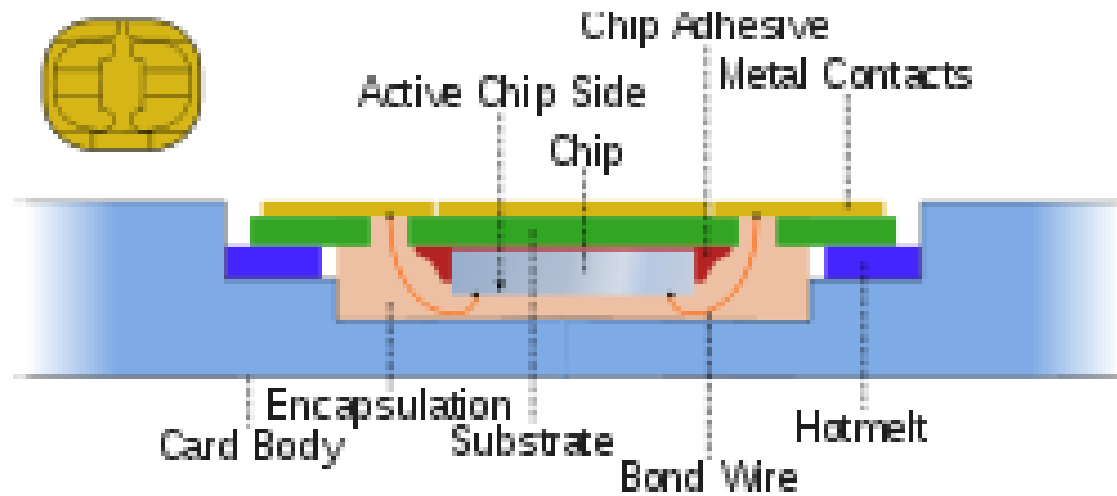




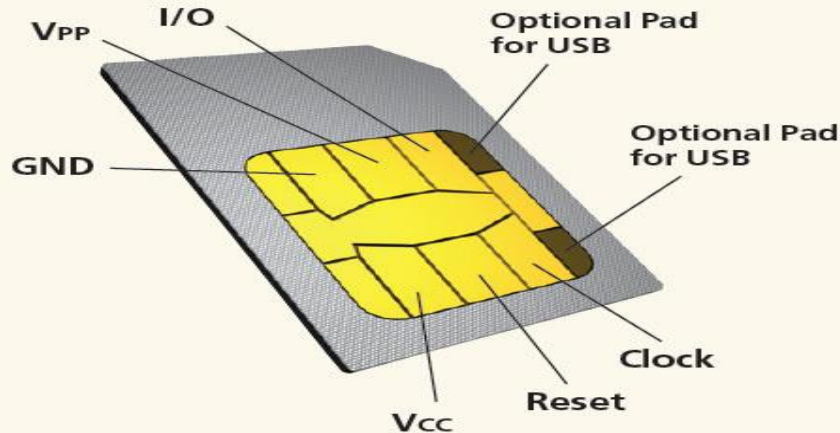
Smart cards

Contact Smart Cards :



Contact smart cards have a contact area of approximately 1 square centimeter (0.16 sq in), comprising several gold-plated contact pads. These pads provide electrical connectivity when inserted into a reader.

How to use signals :



- VCC - power supply
- RST - Reset signal, used to reset the card's communications.
- CLK - Provides the card with a clock signal, from which data communications timing is derived.
- GND - Ground (reference voltage).
- VPP - Programming voltage input - originally an input for a higher voltage to program persistent memory (e.g., EEPROM), but now deprecated.
- I/O - Serial input and output (half duplex).
- C4, C8 - The two remaining contacts are AUX1 and AUX2 respectively, and used for USB interfaces and other uses.

Reader


- Contact smart cards readers are used as a communication medium between the smart card and a host or a mobile telephone this are used subscriber identity modules(Sims)in mobile phone

Applications :

- First introduced in Europe smart cards debuted as a stored value tool for payphones to reduce theft.
- smart cards and other chip-based cards advanced, people found new ways to use charge cards for credit purchases and for record keeping in place of paper.
- In the U.S., consumers have been using chip cards for everything from visiting libraries to buying groceries to attending movies
- Many industries have implemented the power of smart cards in their products, such as the GSM digital cellular phones as well as TV- satellite decoders.

Why can be use smart cards :

- Smart cards improve the convenience and security of any transaction.
- Smart card systems have proven to be more reliable than other machine-readable cards, like magnetic stripe and barcode,
- Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network.
- To making smart cards a cost-effective solution in these environments.
- Multifunction cards can also be used to manage network system access and store value and other data.

- 
- **Securing digital contents & physical Assets**
 - **E-Commerce.**
 - **Bank issued smart cards.**
 - **Health care Informatics.**
 - **Embedded medical device control.**
 - **Enterprise and Network security.**

Physical access:

Businesses and universities of all types need simple identity cards for all employees and students. Most of these individuals are also granted access to certain data, equipment, and departments according to their status.

Security :

- Security is basically the protection of something valuable to ensure that it is not stolen, lost, or altered.
- Smart cards provide computing and business systems the enormous benefit of portable and secure storage of data and value.

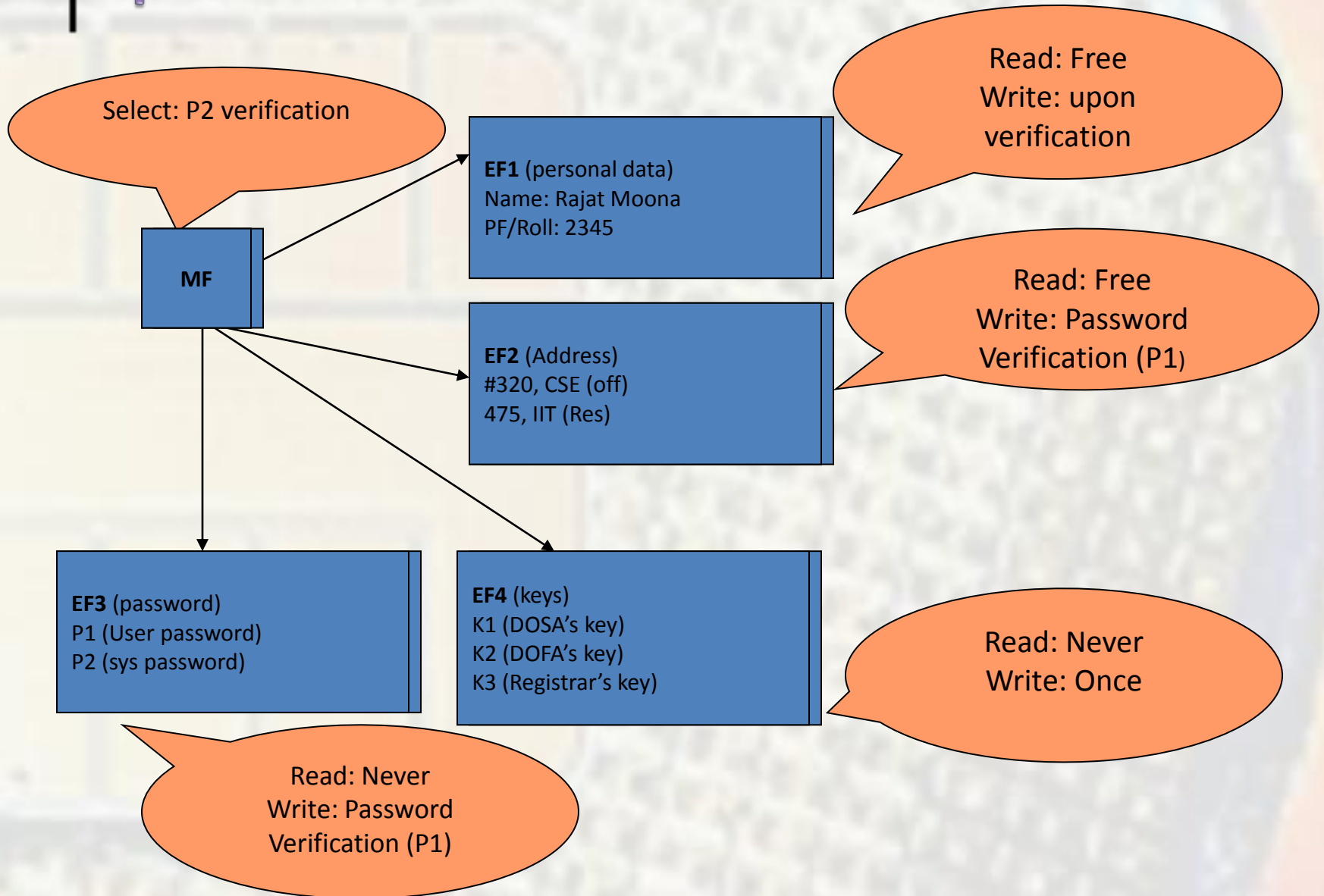
Security mechanism :

- password
- Cryptographic challenge Response
- Biometric information

password verification :

- Terminal asks the user to provide a password.
- Password is sent to Card for verification.
- Scheme can be used to permit user authentication.
- Not a person identification scheme

password verification :



Cryptography Verification :

Cryptographic smart cards are often used for single sign-on. Most advanced smart cards include specialized cryptographic hardware that uses algorithms such as RSA and DSA.

- Terminal verify card (INTERNAL AUTH)
- Terminal sends a random number to card to be hashed or encrypted using a key.
- Card provides the hash or cyphertext.
- Terminal can know that the card is authentic.
- Card needs to verify (EXTERNAL AUTH)
 - Terminal asks for a challenge and sends the response to card to verify
 - Card thus know that terminal is authentic.
- Primarily for the “Entity Authentication”

Biometric techniques:

- Finger print identification.
- finger prints can be kept on the card (even verified on the card)
- Photograph/IRIS pattern etc.
- Such information is to be verified by a person. The information can be stored in the card securely

Standards :

International Organization for Standardization (ISO)

- ISO/IEC 7816 It contains fourteen parts. 1, 2 and 3 deal only with contact smart card. 4,5,6,8,9,11,13 and 15 are relevant to contact as well as contactless.
- ISO/IEC 14443: It defines the interfaces to a "close proximity" contactless smart card, including the radio frequency (RF) interface.

Federal Information Processing Standards (FIPS)

- FIPS 140 (1-3): The security requirements contained in FIPS 140 (1-3) certain Areas related to the Secure design and implementation of a cryptographic module specification; Cryptographic module ports and interfaces
- **FIPS 201** this specification covers all aspects of multifunction cards used in identity management systems throughout the U.S. government.

Conclusions:

Smart cards can add convenience and safety to any transaction of value and data. Evaluations of performance, cost and security that will produce a smart card system that fits today's needs in future, which leads to better business for everybody