory
 - Contiene il sistema operativo della smart card e programmi “fissi”.
 - Dimensione variabile tra 2k e 64k.
 - Dopo la scrittura non è modificabile.
- PROM: Programmable Read Only Memory
 - Contiene il numero seriale della smart card.
 - Molto piccola. Generalmente appena 32/64 byte.
- EEPROM: Electrically Erasable Read Only Memory
 - Memorizza informazioni variabili (tipo hard disk); capacità verso i 128k.
 - Contiene le applicazioni e i dati.

Le componenti delle smart cards (3/4)

- RAM: Random Access Memory
 - Utilizzata per memorizzazioni temporanee.
 - Si cancella quando si sfilava la smart card (power off).
 - Varia in genere tra i 128 byte e i 1024 byte.
- Interfaccia per Input/Output.
 - Spesso la velocità del flusso dati è 9600 bit/sec.
 - Vengono utilizzati due protocolli denominati T=0 e T=1
 - Vengono raggiunte velocità di 115200 bit/sec

Le componenti delle smart cards (4/4)

- Le smart card da sole sono inutilizzabili. Necessitano di un lettore.
- In verità si tratta di un lettore/scrittore.
- I lettori sono di due tipi
 - A inserzione
 - Motorizzati (Utilizzati per gli ATM)
- Alcuni lettori sono dotati di un tastierino numerico per l'inserimento del PIN.

Gli standard delle smart card (1/6)

- Questi standard sono stati sviluppati per incoraggiare l'interoperabilità.
- Gli standard più importanti relativi alle smart card sono:
 - ISO 7816
 - EMV
 - GSM
 - OCF

Gli standard delle smart card (2/6)

ISO 7816 Parte I:

- segue ISO 7810.
- Definisce le caratteristiche fisiche di una smart card.
 - Dimensioni fisiche.
 - Risposte ai raggi X e alla luce UV.
 - Resistenza meccanica.
 - Caratteristiche dei contatti elettrici.
 - Risposte ai campi elettromagnetici e alla elettricità statica.

Gli standard delle smart card (3/6)

ISO 7816 Parte II:

- segue ISO 7811.
- Questo documento descrive:
 - Le dimensioni dei contatti.
 - Il posizionamento dei contatti.
 - Il posizionamento dell'embossing (scritte in rilievo).
 - Il posizionamento della banda magnetica.
 - La struttura del chip.

Gli standard delle smart card (4/6)

ISO 7816 Parte III:

- Un documento cruciale.
- Questo documento descrive :
 - I protocolli di comunicazione.
 - Le funzioni dei vari contatti sulle smart card.
 - Le caratteristiche elettriche di base.
 - Struttura di ATR (Answer to Reset).
- I fornitori che si dichiarano conformi agli standard ISO 7816 sono sostanzialmente conformi a queste parti I, II e III.

Gli standard delle smart card (5/6)

- Lo standard EMV (2000) “Integrated Circuit Card Specification for Payment Systems è composto da quattro documenti.
- 1 : Application Independent ICC to Terminal Interface Requirements.
- 2 : Security and Key Management.
- 3 : Application Specification.
- 4 : Cardholder, Attendant, and Acquirer Interface Requirements.

- Approfondimenti disponibili su www.emvco.com

Gli standard delle smart card (6/6)

- GSM: Global System for Mobile communication.
 - La SIM card del telefono cellulare è una smart card.
- OCF: Open Card Framework
 - rappresenta un'infrastruttura software di tipo object oriented per l'accesso alle smart card.
- PKCS#15: Cryptographic Token Information Format Standard.

Applicazioni principali delle smart card

- Telefonia
- Carte debito/credito
- Salute
- Trasporti
- Controllo di accesso
- Biometria

Obiettivi della CIE/CNS

Security

- Sicurezza fisica ai fini del riconoscimento “a vista”.
- Identificazione nel controllo d’accesso ai servizi in rete.
- Firma digitale (opzionale)

Carta dei servizi

- Nello specifico la CNS non ha i vincoli del riconoscimento “a vista”.
- Attivazione di servizi nazionali (voto, salute, controllo di accesso, ecc.) nello stesso modo e su tutto il territorio nazionale.
- Attivazione di servizi locali secondo le esigenze della PAL.

Interoperabilità

- La stessa smart card a livello nazionale.
- Indipendenza dal singolo fornitore.

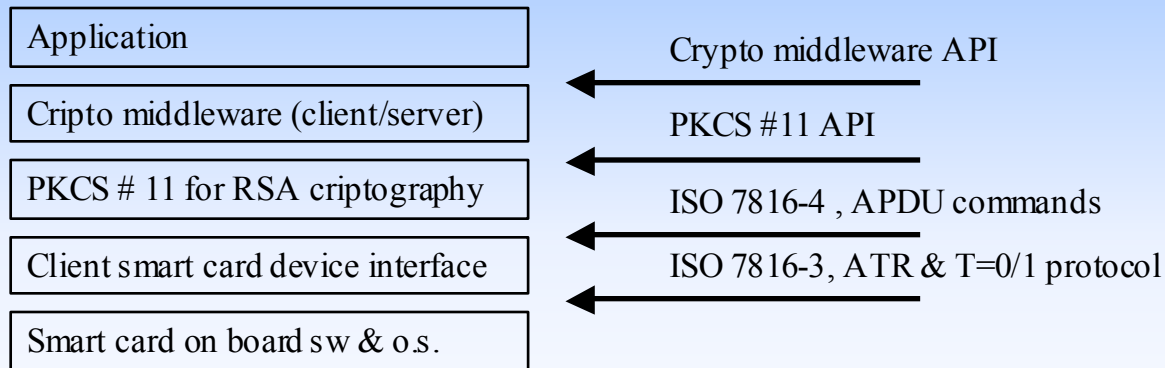
Identificazione e Autenticazione in rete 1/2

CIE/CNS e firma digitale

Bisogna garantire ai certificatori accreditati il proseguimento delle loro attività anche quando le smart card provengono da circuiti di emissione PAC/PAL.

Funzioni di autenticazione

- Viene utilizzata l'autenticazione forte, in modalità challenge-response basata su una PKI. Il certificato di autenticazione è a carico del circuito di emissione.
- E' definita una pila "di interoperabilità":



Identificazione e autenticazione in rete 2/2

- Se il servizio richiede l'installazione nella carta di strutture dati particolari (in generale EF in DF predefiniti) deve essere garantito un canale sicuro tra il server e la carta utilizzando ad esempio meccanismi crittografici basati sulle session key.

Liste di revoca, OCSP e XKMS

- Con elevati numeri di carte emesse è indispensabile ripensare il modello di gestione dei certificati revocati.
- E' bene ricordare che i certificati revocati sono anche quelli delle smart card guaste o danneggiate con l'uso.

Portabilità e interoperabilità 1/2

- Accordo in fase di definizione con TUTTI i produttori di smart card
- Alcuni elementi tecnici:
 - Alimentazione: 5 volt
 - Protocollo: T=1
 - Velocità: procedura ISO PPS da 115kbps (utilizzo del DIV secondo ISO 7816-3)
 - ATR: da registrare a cura di...

Portabilità e interoperabilità 2/2

- Modifica (verso gli standard ISO 7816) di alcune APDU
- Introduzione della APDU “CHANGE KEY DATA” per evitare la gestione delle chiavi DES e RSA, in modo improprio, con il comando “CHANGE REFERENCE DATA”.
- Utilizzo di EXTERNAL AUTHENTICATION per le operazioni di aggiornamento della carta nelle applicazioni “post emissione”.
- Nuovo manuale delle APDU all’inizio del 2003.

Vincoli sul file system della carta

- Quanto fatto per la CIE rimane inalterato (autenticazione e Netlink).
- Bisogna porre dei vincoli per la firma digitale.
- PIN e PUK dedicati alla funzione
- Il file system subisce i vincoli derivanti dalla certificazione necessario per disporre del “dispositivo sicuro per la creazione della firma” previsto dalla direttiva 1999/93/CE.

manca@aipa.it 06-85264431

Grazie per l'attenzione

