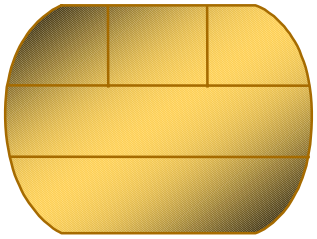
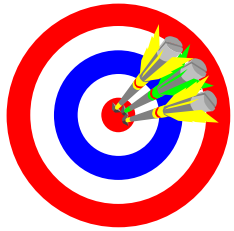
Smart Cards - An Introduction



Rayees Shamsuddin
Oregon State University
23 April 1999

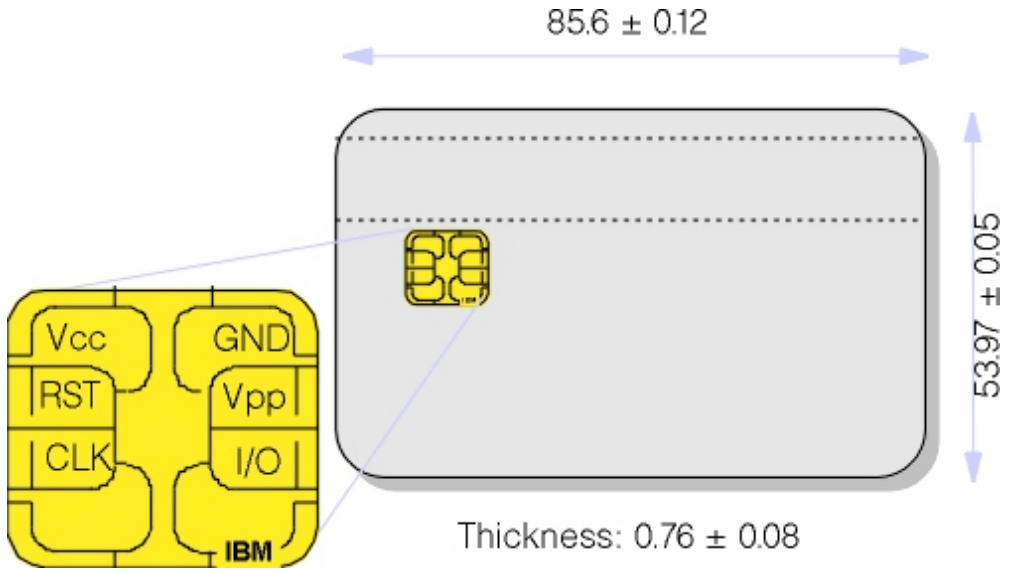
Objectives



- What is a Smart Card?
- Different Types
- Inside the SmartCard
- Standards
- Cryptography
- Java Cards, IButtons, ...
- Applications

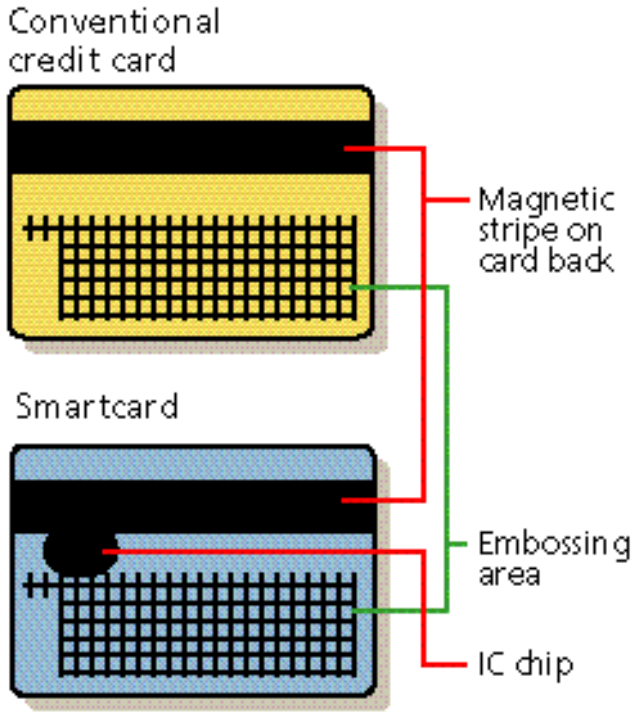
What is a Smart Card?

- Surface contacts (8)
- < 25 mm² Silicon chip
- Micro-controller:
  - Mostly 8-bit today,
  - 32-bit RISC tomorrow…
- Non-volatile memory:
  - < 16Kbytes EEPROM today,
  - 32K Flash and above tomorrow
- Credit-card-sized plastic card (PVC, ABS…)



Advantages of SmartCards

- More reliable
- Store more information
- Difficult to tamper
- Incorporates cryptography
- Can perform multiple functions
- Compatible with portable electronic devices (phone, PDAs, PCs)
- Can be disposable or reusable
- Reduces fraud



Fraud in Magnetic Stripe Cards

- ***Theft:*** Cards can be stolen. Temporary offline ATMs may be used for finding PIN…
- ***Counterfeit:*** Read another legal card and encode the same sequence on the magnetic tape. PIN can be searched with multiple copies
- ***Buffering:*** To avoid card limit in cash withdrawal, data is stored somewhere and then recovered back
- ***Skimming:*** Original data is altered or additional data is encoded

Cost Comparisons

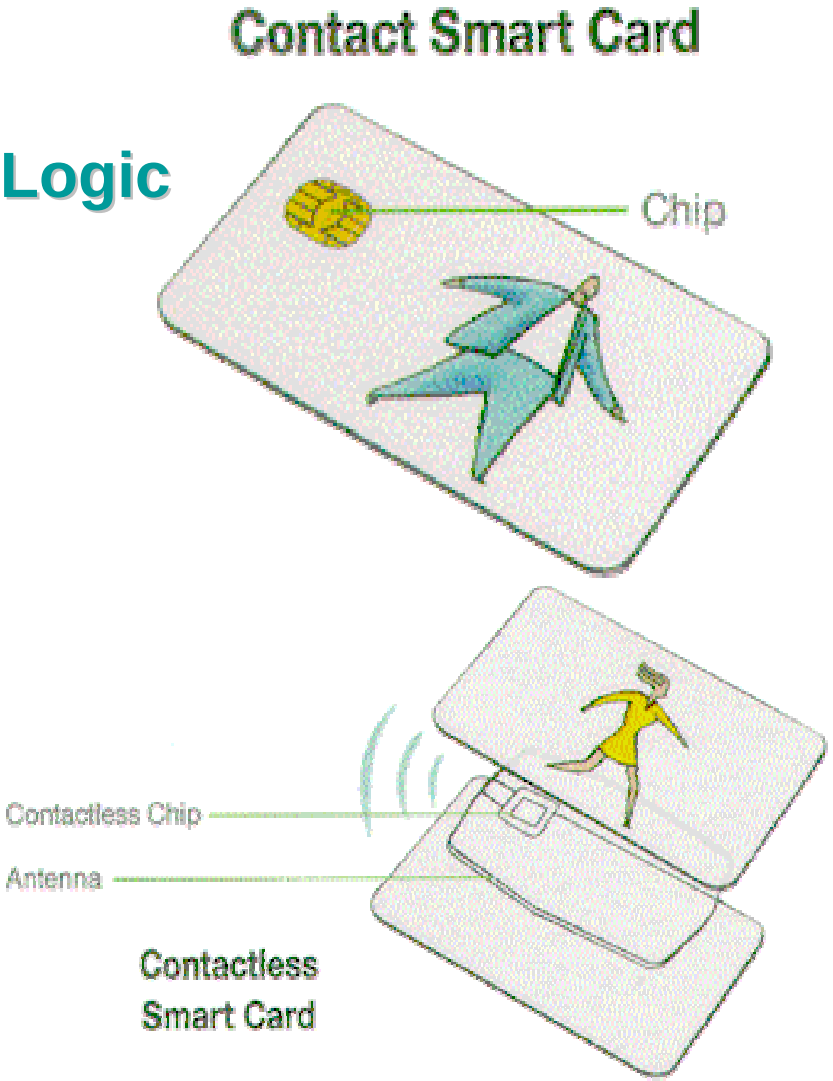
	Card Unit Price	Attached Reader	Standalone Reader
Magnetic stripe	0.15 – 0.6	15 – 20 (2 tracks) 25 – 30 (3 tracks)	150 – 600 (PC) 300 – 1000 (POS) 10,000 (ATM)
Optical	4 – 8	N/A	800 - 3000
Chip Cards		3 - 10	100 – 200 (PC)
Memory:	0.5 – 5		300 – 800 (POS)
Smart:	3 – 15		
Super Smart:	20 – 50		
Contactless:	5 - 20	N/A	500 – 900

Different Types of SmartCards

- Memory cards
- Memory with Security Logic
- Processor cards

- Contact cards
- Contactless cards

- Hybrid cards
- Dual Interface cards
- Optical cards



Smartcard Contacts

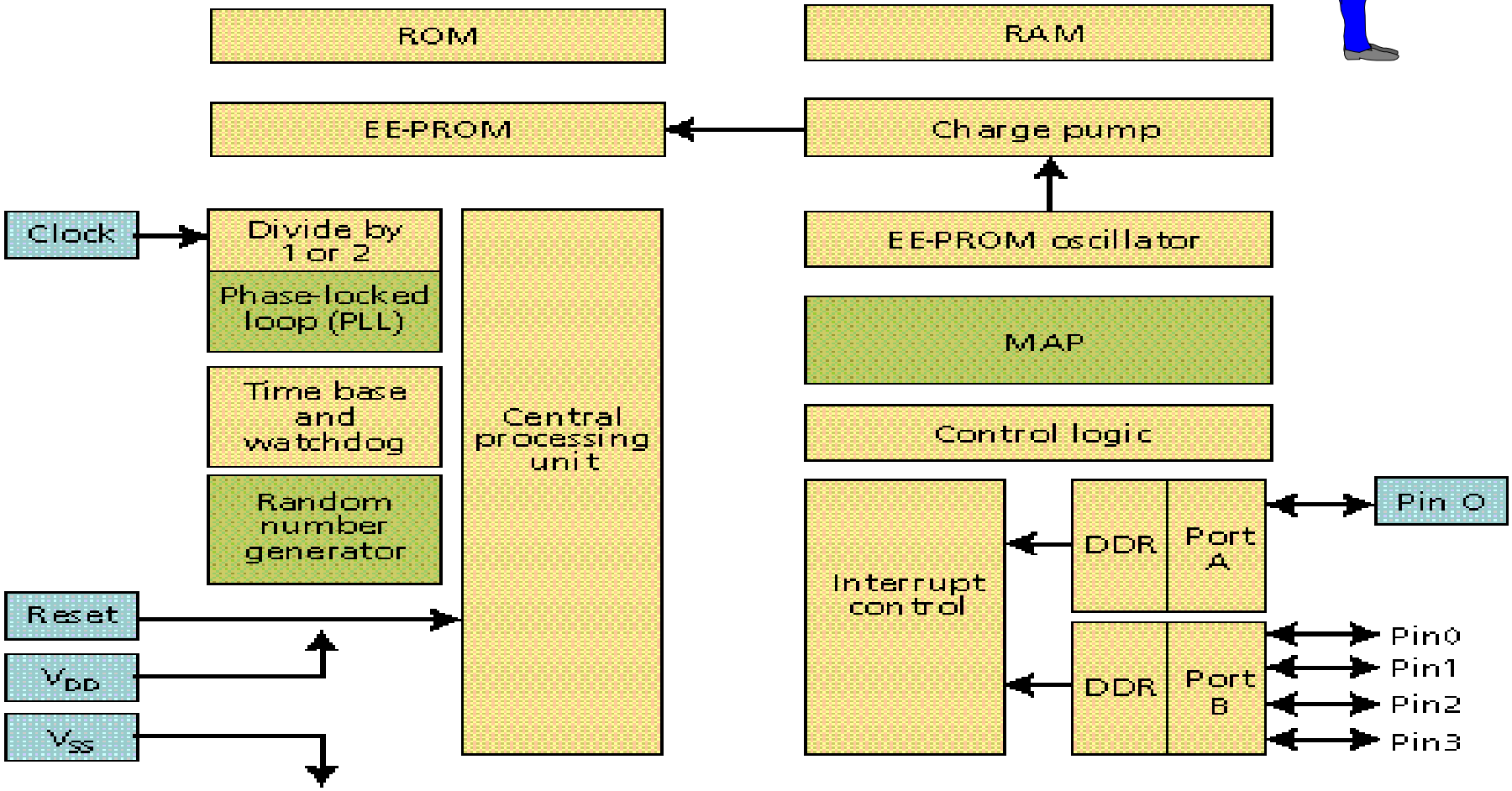
Smartcards have either 6 or 8 contacts (2 are reserved for future use).ISO 7816 Part 2 and 3 describe the functions of the remaining contacts.

- **C1 :** is used for power supply input (V_{cc}) from the interface device. 5V(3V in future)
- **C2:** is called RST and is used by the interface device to send reset signals to the card microcircuit
- **C3:** called CLK and timing signals are send to the card through it (3.5795 MHz and 4.9152 MHz)

Smartcard Contacts contd..

- **C5:** is used as a reference voltage and is called ground (0 V)
- **C6:** optionally used to program (record) or erase the internal non volatile memory. (V_{pp})
- **C7:** performs communication to and from the card. Data flows depends on the mode: reception mode for input and transmission mode for output
- **C4 and C8:** Reserved for future use

Inside the SmartCard



DDR = data direction register
EE-PROM = electrically erasable programmable ROM
MAP = modular arithmetic processor

Inside the SmartCard contd...

- **Volatile Memory:** RAM retains data only while power is applied, so is used as a scratch pad by the CPU for its calculations; 1280 Byte for Siemens SLE66C80S
- **Nonvolatile Memory:** Permanent Information is stored in ROM. Program/data is stored here; 8 KB typical
- **User/Application Memory (UAM):** holds user data, issuer data and operations(transactions) performed by the card. This area is protected by the microprocessor.

Inside the SmartCard contd...

- **CPU :** The CPU executes an instruction set that defines the capabilities of the card. Available architectures are: H8/310 (Hitachi), 627xx (Oki), ST8 (Thomson), 8051 (Intel) and 6805 (Motorola). All employ 8 bit instructions and 16 bit data bus. Gemplus introduced RISC processor

- **Operating System :** allows the CPU to manage the UAM according to external commands the user invokes from an interface device

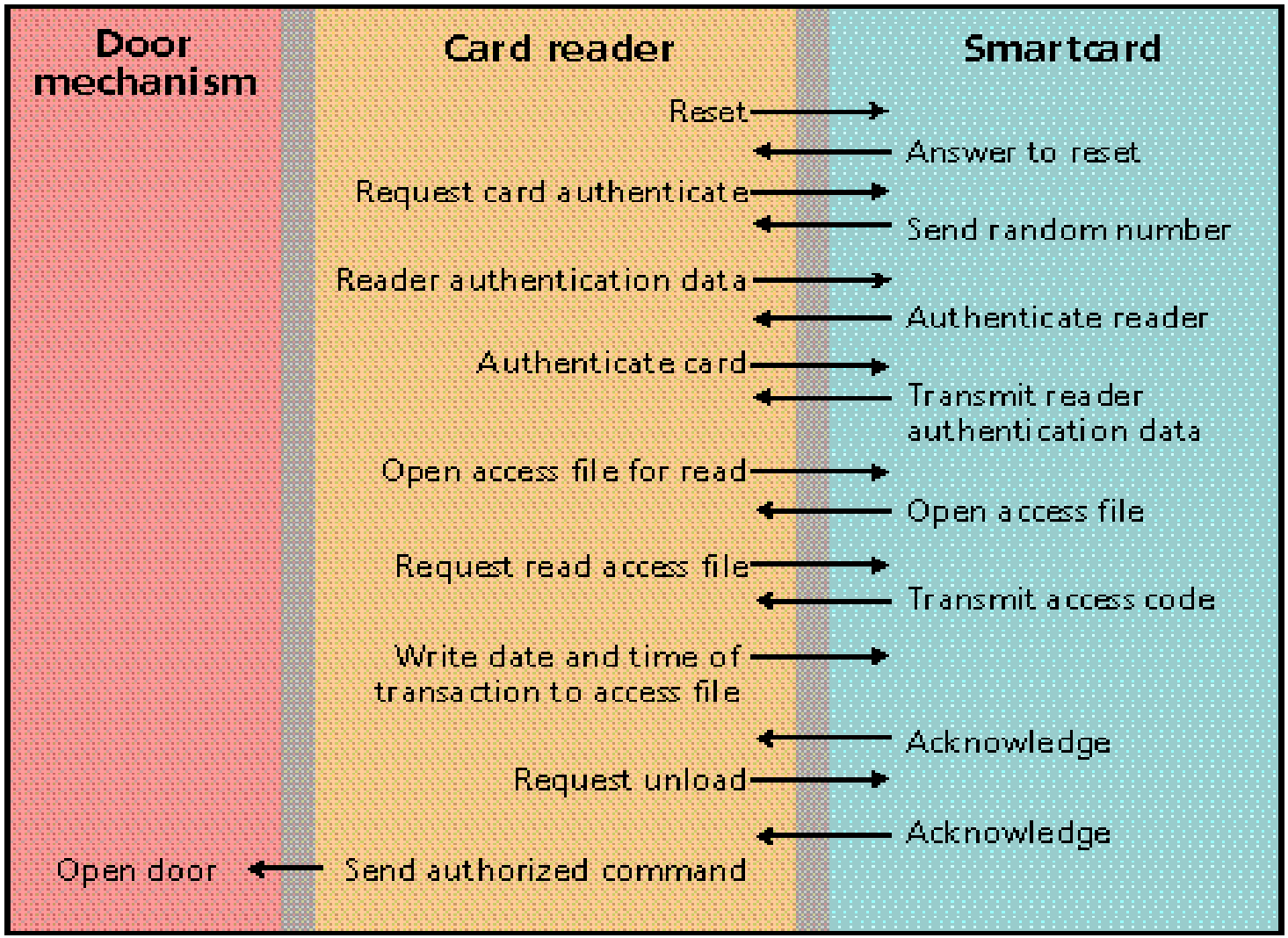
Inside the SmartCard contd...

- The **charge pump** raises the voltage as needed to write to the EE-PROM. On some devices [lightly shaded], a **co-processor** enhances performance of the encryption or decryption algorithm. The **phased-lock loop** increases the externally provided clock frequency for internal use in the **modular arithmetic processor** (MAP), an accelerator that optimizes calculations used for encryption and decryption algorithms. Numbers created by the **random number generator** serve as the algorithm's keys or seeds.

Smart card - card reader interface

- Ensures that both the card reader and the smart card are authorized to undertake operations. When the reader has a card inserted in it, it resets the card, which responds with an answer to reset (ATR). Its ATR provides specific information and often conforms to the ATR described in the ISO 7816 standard. Both the reader and the card use a random number in an algorithm to obtain a result that, when successfully compared, authorizes the card and the reader to continue with the desired operation.

Smart card - card reader interface



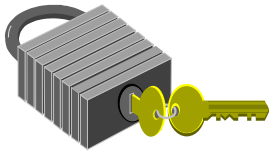
SmartCard Standards

- **ISO 7816:** Covers all smart cards and applies to all application sectors
- **European Standards (CEN 726):** is targeted on the intersector electronic purse applications
- **EMV :** concerning the major debit/credit cards - Visa, Mastercard, Europay (1993)
- **ETSI :** digital telecommunications sector, GSM
- **SET :** Secure Electronic Transaction(SET) for the electronic commerce sector
- **C-SET :** Chip-Secure Electronic Transaction (France)

ISO Standards for identification cards

- **ISO 7810** - Physical Characteristics
- **ISO 7811** - Recording Techniques (six parts)
- **ISO 7812** - Identification of issuer (two parts)
- **ISO 7813** - Financial Cards
- **ISO 7816** - IC Cards with contacts (six parts)
- **ISO 10873** - Test methods
- **ISO 10536** - Contactless (close coupling) IC Cards (four parts)
- **ISO 14443** - Contactless (remote coupling) IC Cards (four parts)

Why is a SmartCard secure?



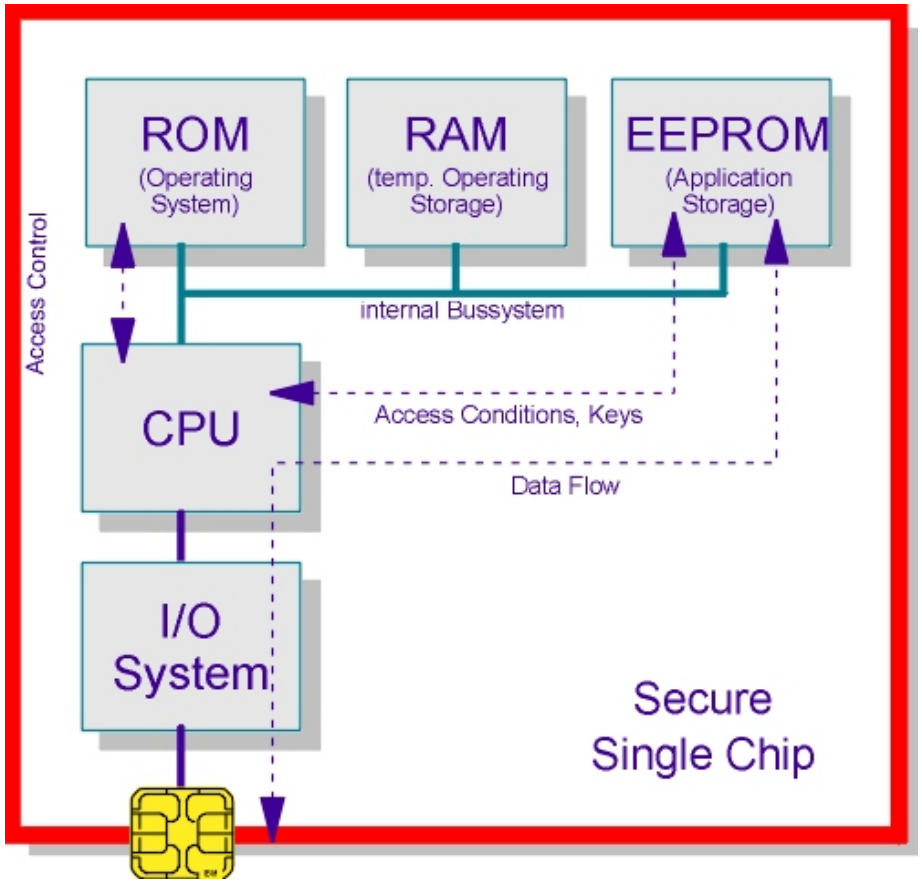
Controlling access to information

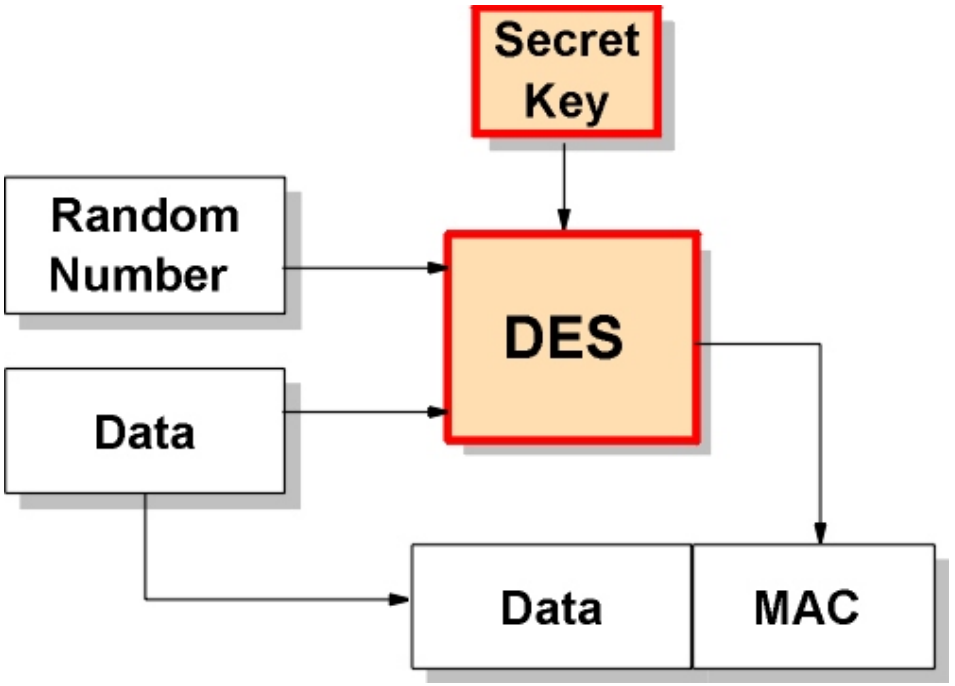
- Who Can Access Information?
  - ☆ Everybody
  - ☆ Card Holder only
  - ☆ Third Party only
- How Can Information be accessed?
  - ☆ Information which is read only
  - ☆ Information which is added only
  - ☆ Information which is updated only
  - ☆ Information with no access available

Card Chip Security

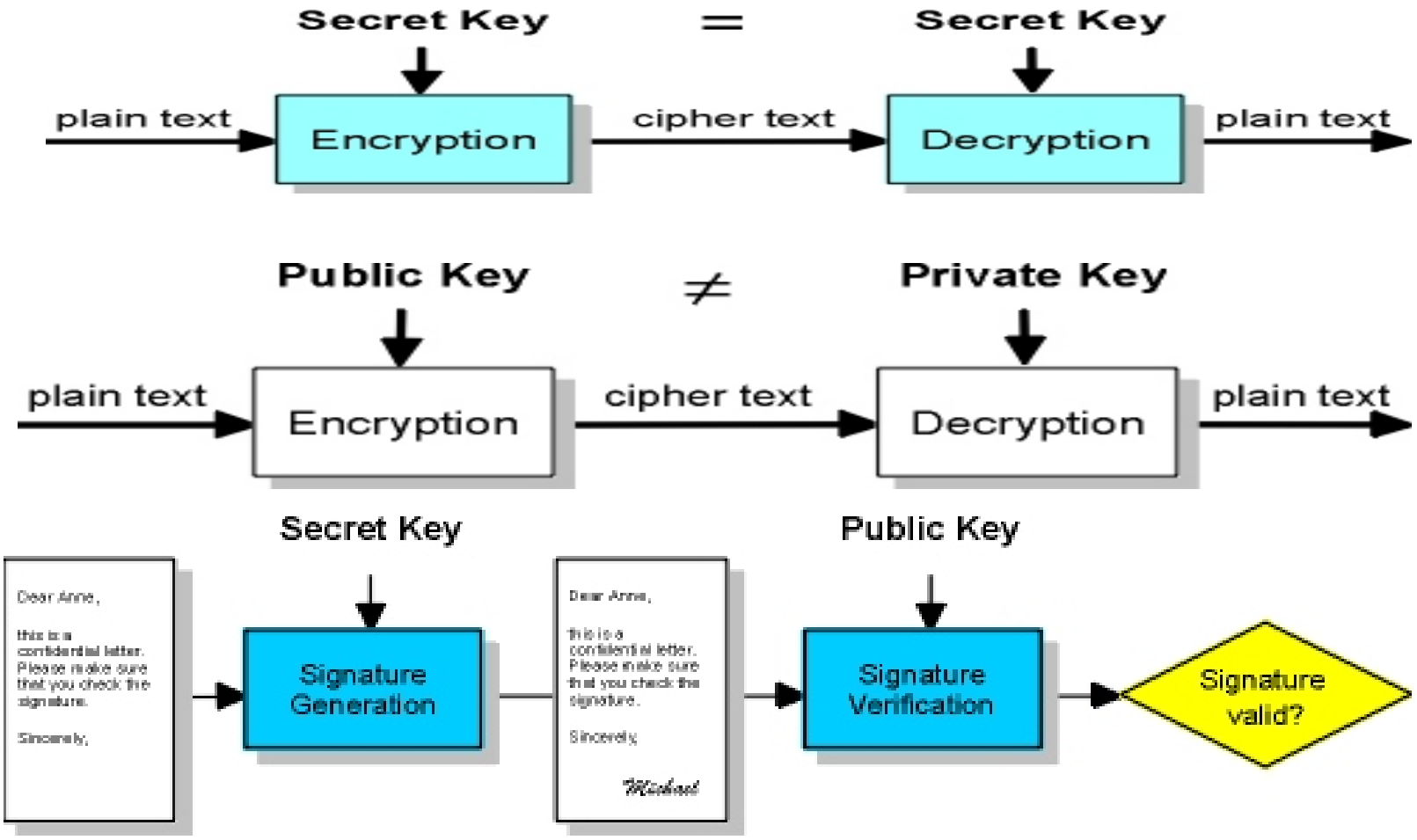
- **Power Consumption:** Instruction sequences can be tracked. Prevents by generating erratic consumptions or by performing dummy operations
- **Chip Extraction:** should refuse to work when encapsulation protection is removed
- **Low/High Voltage:** Sudden change in power supply voltage may cause the card to give access to forbidden areas. Provide with reference voltage
- **Partial erasing:** Card memory is scrambled to prevent erasure by focussed beams. Also sentinel bits are randomly placed in the memory area

Cryptography in SmartCards





Cryptography in SmartCards (contd.)



Implementation Constraints

- 108 - 1024 bytes of RAM
- 1 - 16 kB of EEPROM
- 6 - 16 kB of ROM
- 8 bit CPU 3.57 MHz clock
- slow transmitters; data passed between card and terminal is very slow

The Solution - ECC

- Small key and Certificate sizes mean less EEPROM is required; also less data to be transmitted
- Scalability
- No coprocessor required
- Low cost
- On card key generation

Applications

Debit / Credit cards

Electronic Purse

Proton, VisaCash (UK, USA, Sweden, Australia, Spain), Clip(Italy), Mondex (UK, USA, Canada, HongKong, NewZealand

Electronic Commerce

Transport

Applications (contd…)

Health

Telecommunications

Loyalty

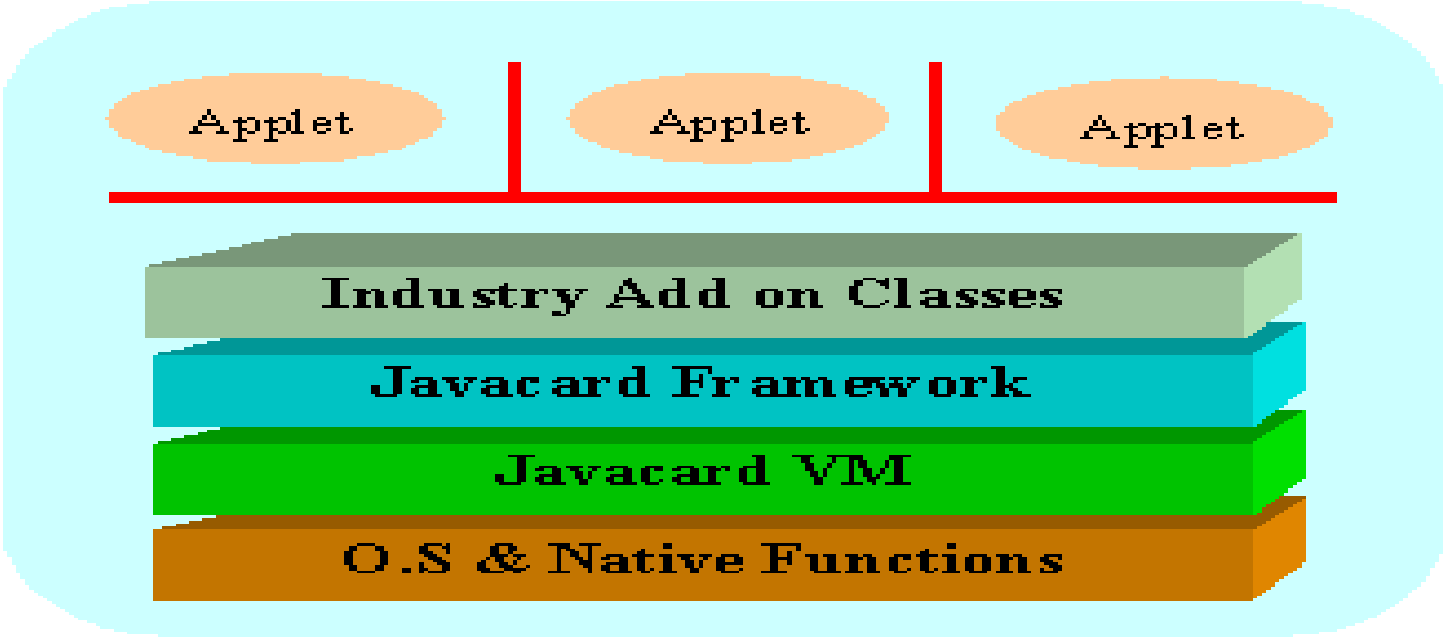
Television

Some Smartcard Projects

Program (locations)	No. of cards, status	Date begun
Mondex (worldwide)	50,000	1992
Danmont (Denmark)	1 000 000	1993
Proton, Cash, ChipKnip (worldwide)	2 000 000 in 1996; 12 000 000 in 1997	1994
Visa Cash (worldwide)	2 000 000	1996 pilot at Atlanta Olympics
Clip (pan-European)	50 000	1996
NYC pilot 50 000 1997	50 000	First to accept both Visa Cash and Mondex

JavaCard

- JavaCard is a smart card that is capable of running Java programs. Minimum system requirement is 16K ROM, 8K EEPROM and 256 bytes of RAM



IButtons and JavaRings

IButtons - Dallas Semiconductor

16mm computer chip housed in a stainless steel can

- different types
  - password protected
  - clock
  - monetary
  - cryptographic
- Cryptographic IButton uses Java VM or Dallas O/S; can be used for secure e-mail, remote login authentication and e-commerce