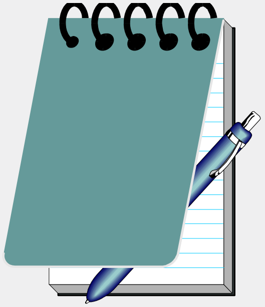


Summary

- 1- What is a smart card ?
- 2- Standards in the smart card industry
- 3- Card life cycle
- 4- Security features

1 - What is a smart card ?

A secure way of storing small amount of sensitive data

Characteristics of Microprocessor Cards

- Memory and processor on the same chip
- Unique and permanent serial number
- Secret code protection in the card
- Cryptographic capabilities

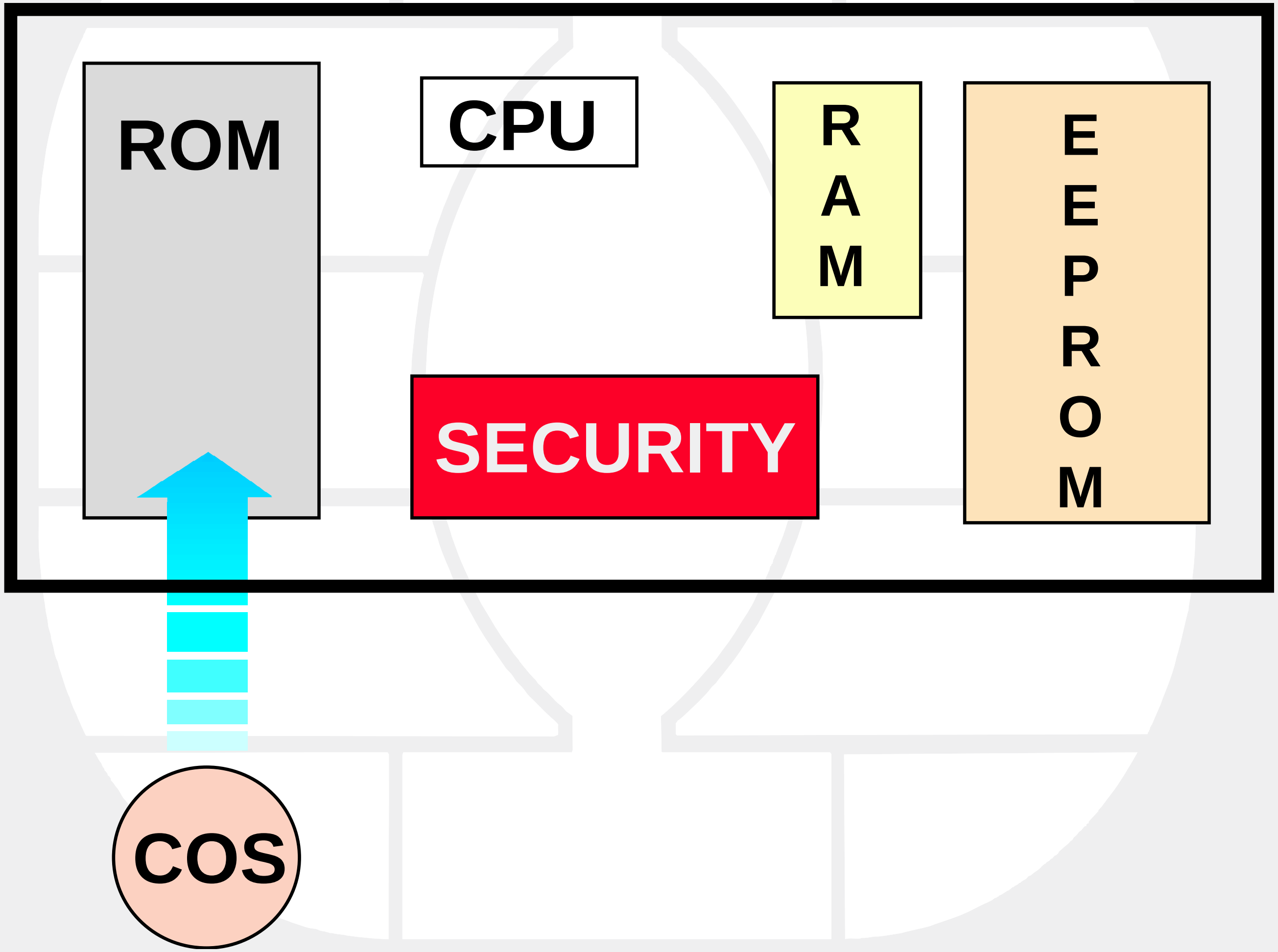
What Information needs to be in the card ?

- Everything that relates to the intrinsic operation of the application
  - identification of the card holder
  - rights of the card holder
- Everything that relates to the **security** of the card and the application
  - Card Serial Number
  - secret codes
  - keys for cryptographic algorithms

A smart card is not a mass-storage device

GEMPLUS

Inside the Chip of a Microprocessor Card



Role of the Operating System

- The operating system transforms a physical device into a logical tool by providing these features :
  - Memory Management
  - Security Management
  - Cryptographic Functions
  - Customization

Types of Objects Managed by the Operating System

- Data is organized in **files**
  - There are different types of files : data, code, key ...
- The **security** is managed by the OS :
  - Secret codes control access to files
  - Keys are used for cryptographic functions

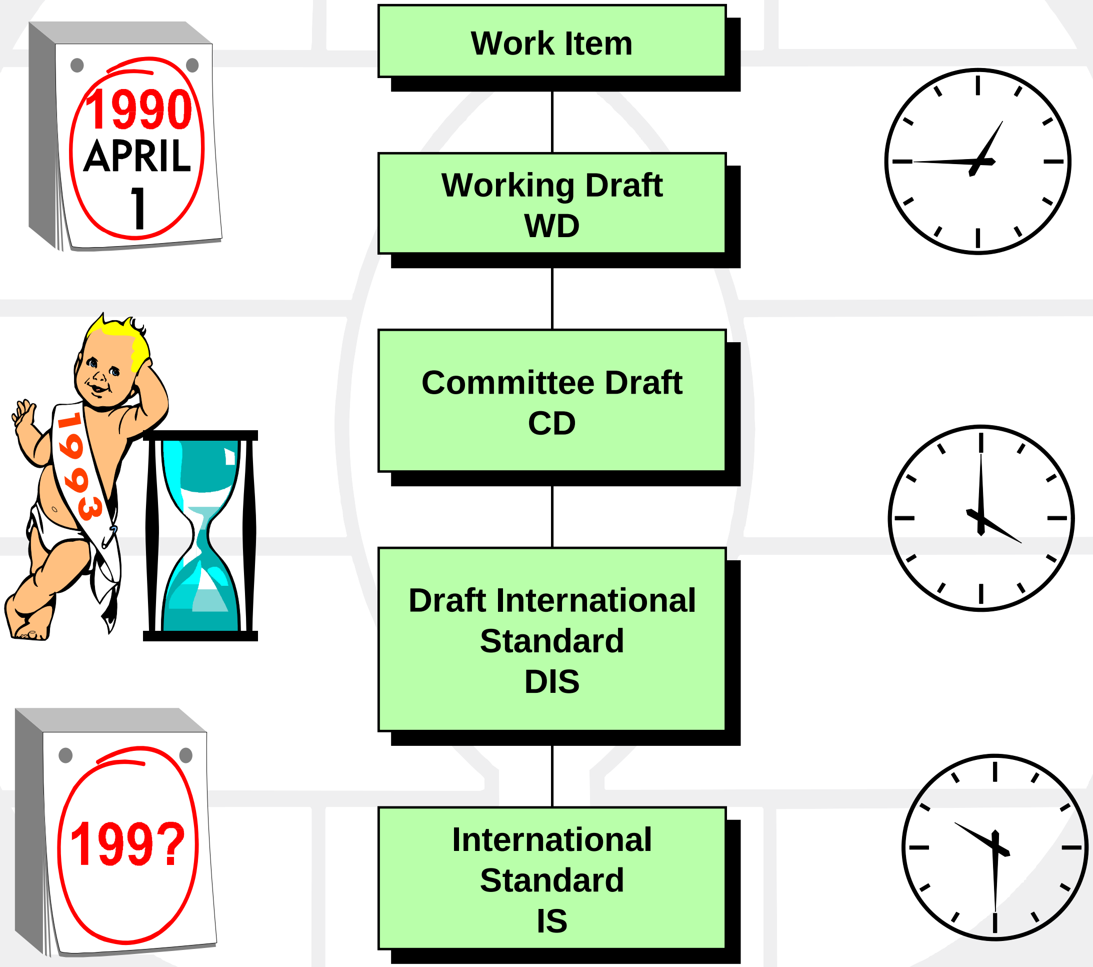
All data and security features are managed by the OS

Types of Commands Performed by the Operating System

- **Administrative commands**
  - File and directory management : create, read, write, update, ...
- **Security related commands**
  - Operations on secret codes and keys
- **Loyalty commands** (where applicable)
  - Award, Redeem...
- **Payment commands** (where applicable)
  - Credit, Debit, Read Balance, ...

2 - Standards in the Smart Card Industry

ISO : Document Genesis



Work Item

Working Draft
WD

Committee Draft
CD

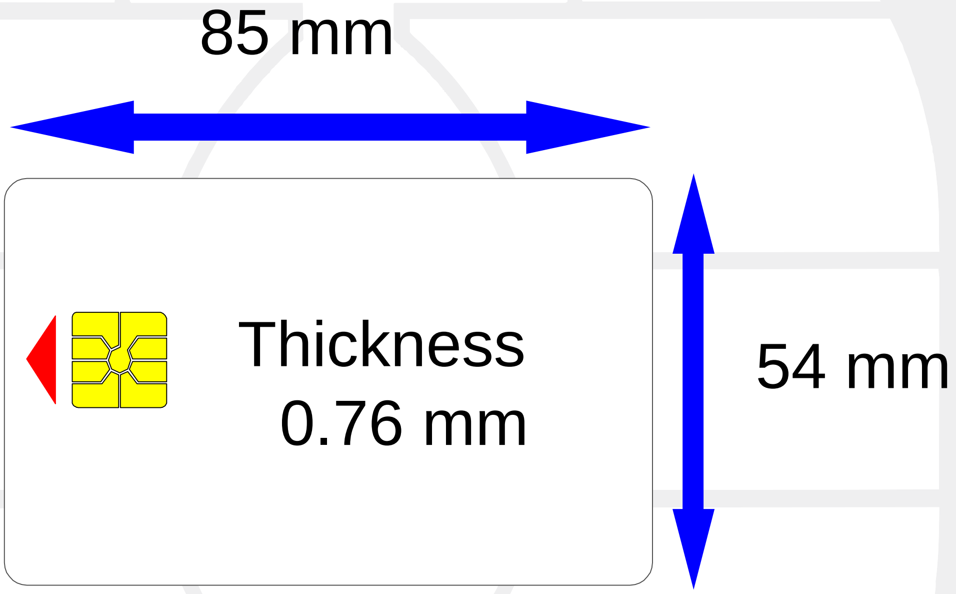
Draft International
Standard
DIS

International
Standard
IS

ISO 7816 - Identification Cards - Integrated Circuits Cards With Contacts

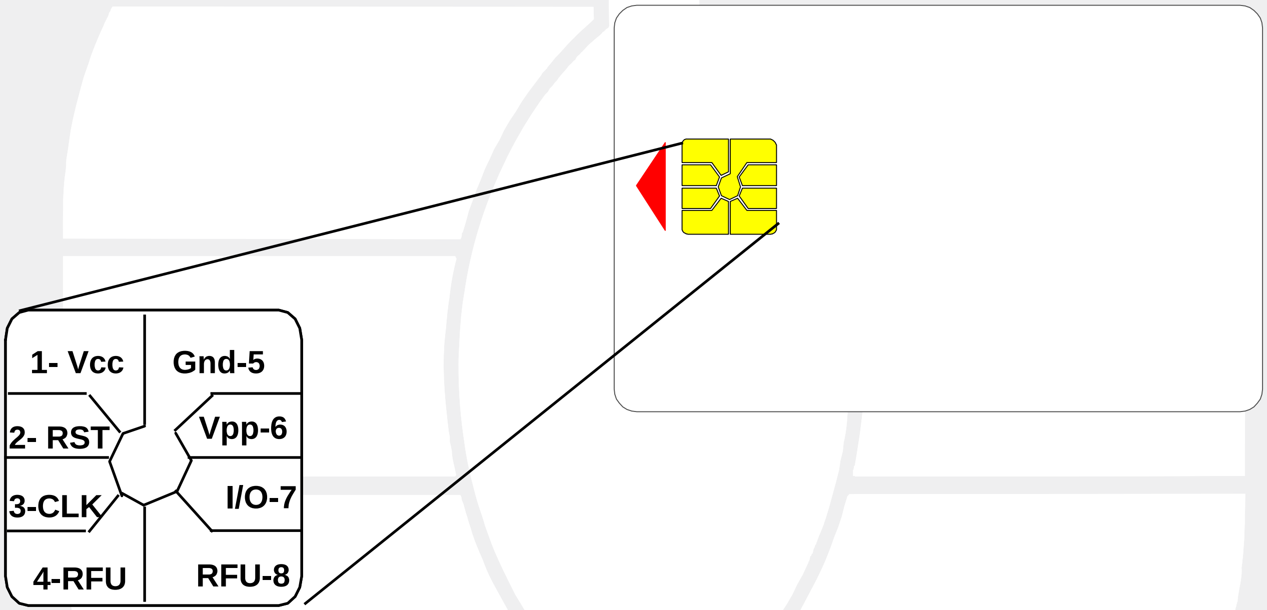
- **IS 7816-1 :** Physical characteristics
- **IS 7816-2 :** Dimension & location of contacts
- **IS 7816-3 :** Electronic signals & transmission protocols
- **IS 7816-4 :** Interindustry commands
- **IS 7816-5 :** Registration system for applications in IC card
- **IS 7816-6 :** Interindustry data elements
- **IS 7816-7 :** Interindustry commands for Structured Card Query Language (SCQL)
- **IS 7816-8 :** Security architecture and related commands

ISO 7816-1



Governs the physical characteristics of a smart card

ISO 7816-2



Governs the dimension and location of the chip contacts

ISO 7816-3

- Electrical Characteristics
  - clock frequency : [1 MHz, 5 MHz]
  - communication speed
- Transmission Protocols
  - T=0 and T=1 defined
  - T=14 reserved for proprietary protocols
- Protocol Type Selection (PTS)
  - if several protocols supported
- Answer-to-Reset

Governs the electronic signals and transmission protocols

Communication Protocols

- **T=0** : asynchronous half duplex character transmission protocol
  - One Way communication - any command expecting a response must send a second command to receive the response
- **T=1** : asynchronous half duplex block transmission protocol
  - Two Way communication - a single command may send and/or receive data
- **T=2 to T=13** : Reserved for future use
- **T=14** : reserved for protocols not standardized by ISO

Almost all currently available cards follow T=0

GEMPLUS

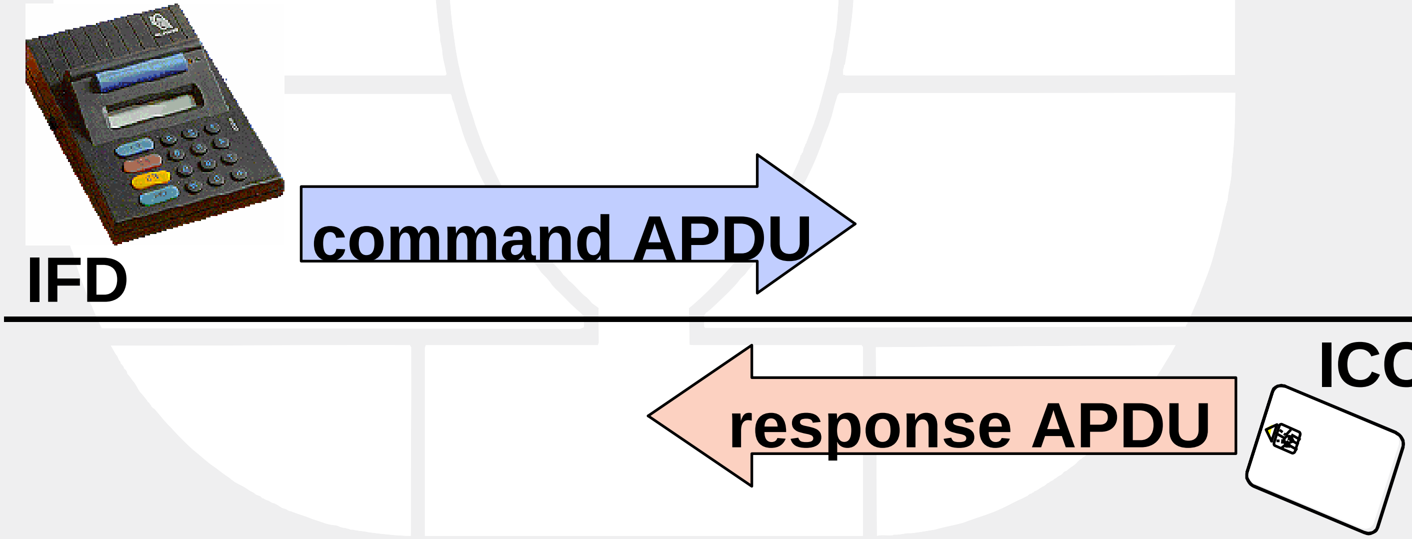
Scope of ISO 7816-4

- Contents of messages
  - commands
  - responses
- Structure of files and data
- Access methods to files and data
- Security architecture defining access rights to files and data
- Methods for secure messaging

Ensures Interoperability

The Application Protocol Data Unit (APDU)

- An APDU contains either
  - a command message
  - a response message



APDU Command

Command Format (ex: Read) without Body

Header				
CLA	INS	P1	P2	Le

- **Header**
  - **CLA** : indicates
    - ISO or Gemplus proprietary command
    - Secure messaging or not
  - **INS** : Instruction code (what type of command. ex.Read)
  - **P1, P2** : Parameters (ex. Read, where in the memory)
  - **Le** : Expected length of data to be returned

APDU Command

Command Format (ex: Write) with Body

Header					Body (if data for card)
CLA	INS	P1	P2	Lc	Data

- **Header**
  - **CLA** : indicates *ISO* or *Gemplus* proprietary commands
  - **INS** : Instruction code (what type of command. ex: *Write* data to the card)
  - **P1, P2** : Parameters, ex: *Write* where in the memory
  - **Lc** : Length of data sent to the card
- **Body**
  - Data for card

APDU Response

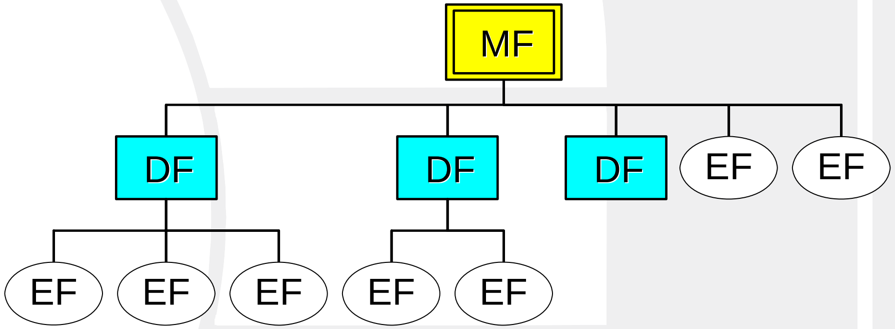
Response Format

Body (if data for terminal)	Trailer
Data	**SW1, SW2**

- **Body**
  - Optional
  - Holds the data returned by the card (ex: after *Read*)
- **Trailer**
  - Status returned by the card

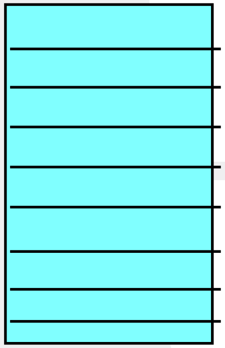
File Organization

- Card organized into files
  - MF - *Master File*
    - Root of the file structure
    - Contains other files
  - DF - *Dedicated File*
    - Contains other files
    - Can be seen as a directory
  - EF - Elementary File
    - Contains data

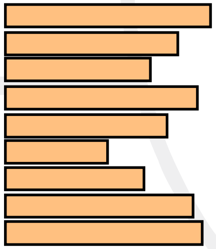


Elementary File Structures

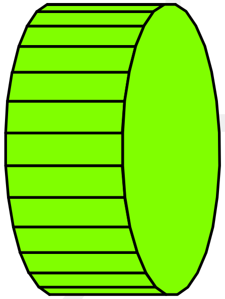
- ISO 7816-4 defines four different types of files :



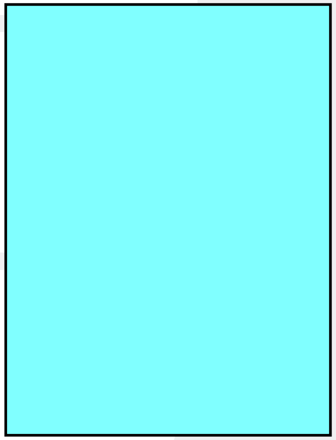
Linear fixed



Linear variable



Cyclic



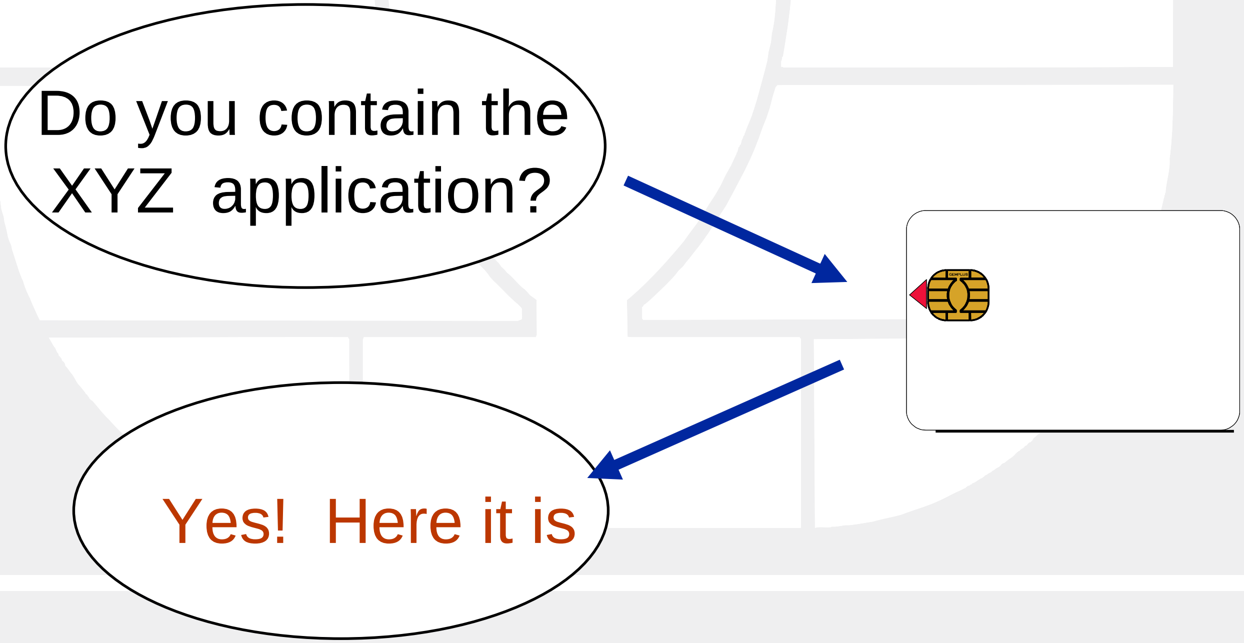
Transparent

Implementation for Files Organization

- Each file is made of
  - File descriptor containing information for
    - file management
    - security management
  - File body
    - DF
      - *optional*
      - *contains the DF name*
    - EF
      - *mandatory*
      - *contains data stored in the EF*

ISO 7816-5

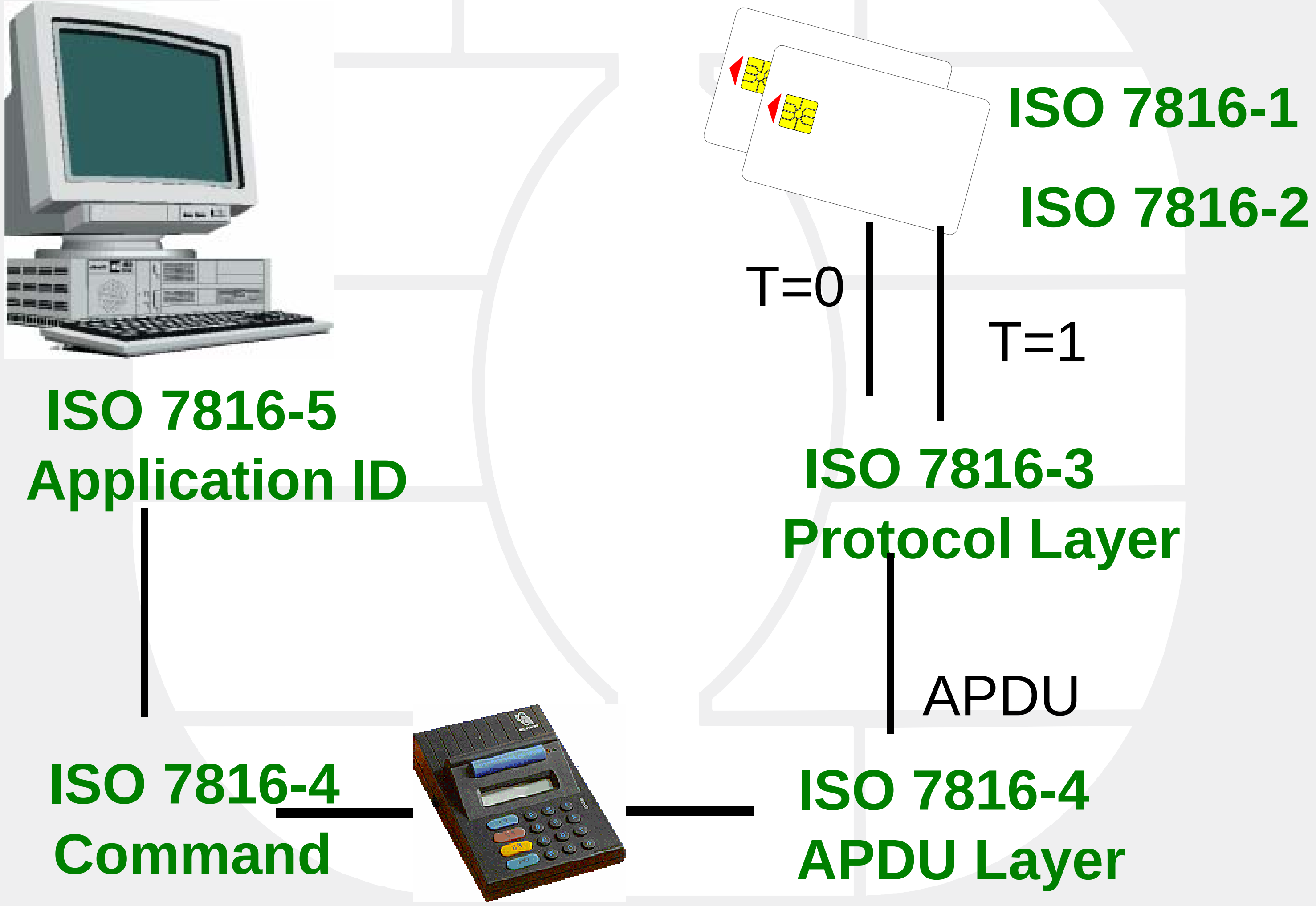
- Specifies
  - **Numbering system** for application identifiers
    - To identify if a given card contains an application
  - **Registration procedure** for application provider identifiers
    - AID is used to address an application in the card



Do you contain the XYZ application?

Yes! Here it is

Global Scheme



ISO 7816-1

ISO 7816-2

T=0

T=1

ISO 7816-5
Application ID

ISO 7816-3
Protocol Layer

APDU

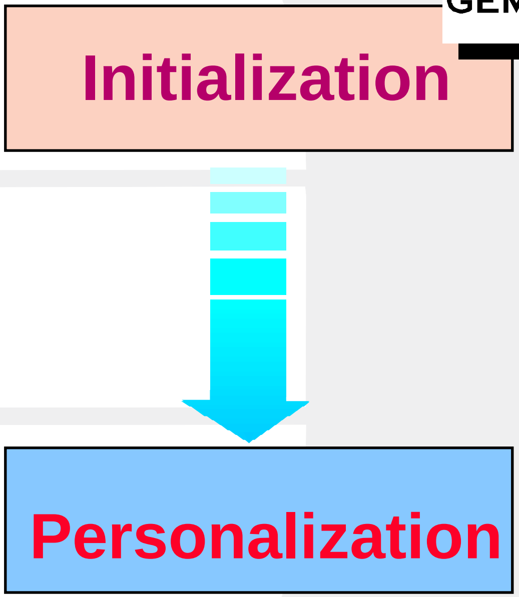
ISO 7816-4
Command

ISO 7816-4
APDU Layer

3 - Card Life Cycle

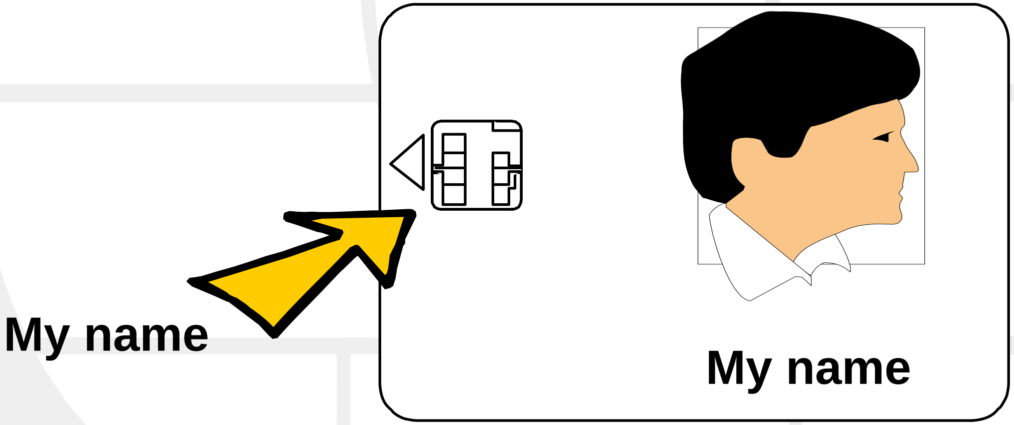
Card Life Cycle

- **Initialization**
  - Card associated with issuer
  - Security features loaded
- **Personalization**
  - Application profile loaded (card belong to one given application).
  - Cardholder profile loaded



Card Personalization

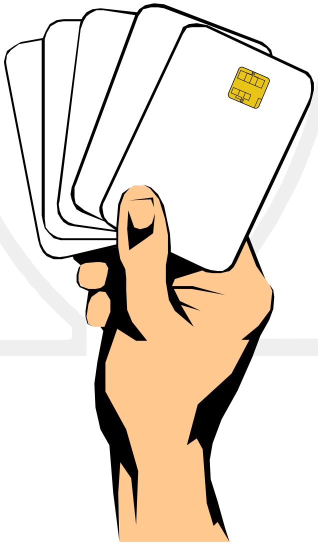
- **Electrical personalization**:
  - **downloading** of **data** (application & cardholder)
- **Graphical personalization**:
  - **printing text** or **artwork** on the card body



Making each card unique !

End-User Stage

- The memory can be accessed according to the rules defined at personalization stage

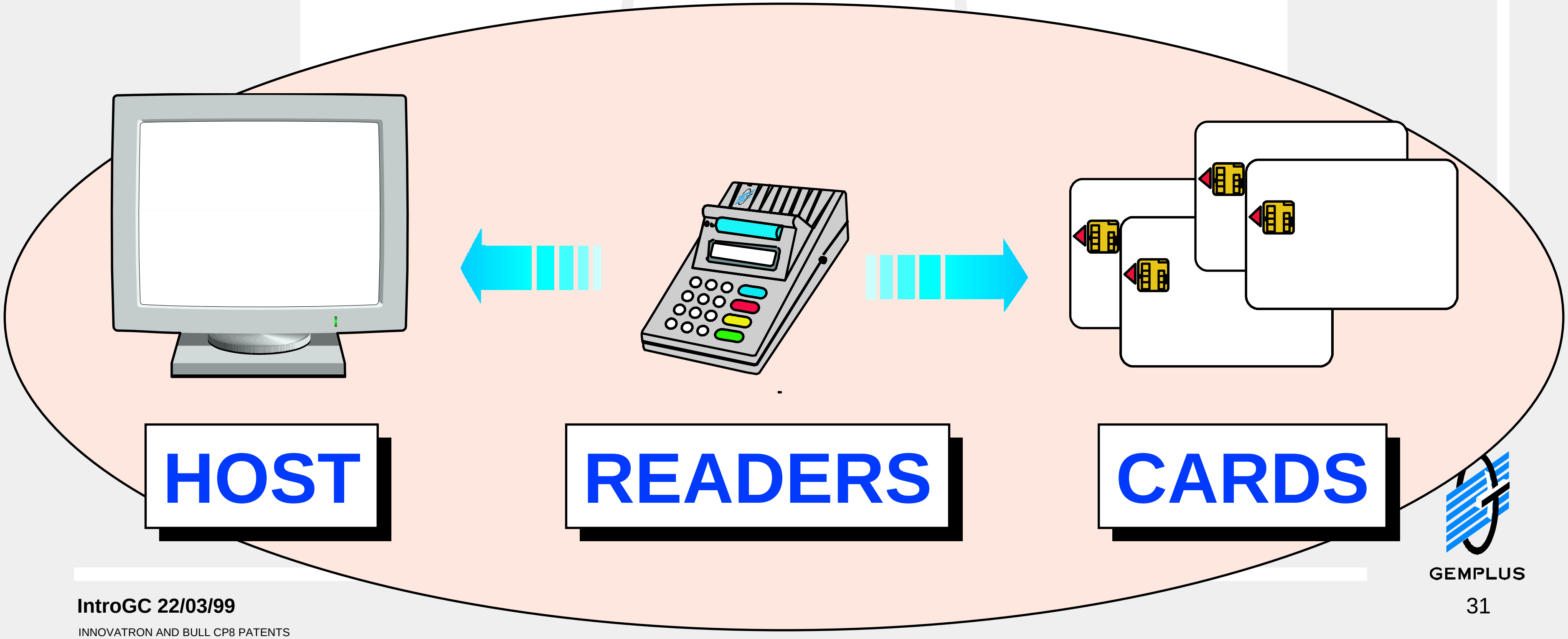


4 - Security Features

Security Scheme

- The smart card is not the only element involved in the security of an application

➡ **Security** must be managed for the entire application

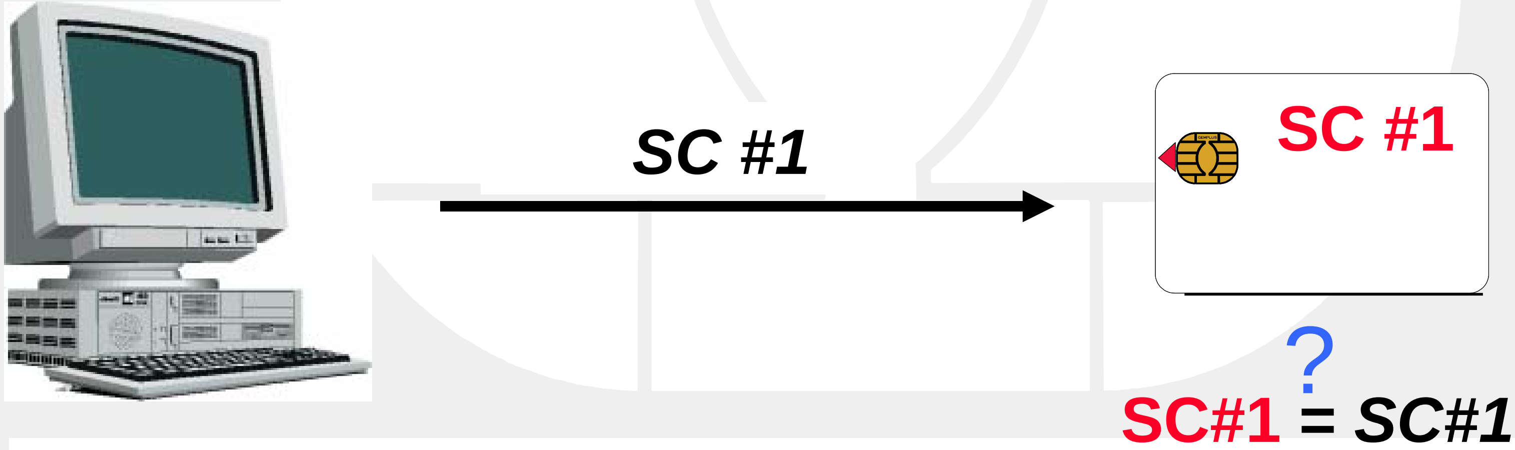


Definitions

- **Authentication** : to make sure that the card belongs to a genuine family of cards
- **Identification** : after authentication, to check the identity of the card (serial number, cardholder's identity, ...)
- **Integrity** : to ensure that the message has not been altered between the terminal and the card
- **Non repudiation** : to prevent the denial of previous transactions

Secret Codes

- Secret codes are used to protect
  - Access to files (read, write, update, ...)
  - Financial functions (read balance, debit, ...)
  - Administrative commands (create file, ...)
- A secret code is presented to the card and then checked by the card



SC #1

SC #1

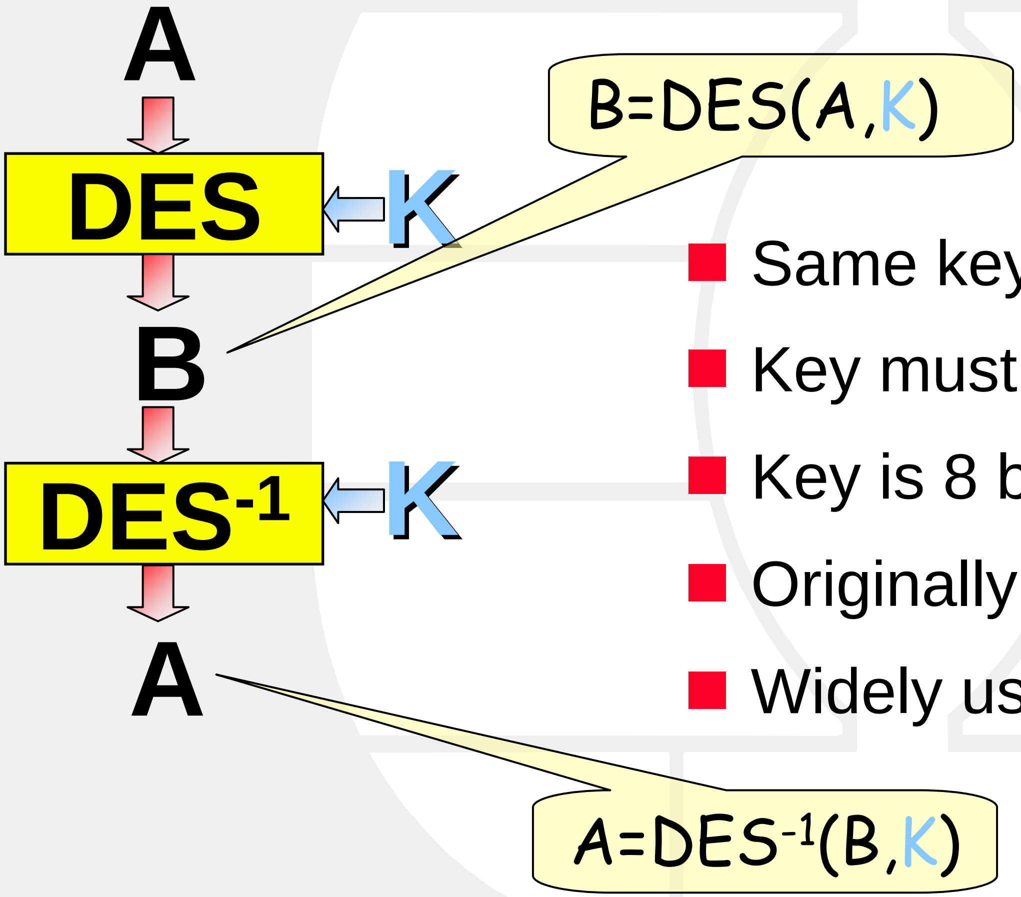
$SC\#1 \overset{?}{=} SC\#1$

Keys

- Keys are used by cryptographic algorithms
- Cryptosystems use two types of algorithms :
  - **Secret key** (e.g., DES, 3DES)
  - **Public key** (e.g., RSA, DSA)
- Keys are used for :
  - Secure messaging
  - Computing and verifying certificates/signatures

Secret Key Cryptography : from DES to 3DES

DES : Data Encryption Standard



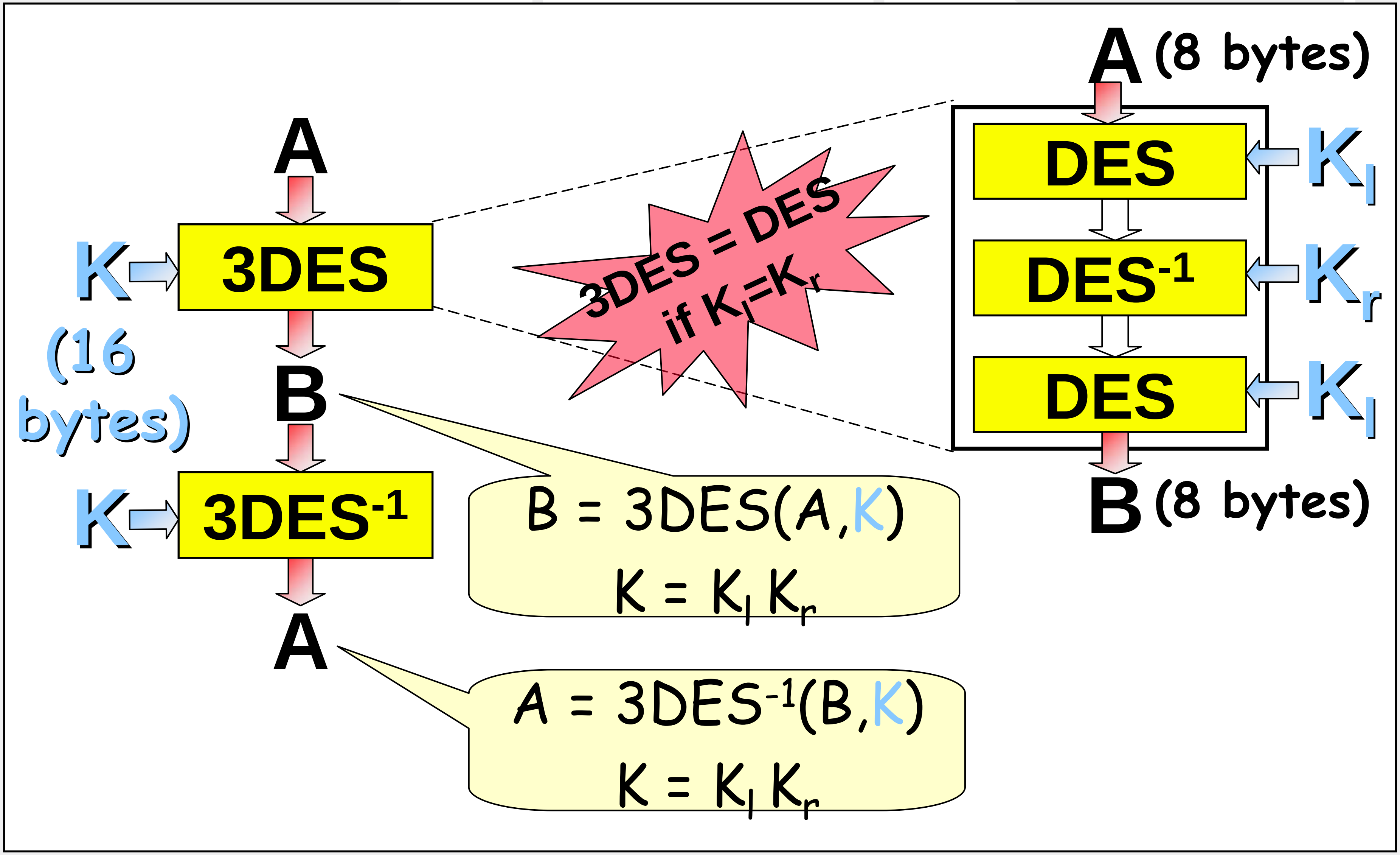
- Same key ⇒ Symmetric algorithm
- Key must be secret!
- Key is 8 bytes long
- Originally developed at IBM
- Widely used algorithm in the world

Switching to 3DES

- Improvement in computational performance and cryptanalysis techniques
- De facto standard is now Triple DES
- Triple DES is now endorsed by NIST, replacing DES
- DES does not offer sufficient long-term security

⇒ **Triple DES**

Triple DES



A

K (16 bytes) → 3DES

B

K → $3DES^{-1}$

A

3DES = DES if $K_l = K_r$

A (8 bytes)

DES ← K_l

DES^{-1} ← K_r

DES ← K_l

B (8 bytes)

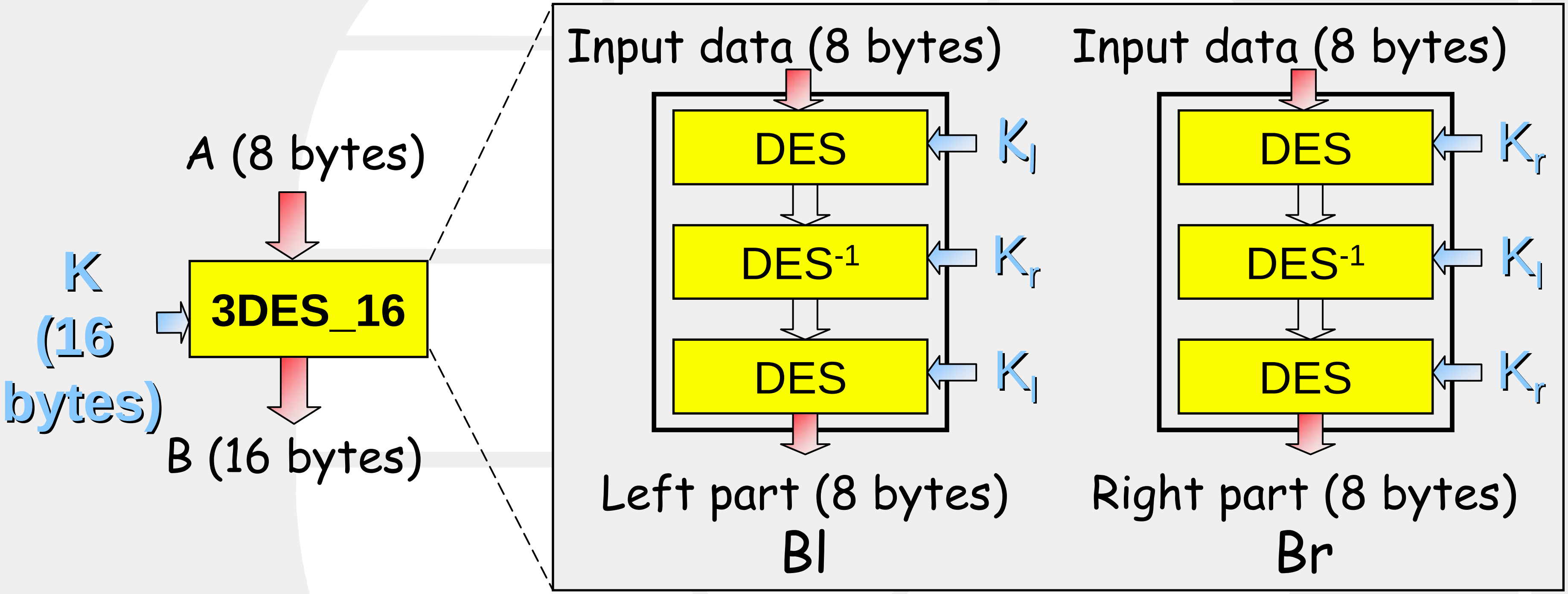
$B = 3DES(A, K)$

$K = K_l\,K_r$

$A = 3DES^{-1}(B, K)$

$K = K_l\,K_r$

Triple DES implementation
(16-byte result)



A (8 bytes)

K (16 bytes)

3DES_16

B (16 bytes)

Input data (8 bytes)

DES K_l

DES^{-1} K_r

DES K_l

Left part (8 bytes)
Bl

Input data (8 bytes)

DES K_r

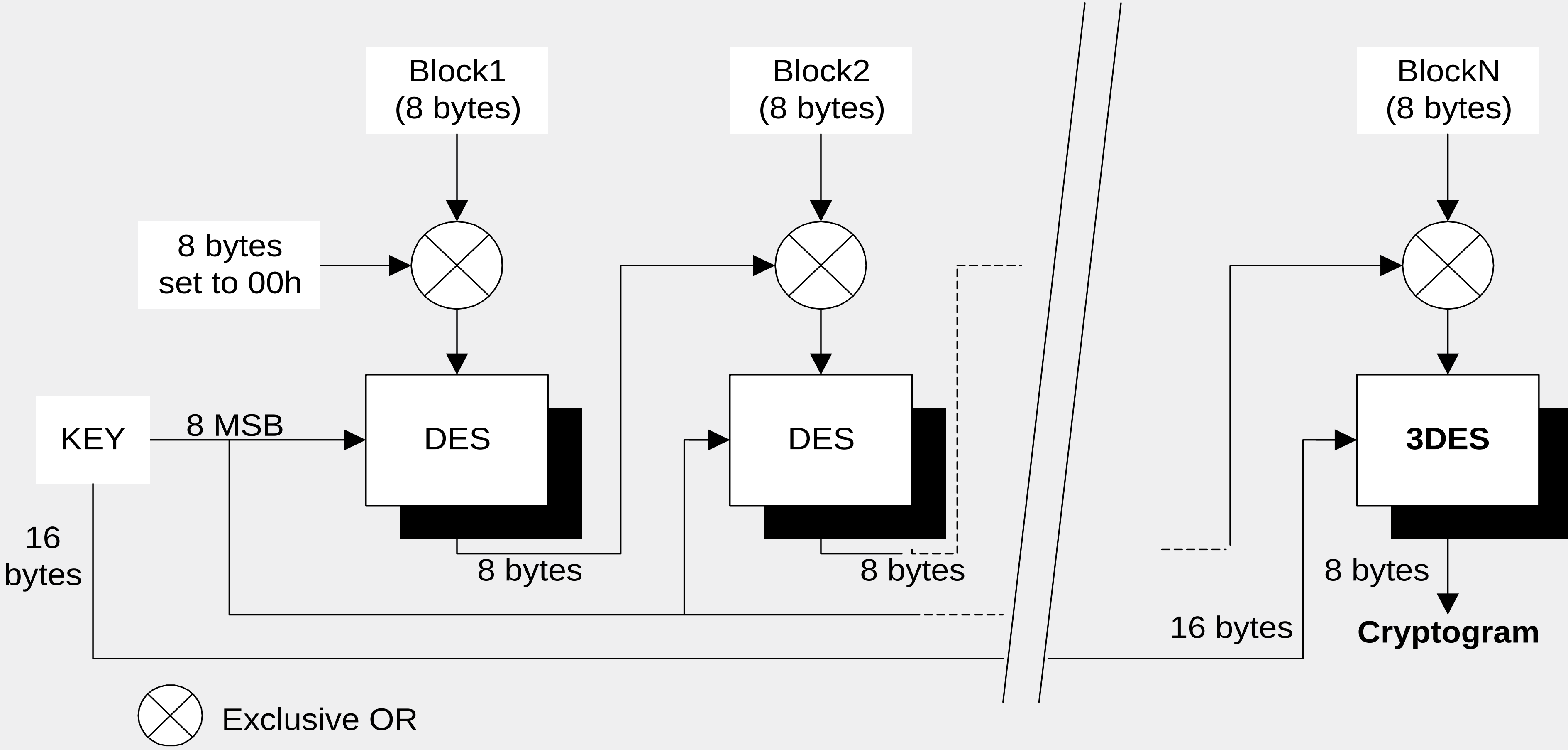
DES^{-1} K_l

DES K_r

Right part (8 bytes)
Br

- Used when a result on 16 bytes is required
- B = 3DES_16 (A, K)
  = Bl Br

3DES in CBC Mode



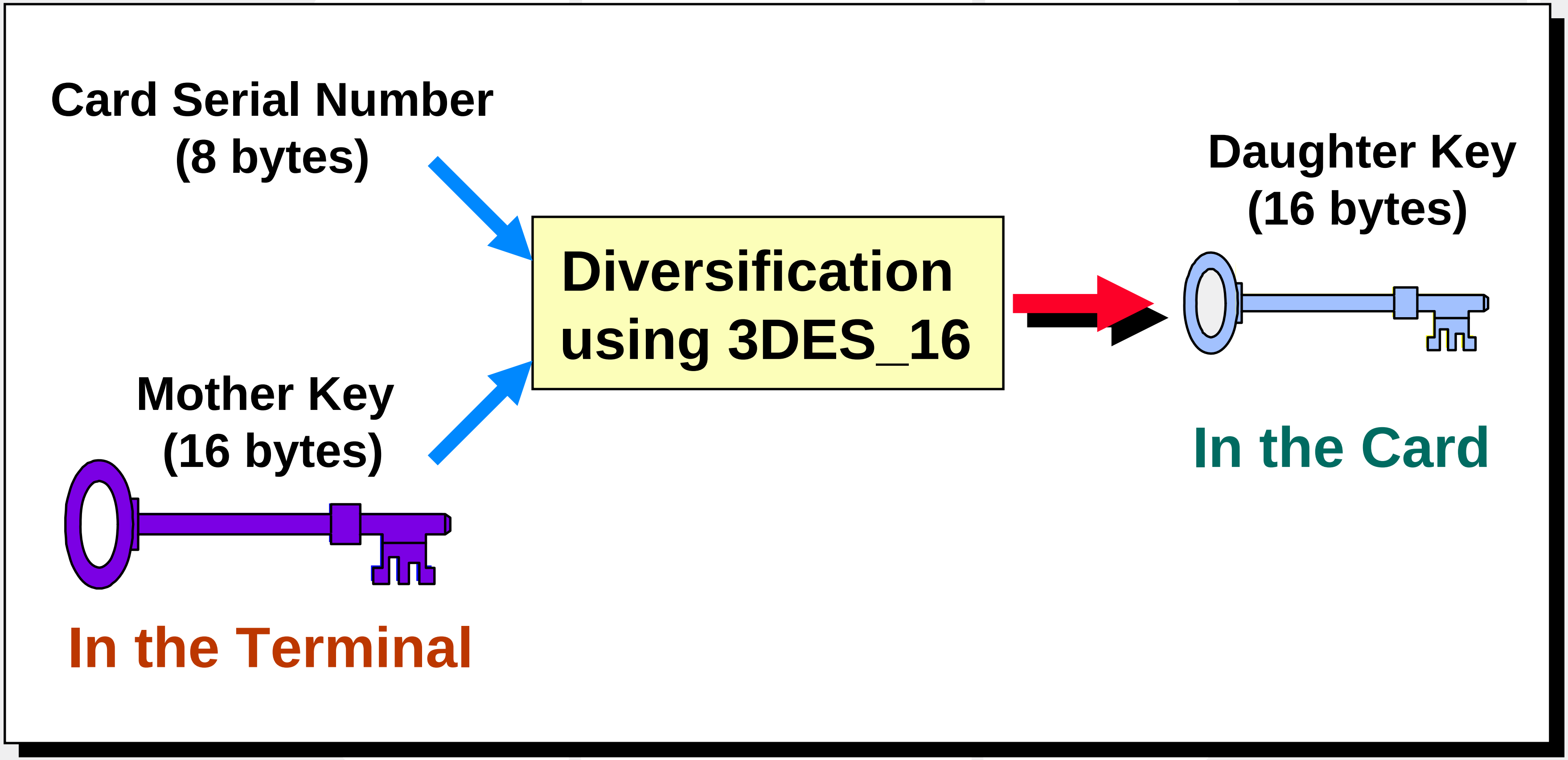
3DES Limitations

- The terminal and the card must know the same key K
- Same key in every card and in every terminal :

NOT SECURE!!

➡ **Diversification**

Diversification Process



Card Serial Number
(8 bytes)

Mother Key
(16 bytes)

In the Terminal

Diversification
using 3DES_16

Daughter Key
(16 bytes)

In the Card