# CSE 334: Pervasive Computing

Dept. of Computer Science & Engineering
Daffodil International University

## Lecture- 3: Smart Identification

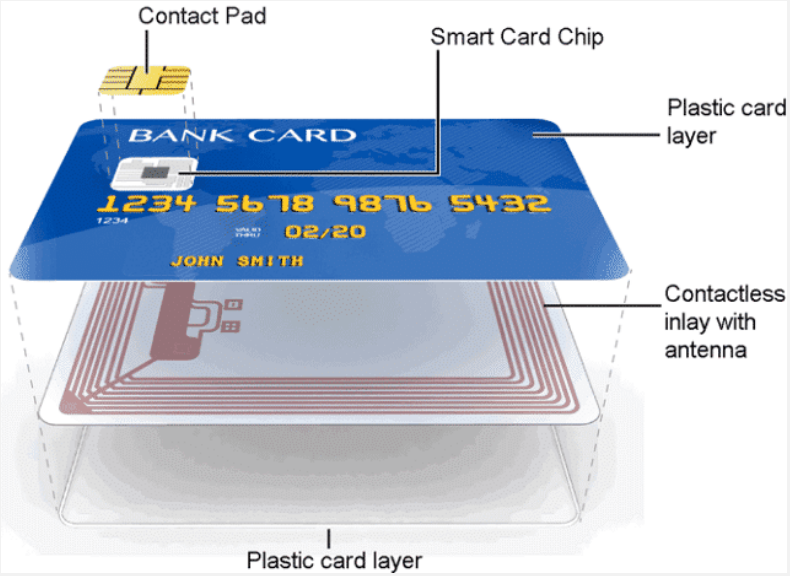
**A I Tazib**
Contact: tazib.cse@diu.edu.bd

**Content**

1. Smart card
    I. History and introduction
    II. Smart card hardware
    III. Smart card software
    IV. Communication protocol
2. Smart Label
    I. Introduction
    II. Bar code
    III. Smart label
    IV. Smart label reader

## Smart card

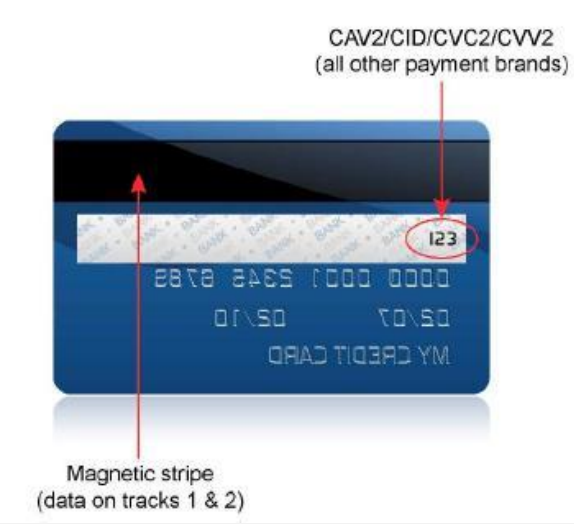
A smart card is a secure, tamper-resistant device consisting of a single-chip microcomputer, which is mounted on a plastic card of the size of a standard credit card.



## Magnetic strip

The first credit cards just had the name of the owner printed on the front. Later, cards with embossed printing were introduced.

- It was less secure
- Copying information was so easy



## Smart Card

In 1968, a patent for an identification card with an integrated circuit was filed, and the smart card was born.

- Information on it cannot be copied
- More secure

# 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.

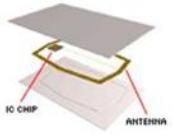
## Contact / Contactless Smart Cards

CONTACT:

- Cards the size of a conventional credit or debit card with a single embedded 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



# Smart Card Chip and its Components

**CPU** Today, most smart cards have an inexpensive 8-bit microprocessor, but high-end cards can contain a 16-bit or 32-bit processor.

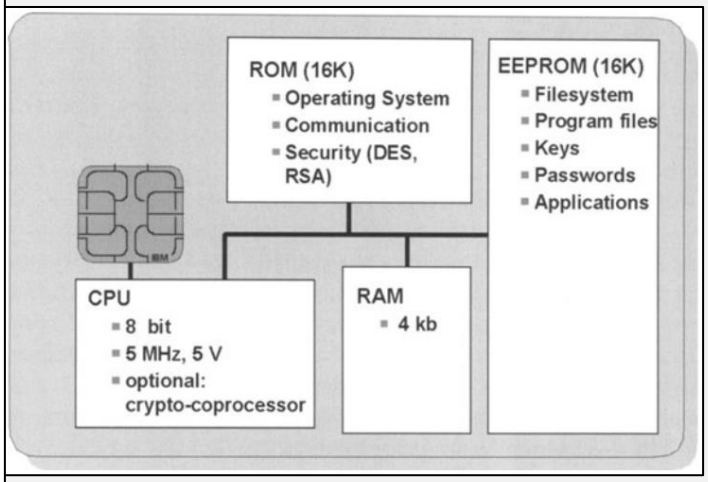
**Cryptographic coprocessor** An optional cryptographic coprocessor increases the performance of cryptographic operations. By performing signature operations on the card itself, the user's private key never needs to leave the card.

**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.

**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.

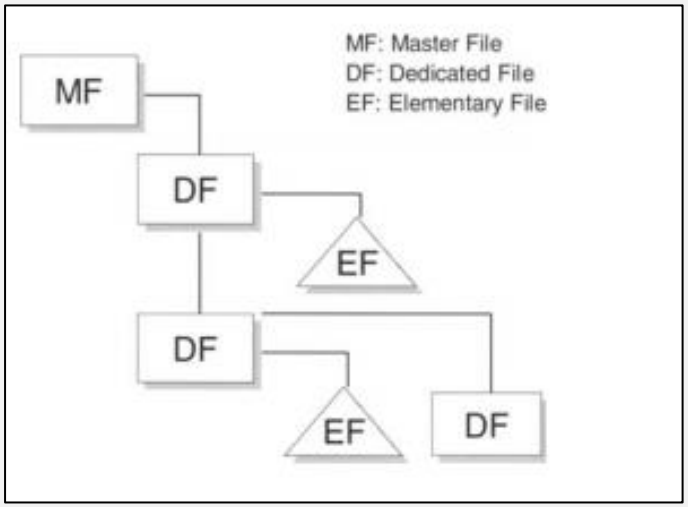


# Smart Card Software

**Off-card application-** 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.

**On-card application-** 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.

**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 a11 kinds of data and is useful for many types of applications.

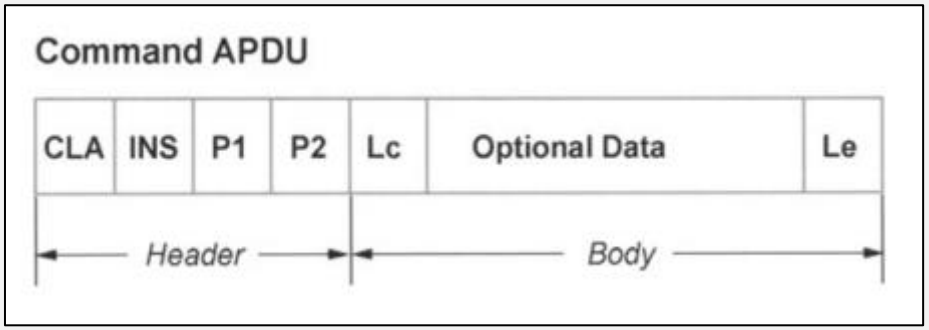


# Application Protocol Data Unit (APDU)

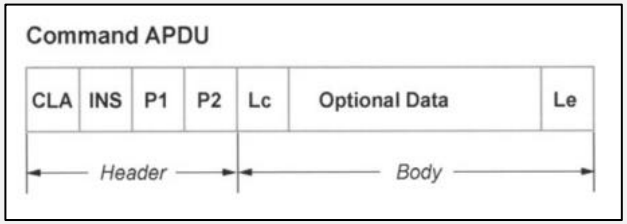
Application Protocol Data Units are used to exchange data between the host and the smart card.

ISO 7816-4 [IS099] defines two types of APDUs:

- **Command APDUs** (sent from the off-card application to the smart card)
- **Response APDUs** (sent back from the smart card to reply to commands)

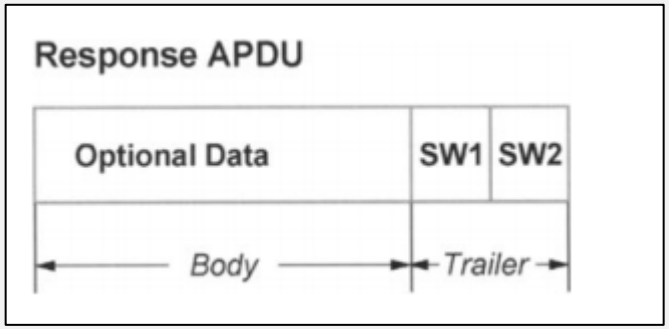


# Command APDUs




- 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 PI 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 0x00 , the host side expects the card to send all data available in response to this command.

# Response APDUs




A Response APDU contains:

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

# Smart Label and Label Reader

**The current solution of object identification in Pervasive Computing is through use of bar codes.**

Everyone has seen bar codes on product packaging. They have many advantages:

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

However, there are also a number of 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.

## Smart Label Reader

Smart label readers contain no moving parts. All that is needed is an antenna and an electronics module. This reduces the cost of the reader and opens the door far integration into many new applications.

**Why is it convenient?**

Data can be read and written at distances of over one meter. Through use of collision avoidance algorithms, several smart labels can be accessed simultaneously. This means that separation of individual items before reading them is not required.

**Thank you!**