Smart Identification

CSE334

Md. Ferdouse Ahmed Foysal
Daffodil International University

Smart Card

- A smart card is a secure, tamper-resistant device consisting of a single-chip microcomputer, which is mounted on a plastic card of the size of a standard credit card.
- The chip has only a size of 25 mm2 at most.

First Smart Card

- The first credit cards just had The first cards the name of the owner printed on the front.
- Later, cards with embossed printing were introduced. The embossing made it possible to take an imprint of the cardholder information instead of copying it down manually.
- A few years later, the magnetic stripe, which carries the account information and the name of the cardholder, was introduced. This made the card machine-readable: Now the information could be electronically processed. Still, one problem remained: Everybody with the necessary equipment can read and write the data on the magnetic stripe. This led to a fraud problem.

First Smart Card

- In 1968, a patent for an identification card with an integrated circuit was filed, and the smart card was born (RAN98).
- An important characteristic of a smart card is that the information on it cannot be copied.
- A credit card's magnetic stripe can easily be copied and then be misused. This could never happen with a smart card-based credit card.

Usage of Smart Card

- Today every mobile phone that complies with the GSM standard contains a smart card that authenticates the owner.
- In a building access system, the card can be used to store the data required to open a door. The same data can later authenticate the employee to his computer. Or it can be used for payment in the company‘s cafeteria.
- In home banking applications, the card can be used as a secure token to authenticate the user over a public network between the user’s computer and the bank's system. This is more secure than using today’s passwords.
- In a multi-company loyalty scheme, the card can store the loyalty points that the customer already earned.
- In a mass-transit system, the card can replace paper tickets. The fare can be calculated based on the distance. This can be done at the time the customer leaves the public transport system, and the fare can be deducted from the card on the spot. Using a contactless card, the traveler could even leave the card in his pocket.

Contact and Contactless Smart Cards

- Contact - The chip communicates with external devices through a direct physical connection, for example, the card is inserted into a terminal.
- Contactless - The chip communicates with external devices using radio frequency identification (RFI) or radio waves, so no physical connection is necessary, for example. the card is “waved” in the proximity of the terminal.

Contact and Contactless Smart Cards

- Contact: Cards the size of conventional credit or debit card with a single integrated circuit chip that contains just memory or memory plus a microprocessor.

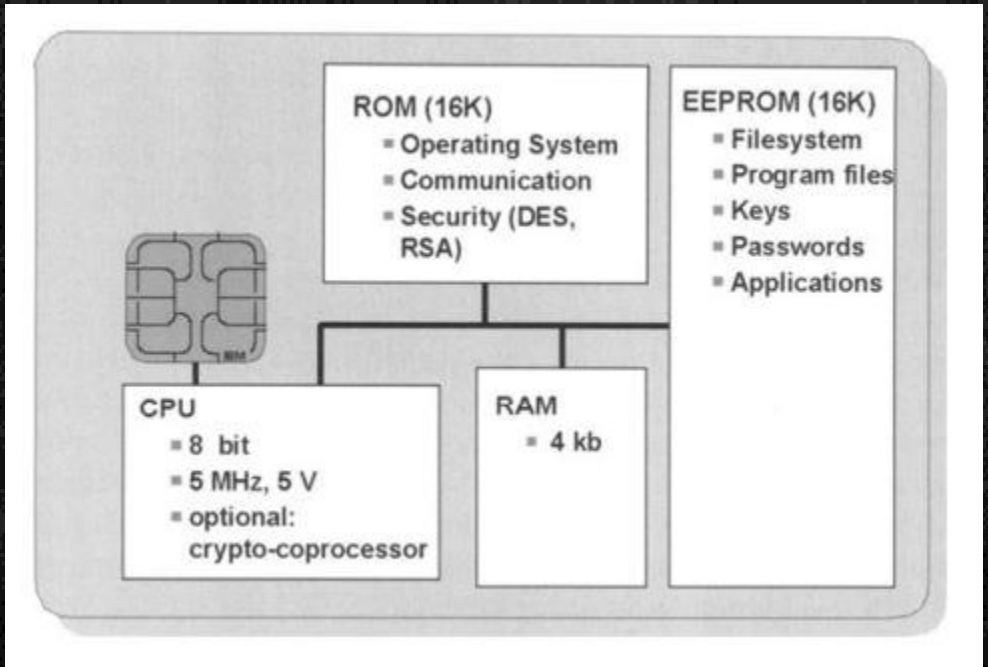
Popular Uses: Network security, vending, meal plans, loyalty, electronic cash, Government IDs, campus IDs, e-commerce, health cards

- Contactless: Cards containing an embedded antenna instead of contact pads attached to the chip for reading and writing information contained in the chip's memory.

Popular Uses: Student identification, electronic passport, vending, parking, tolls, IDs.

The Computer on the Smart Card

- The most important characteristic of a smart card is that it contains a computer with CPU and memory. Today's smart cards have approximately the same computing power as the first IBM PC.



The Computer on the Smart Card

- CPU: Today, most smart cards have an inexpensive 8-bit microprocessor, but high-end cards can contain a 16-bit or 32-bit processor.
- Cryptographic Coprocessor: An optional cryptographic coprocessor increases the performance of cryptographic operations. By performing signature operations on the card itself, the user's private key never needs to leave the card.
- ROM: The information stored in the ROM is written during production. It is the same for all chips of a series. It contains the card operating system and maybe also some applications.

The Computer on the Smart Card

- EEPROM: The EEPROM is used for permanent storage of data. Even if the smart card is unpowered, the EEPROM still keeps the data. Some smart cards also allow storing additional application code or application specific commands in the EEPROM.
- RAM: The RAM is the transient memory of the card and keeps the data only as long as the card is powered.
- ISO 7816: The basic smart card standard is the ISO 7816 series (ISO99). This standard details the physical, electrical, mechanical, and programming properties of smart cards. The EMV specification is based upon the ISO standard and is intended to be an industry-wide chip card specification, which ensures that all chip cards would operate with all chip-reading terminals, regardless of location, application, or manufacturer.

Hardware Security

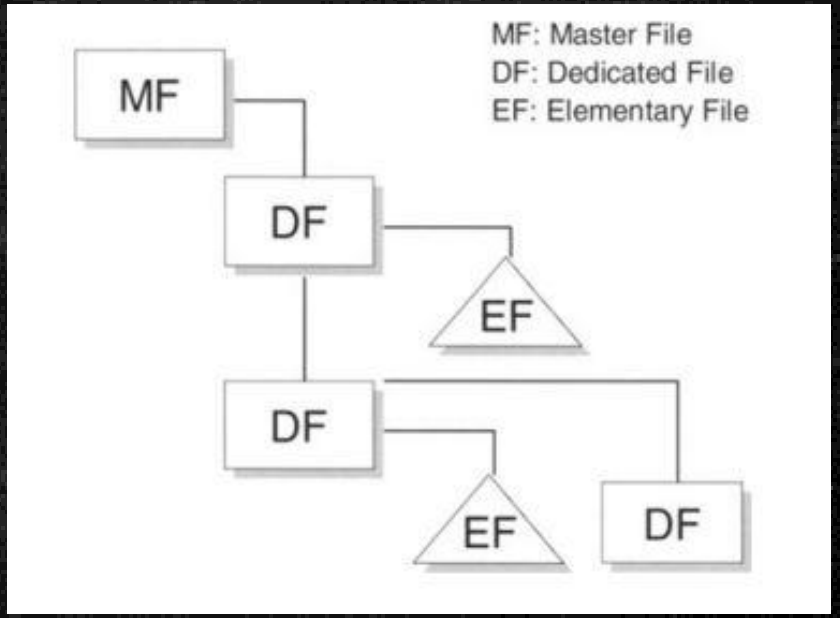
- The design of a smart card chip considers many more possible threats [RAN98]. These include slicing off layers of the chip to optically read out data, manipulating the voltage or dock to make the processor fail, attacks using high temperature or X-rays, and several others.
- Sophisticated counter measures are applied to guard the chip against the various attacks.
- For example, passivation layers are added to prevent analysis in combination with slicing off layers of the chip.
- Address lines and the memory cells of the chip are arranged in unusual patterns to make the physical examination harder.
- Furthermore, some chips have the capability to detect if the layer above the chip was removed, as it would occur if somebody were to examine the chip.
- Chips can detect unusual variations in the clock or in the voltage and react with shutdown of the operation.

Card Acceptance Devices

- Card acceptance devices range from simple card readers to highly sophisticated, programmable payment terminals with several slots and user interface support.
- Readers can be attached to a PC via serial port, they can be integrated in a keyboard, or embedded into appliances such as banking terminals. Many pervasive devices like set-top boxes, cellular phones, or handhelds are equipped with smart card readers.

File-system cards

- The majority of current smart cards have a file system integrated into the operating system.
- A file system on a smart card supports the storage and retrieval of all kinds of data and is useful for many types of applications.
- According to ISO 7816, a file system consists of directories (DF) and files (EF). The root directory is referred as MF .
- When multiple applications share one card, usually each application uses a different directory in order to separate their data from each other.
- In order to find the directory assigned to a specific application, the EMV -specification introduced a directory file , listing all applications present on a card.



Smart Card Software

Usually a smart card application consists of the following two parts:

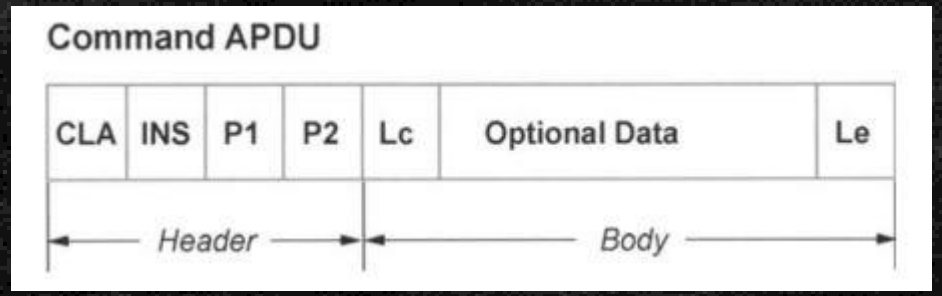
- Off-card: The off-card part of the application is the part that resides on the host computer or terminal connected to the smart card through a smart card reader device. For instance, the OpenCard Framework (OCF) is a framework that supports off-card application development using Java.
- On-card: The on-card part of an application is stored in the chip of the smart card. This part can consist of data and maybe executable code. If the on-card part has executable code, this code is executed by the smart card operating system and can use operating system services, such as encrypting or decrypting data. These functions can be used to make the smart card and the communication with the smart card notably secure.

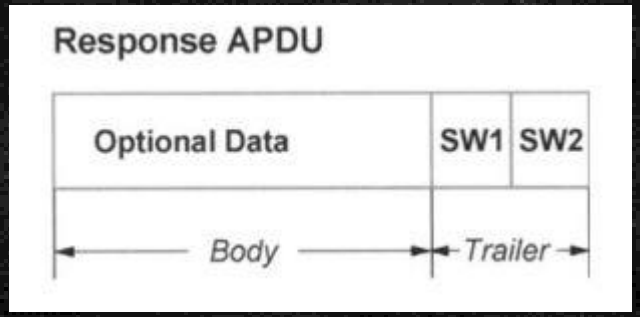
Communication Between the On-Card and Off-Card Ports

- The protocol stack of the communication between the smart card and the host has several layers. On the application layer, the communication takes place between the off-card part of an application and its corresponding on-card part. The commands and data exchanged are specific to a particular application and cover tasks like read, write, decrease, and others. The next lower layer is the layer of the Application Protocol Data Units (APDUs). The format of the APDUs is independent of the application.

Application Protocol Data Unit (APDU)

- Application Protocol Data Units are used to exchange data between the host and the smart card. ISO 7816-4 (SO99) defines two types of APDUs: Command APDUs, which are sent from the off-card application to the smart card, and Response APDUs, which are sent back from the smart card to reply to commands.





Command APDU

There are several variants of Command APDUs. Each Command APDU contains:

- A class byte (CLA). It identifies the class of the instruction, for example if the instruction is ISO conformant or proprietary, or if it is using secure messaging.
- An instruction byte (INS). It determines the specific command.
- Two parameter bytes P1 and P2. These are used to pass command specific parameters to the command.
- A length byte Lc ("length command"). It specifies the length of the optional data sent to the card with this APDU.
- Optional data. It can be used to send the actual data to the card for processing.
- A length byte Le ("length expected"). It specifies the expected length of the data returned in the subsequent response APDU. If Le is 0 x 00 , the host side expects the card to send all data available in response to this command.

Response APDU

A Response APDU contains:

- Optional data.
- Two status word bytes SW1 and SW2. They contain the status information as defined in ISO 7816-4.

Smart Labels

- One of the major problems to solve in the Pervasive Computing world is the identification of objects. The current solution is through use of bar codes.

Bar Code Advantages

- They can be printed on labels.
- They are very inexpensive
- They can be reliably scanned.

Bar Code Disadvantages

- Since bar codes are scanned optically, they must be visible on the outside of the object.
- Scanning takes place at a fairly short range - a few centimeters.
- The objects must be separated in order to be identified.
- The information conveyed by a bar code is fixed when the bar code is printed and cannot be changed.
- The bar code itself is completely passive and any bar code reader can access its information, making it very difficult to fulfill security requirements demanded by some applications.
- If a bar code is hidden from the scanner, it cannot be read, making it useless for Electronic Article Surveillance applications.
- The bar code scanners are fairly complicated - typically involving a laser, moving mirrors, and detection hardware - making them expensive.

Acknowledgements

These slides contain material developed and copyright by:

- Pervasive Computing Handbook - Uwe Hansmann