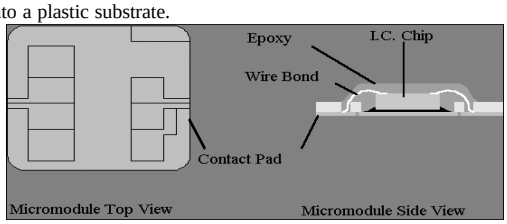
Smart Cards

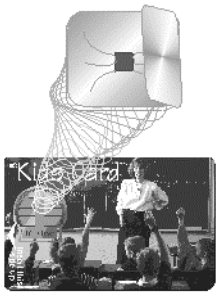
Introduction to Smart Cards

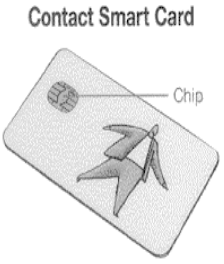
- Smart card is a credit-card sized plastic card that can store and process information on tiny microprocessors (or chips) embedded within them.
- There are two types of smart cards: **memory cards** and **intelligent cards**.
- The chip can either be a microprocessor with internal memory or a memory chip with non-programmable logic.
- The chip connection is either via direct physical contact or remotely via a contact less electromagnetic interface.

Two another general categories of smart cards: *contact* and *contact less* smart cards.

A **contact smart card** requires insertion into a smart card reader with a direct connection to a conductive micro module on the surface of the card (typically gold plated). It is via these physical contact points, that transmission of commands, data, and card status takes place. Below is a contact micro module which is embedded into a plastic substrate.







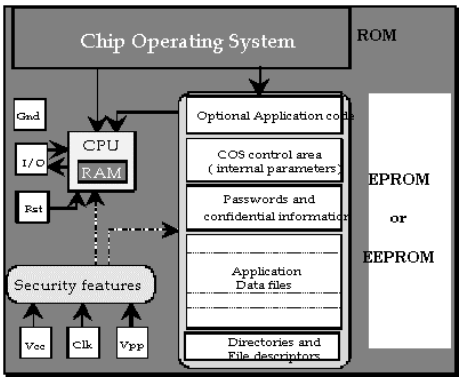
A **contact less card** requires only close proximity to a reader. Both the reader and the card have antenna and it is via this contact less link that the two communicate. Most contact less cards also derive the internal chip power source from this electromagnetic signal. The range is typically two to three inches for non-battery powered cards, and this is ideal for applications such as mass transit which require very fast card interface.

This diagram shows the top and bottom card layers which sandwich the antenna/chip module. The antenna is typically 3 - 5 turns of very thin wire (or conductive ink), connected to the contact less chip.

- **Memory cards** are primarily information storage cards with some type of stored value that the cardholder can "spend." Many of the prepaid telephone cards available today are memory-only cards, and are disposed when all the value is used.
- **Intelligent cards** contain an integrated circuit (IC) microprocessor that not only lets them store information but also act on it intelligently. These smart cards can do encryption/decryption. These smart cards can have information added or deleted, as required. These smart can be reloadable with new data.

- Memory cards can hold from 103 bits to 16,000 bits of data. They are less expensive than microprocessor cards but with a corresponding decrease in data management security. They depend on the security of the card reader for their processing and are ideal when security requirements permit use of cards with low to medium security.
- SISHELL is a tamper-resistant layer placed over the smart card chip by the card manufacturer.

- A microprocessor chip can add, delete and otherwise manipulate information in its memory. It can be viewed as a miniature computer with an input/output port, operating system and hard disk. Microprocessor chips are available 8, 16, and 32 bit architectures. Their data storage capacity ranges from 300 bytes to 32,000 bytes with larger sizes expected with semiconductor technology advances. Their ability to download not just data but applications is being advanced by Sun with Java Card technology and Mondex with Multos.



Smart Card Applications Include:

Payment vehicles: smart card technology allows credit and debit transactions to be made in a much more secure environment. Electronic purse and stored value cards provide great convenience to the customer. There are over 100 countries world wide who have reduced or eliminated coins from the pay phone system by issuing smart cards.

Information managers: smart cards can manage large amounts of information with maximum security and privacy protection.

Smart Card Applications Include: (contd.)

Access keys: smart cards provide the most secure environment for transaction authorization, storage of information, and delivery of financial transactions and other information in both an on-line and off-line environment. They also serve as "keys" for secure access to buildings and even access to networks and software programs. Smart cards are the ideal vehicle to provide secure access to Internet and home banking services.

Reward cards: Electronic coupons and gift certificates can be stored on the card as well.

Different Smart Card Readers

Major Benefits

- Reduced paperwork
- Potential of having one card with ability to access multiple services, networks, internet, etc.
- Fraud reduction
- Ability to manage or control expenditures more effectively
- Access control for buildings or computer systems, etc.
- Storage of large information like emergency medical information
- Ticket less travel on airlines, subways, buses, trains, etc.
- Unscrambling of cable or satellite signals
- The smart card readers are becoming easily available for PCs.

Block or Unblock A Smart Card

- The terminal or host computer can block or unblock a smart card by setting some flags. It can block the application or entire card. E.g.,
  - Failure of Authentication
  - Invalid PIN
  - Insufficient Balance
  - Expired Date
- Some cards can commit suicide, some can be killed by the terminal or host computer, some can be temporarily blocked and can be reset.

SMART CARD PROTOCOLS

- Majority of microprocessor smart cards today use single bi-directional serial I/O
- The standard for this is set by ISO 7816-3: asynchronous character-oriented protocol.
- The terminal starts by "waking up" the card by applying power followed by a reset (RST) signal.
- The card responds with an answer to reset (ATR), which tells the terminal what type of card it is and which communication protocol it will use.

CHIP Security Features

- Electron microscopes inspect the physical structure of the chip
- To protect against this tamper resistance layers may be added over the whole chip
- It includes some links into main circuitry so that any attempt to remove this layer destroys the chip
- One advantage of smart card based systems is that it allows **challenge and response** authentication instead of simple password
- Unlike a password, the response is never the same which defeats many potential attacks
- Access control can be a combination of a token (the smart card) and a password or biometric

CHIP Security Features (contd.)

- When the card is challenged it asks for and checks the password or PIN before issuing the response
- Neither stealing the token nor gaining access to the password on its own is enough to gain access to the system
- Cards are blocked by sending the card a sequence of wrong PINS, until the card refuses to accept any more attempts
- To unblock, the card issuer should give the cardholder a PIN unblocking key (PUK)
- This key (previously stored in the card) allows the PIN try counter to be reset only once

PIN in Magnetic Stripe Cards

- Magnetic stripe cards usually hold a PIN for the cardholder to prove his/her identity.
- An enciphered version of the PIN is stored in one of the card tracks.
- Card security relies on an external system (a networked computer or an off-line EPOS), it is the system's responsibility to allow the transaction to progress.
- The enciphered version of the PIN is read; the user is requested to enter the PIN, and the external system performs a number of operations using the PIN and one or several secret numbers carefully hidden in the system's memory.

PIN in Magnetic Stripe Cards (contd.)

- The result of such operations is then compared to the card's enciphered PIN. If both match, the transaction is permitted.
- The weakest point of this scheme is interchange. ATMs from different financial companies and off-line EPOSs manufactured by others must share their enciphering keys for any system to manage someone else's cards.

Message Encryption and Decryption

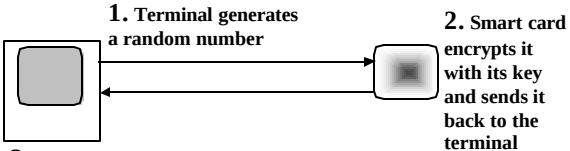
- **Encryption** - an enciphering procedure to make a message meaningless to everyone except those who have the required keys. Decryption is an opposite procedure of encryption.
- In **symmetric cryptosystem**, there is one secret key, which is shared by the sender and the recipient of the message. The same key is used to encrypt and decrypt the message. Confidentiality is guaranteed as long as the key is kept secret. Best example is DES (Data Encryption Standard). It is commercially available by NIST. Algorithm is based on a technique which provides 2^{56} possible combinations.

Message Encryption and Decryption (contd.)

- Another process, called **challenge**, is used by the card to verify that the external system is authorized to work with it, or vice versa. The card challenges the system by generating a random number and sending an encrypted version to the external device. The system must decrypt the number and give the correct answer back to the card. This can only be achieved if the system holds the same keys as the card. The challenge may also be initiated by the system to verify the card.
- In **asymmetric cryptosystem**, two keys are used. The first one called the *private key*, is known to user only. The second key, called the *public key*, is publicly known. Every user has a private and a public key. These keys are linked to each other: one is used for encryption and other for decryption.

Challenge & Response

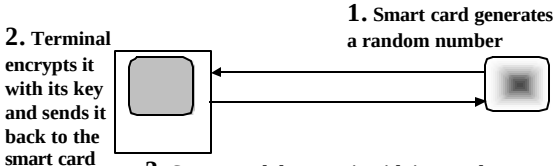
• Terminal Challenges the Smart Card



3. Terminal decrypts it with its own key. If the number is same as it is generated by the terminal's random number generator, It will authenticate the smart card.

Challenge & Response (contd.)

• Smart Card Challenges the Terminal



3. Smart card decrypts it with its own key. If the number is same as it is generated by the smart card's random number generator, It will authenticate the terminal.

Computer System Access

- When the card is inserted the system asks for user ID, it may be given by card or system, the system then authenticates the card
- The use of random or time-dependent functions is important to prevent replay attacks
- Smart cards are more expensive than all other forms of cards used for access control, but their advantage lies in their ability to operate offline and its security
- In buildings where all locks can be linked to a single computer system, online biometrics are a very attractive solution