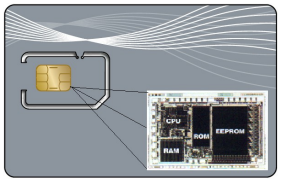
# Academic Day on Mobile Solutions for Senegal 2010 - June 7, 8 and 9 - Dakar

## SIM Card, SIM based Applications & Solutions

***June 8th, 2010***
***Dakar, Senegal***


**Presented by:** **Assane KEBE**
**Mobile Technical Consultant**
**Oberthur Technologies Senegal**
**assanekebe@gmail.com / +221 77 450 8354**





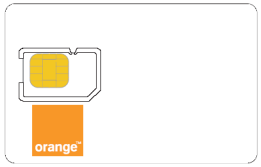

SIM Card, SIM based Applications & Solutions

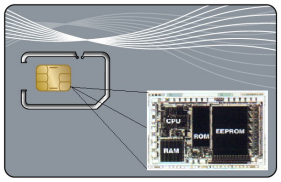
# Smart Card Basics

## AGENDA

- Architecture & memory types
- ISO7816 protocols
- Card Security
  - CHV / Key Management
- File System
- APDU



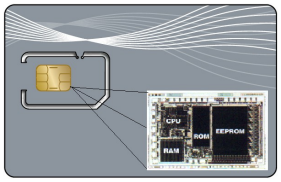





# Smart Card – Architecture & memories

## A Smart Card is :

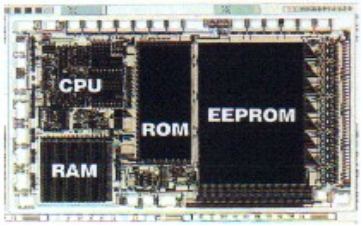
- **Plastic with a built-in microprocessor**
- **Standardized by ISO 7816**
- **Used for:**
  - Mobile Telephony: GSM/UMTS (U)SIM card
  - Indentity applications: Passport, Access card,…
  - Banking
  - Pay-TV




# Smart Card – Architecture & memories

## Microprocessor

*Overview (1/2)*




- **CPU**

  → *For commands processing*

- **ROM**

  → *Read Only Non volatile*

- **EEPROM**

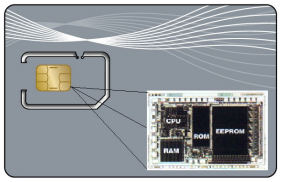
  → *Electrically Erasable Programmable ROM, Non volatile*

- **Flash**

  → *Non volatile*

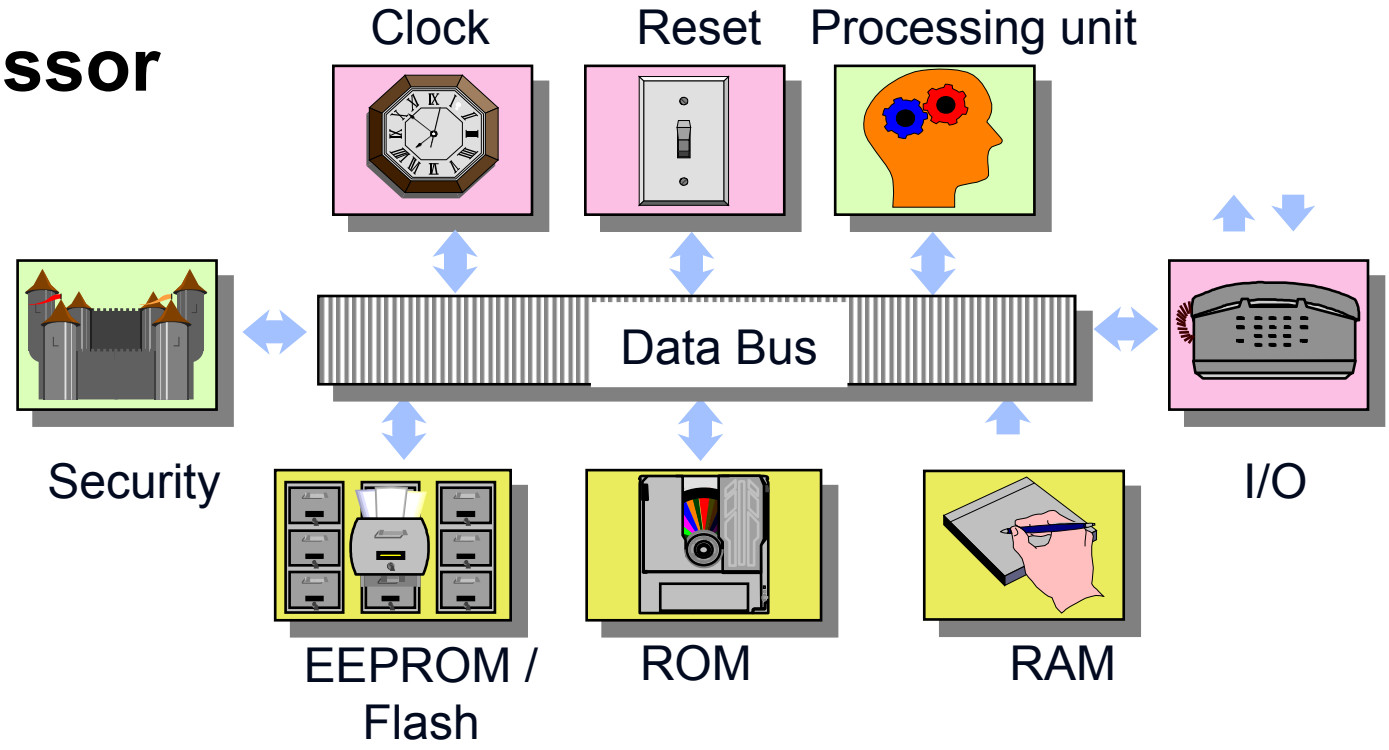
- **RAM**

  → *volatile*



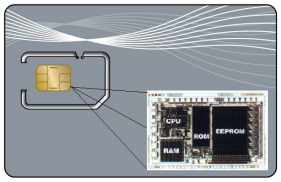
# Smart Card – Architecture & memories

## Microprocessor



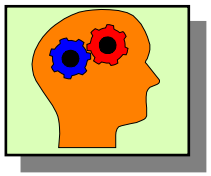

***Overview (2/2)***

**Samsung, Electronic Marin, Infineon, Atmel...**



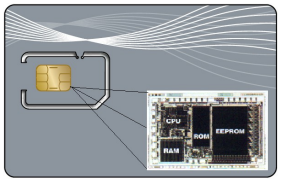

# Smart Card – Architecture & memories

## Microprocessor



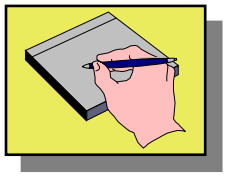
- CPU 6805/8051
- 8 bits data / 16 bits address
- 3,57 / 5Mhz  (clock)
- 5 / 3 / 1.8 Volts  (Vcc)

***Processing unit: CPU***



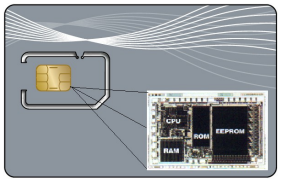

# Smart Card – Architecture & memories

## Microprocessor



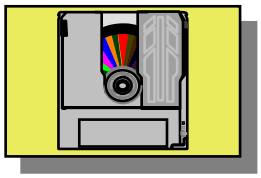
- RAM = Random Access Memory
- 128 bytes up to 8 kilobytes
- Volatile Memory
- Checked and cleared after reset

***RAM:*** ***Volatile***



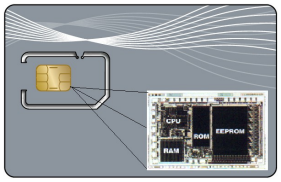

# Smart Card – Architecture & memories

## Microprocessor



- Read Only Memory
- Operating System
- I/O protocol
- External commands
- Memory management
- Authentication algorithms
- 6kb to 384kb

***ROM:*** ***Non volatile***

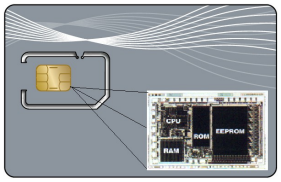



# Smart Card – Architecture & memories

## Microprocessor

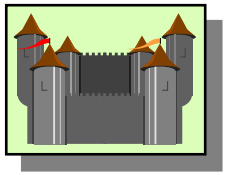
***EEPROM/Flash:***
***Non volatile***

- **Application memory**
- **Specific file architecture**
- **Data information**
- **CODOP \ OS Data \ Flashmask**
- **EEPROM: Presently up to 512Kb**
- **Flash: Presently up to 1Mb**



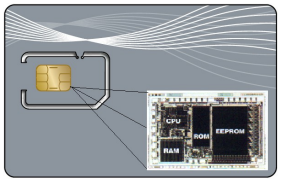

# Smart Card – Architecture & memories

## Microprocessor



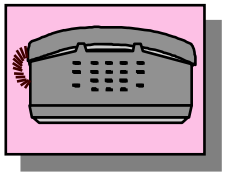
- Light
- Temperature
- Clock
- Vcc

***Security Component***



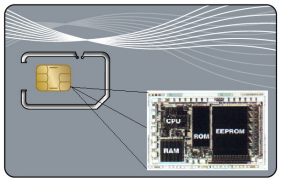

# Smart Card – Architecture & memories

## Microprocessor



- Bi-directional Input / Output
- T=0 protocol (bit oriented)
- Serial half-duplex communication

***Input***
***Output***





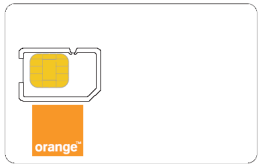

SIM Card, SIM based Applications & Solutions

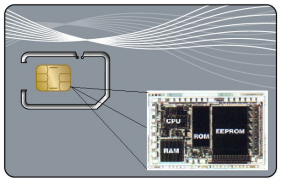
# Smart Card Basics

## AGENDA

- Architecture & memory types
- ISO7816 protocols
- Card Security
  - CHV / Key Management
- File System
- APDU





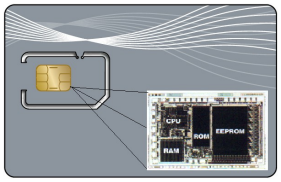



# Smart Card – ISO 7816-x protocols

## Define :

International Organization for Standardization

- Contacts location and dimension
- Electrical signals
- Data exchange protocol (with applications)
- Security




# Smart Card – ISO 7816-x protocols

## 7816 Main parts :

- 7816-1: Physical characteristics
- 7816-2: Dimension and location of contacts
- 7816-3: Electronic signals and transmission protocols
- 7816-5: Registration of application providers
- 7816-8: Commands for security operations
- 7816-9: Commands for card management
- …

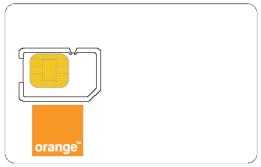
SIM Card, SIM based Applications & Solutions

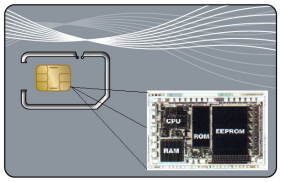
# Smart Card Basics

## AGENDA

- Architecture & memory types
- ISO7816 protocols
- Card Security
  - CHV / Key Management
- File System
- APDU

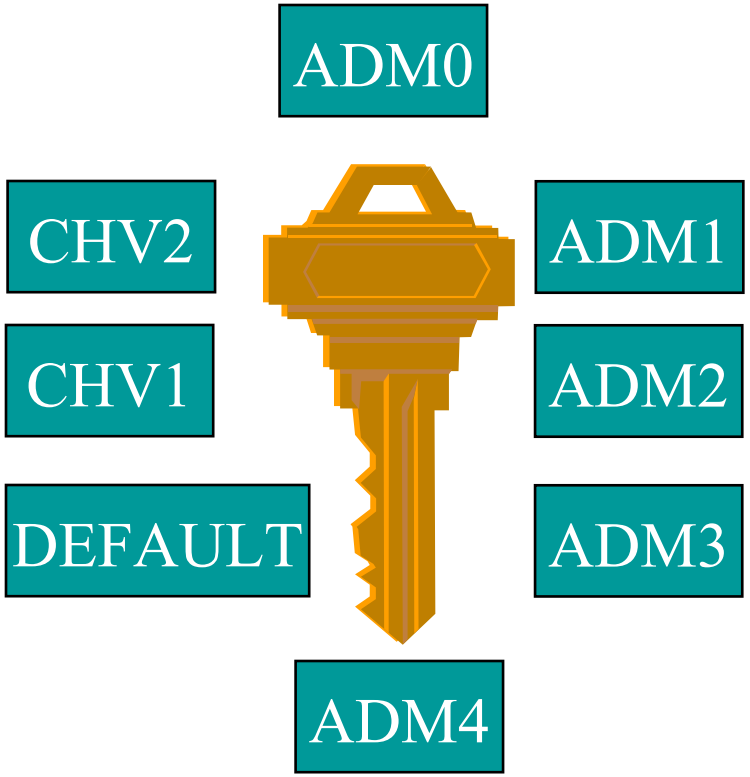




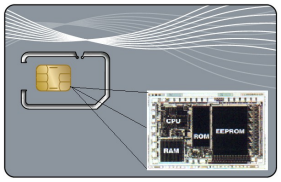



# Smart Card – Card Security

## Several security identities :



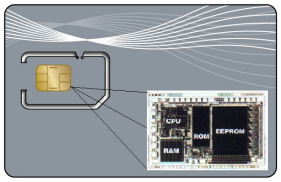

- like login / username
- Card Holder Verify
- ADMinistrative keys: The ADM0/1/2/3/4 security




# Smart Card – Card Security

## CHV codes :

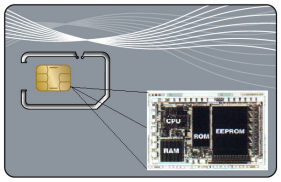
- Card Holder Verification = User PIN Code
- CHV1,2 = PIN1,2
- Reset of counter after correct PIN supply
- Unblocked by PUK1/2 code (usually 10 attempts)
- No unblocking key for PUK




# Smart Card – Card Security

## ADM codes :

- Advanced administration codes
- Such as Create/Delete/Rehabilitate/Invalidate
- Configurable number of attempts





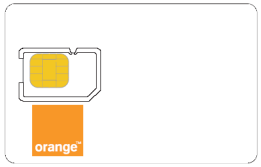

SIM Card, SIM based Applications & Solutions

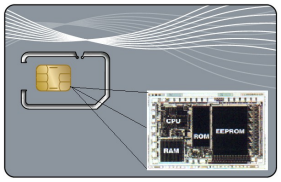
# Smart Card Basics

## AGENDA

- Architecture & memory types
- ISO7816 protocols
- Card Security
  - CHV / Key Management
- File System
- APDU



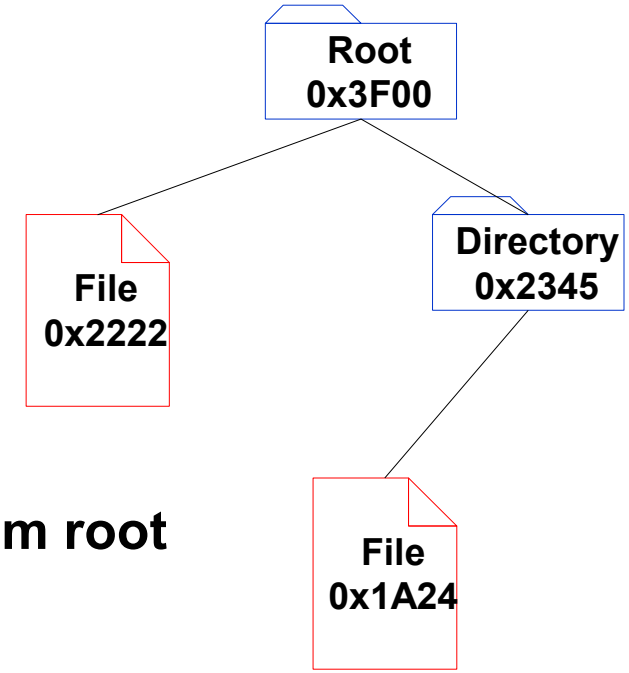


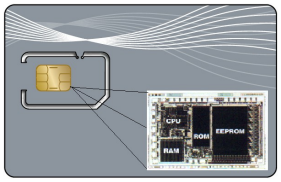



# Smart Card – File system

## Description :

- 2 types of file
  - DF (Dedicated File) → Folder
  - EF (Elementary File) → File
  - MF (Master File/3F00) → file system root
- Hierarchical file system
- Identified with a 2-bytes number

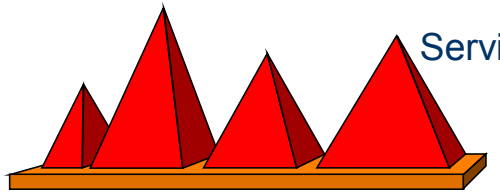




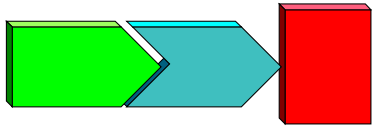

# Smart Card – File system

## File types :

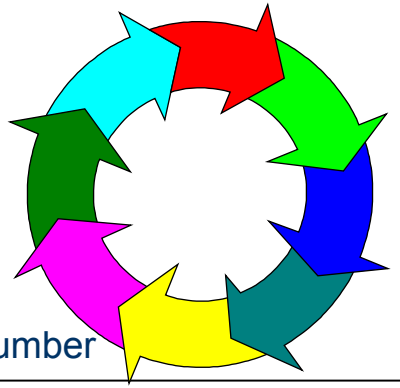
- **TF (Transparent File)**
  - **Binary file**
  - **Sequential, no organisation**
- **LF (Linear Fixed)**
  - **Sequential records**
- **CF (Cyclic File)**
  - **Cyclic sequential records**



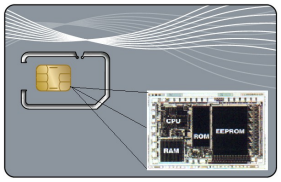
Service provider name



Phonebook



Last dialled number




# Smart Card – File system

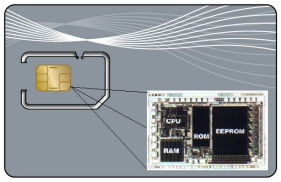
## File access :

- **1 file accessible at a time**
- **File access prerequisites**
  - **File selection: pointer set to its address**
  - **Files access rights**

    READ, UPDATE, INVALIDATE, REHABILITATE:

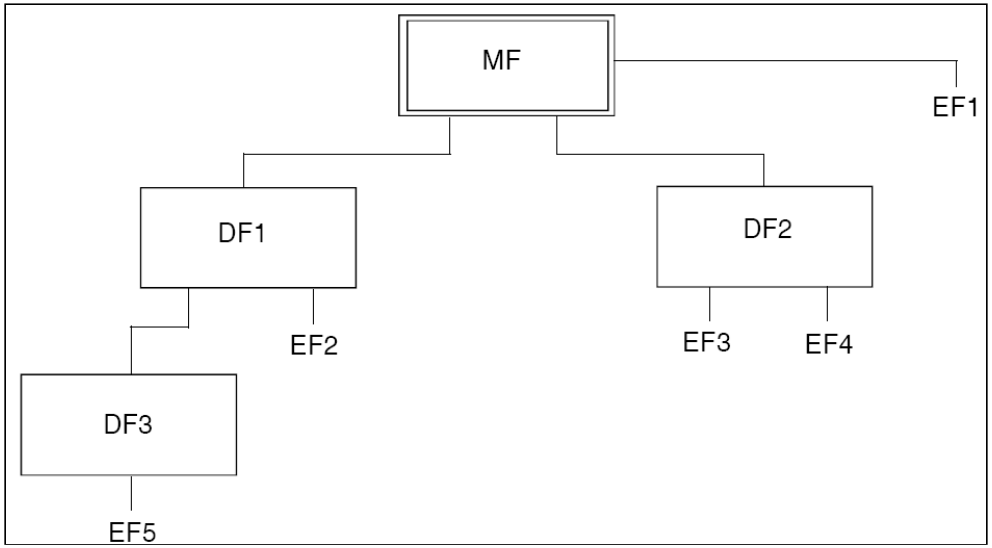
    → defined in file's header
  - CREATE, DELETE, RESIZE

    → defined in parent's header




# Smart Card – File system

## File selection rules :




| Last selected file | Valid Selections |
|---|---|
| MF | DF1, DF2, EF1 |
| DF1 | MF, DF2, DF3, EF2 |
| DF2 | MF, DF1, EF3, EF4 |
| DF3 | MF, DF1, EF5 |
| EF1 | MF, DF1, DF2 |
| EF2 | MF, DF1, DF2, DF3 |
| EF3 | MF, DF1, DF2, EF4 |
| EF5 | MF, DF1, DF3 |

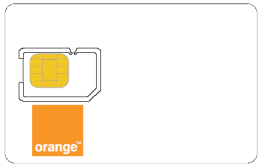
SIM Card, SIM based Applications & Solutions

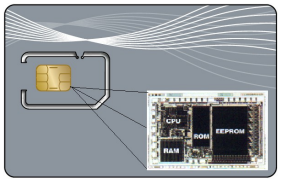
# Smart Card Basics

## AGENDA

- Architecture & memory types
- ISO7816 protocols
- Card Security
  - CHV / Key Management
- File System
- APDU



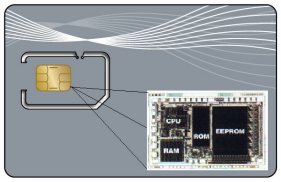





# Smart Card – Application Protocol Data Unit

## ATR: Answer To Reset :

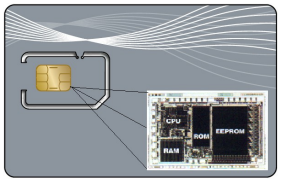
- Sent on POWER ON and RESET
- Up to 32 bytes / card's signature
- Gives the card description to the terminal
  - Capabilities
  - Communication stuffs to be established




# Smart Card – Application Protocol Data Unit

## APDU :

- Expected by the card after ATR
- Sent by the terminal (handset, card reader,…
- Several parameters
- Status Word expected
- Refer to documentation
  - *ISO 7816-4*

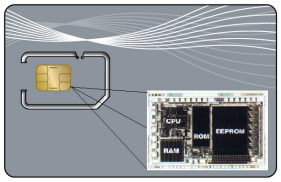



# Smart Card – Application Protocol Data Unit

## A five bytes message :

- byte 0: CLA, class of the command
- byte 1: INS, type of the command
- byte 2: P1, parameter 1
- byte 3: P2, parameter 2
- byte 4: LC, length of extra data

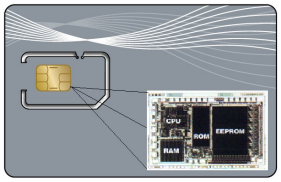
| CLA | INS | P1 | P2 | LC |
|---|---|---|---|---|






# Example : read & update a binary file

- **You first need to select it:**
  - *Select File: A0 A4 00 00 02 (FileID)* → **`A0 A4 00 00 02 2FE2`**
- **Then read from it:**
  - *Read Binary: A0 B0 offset(2) (Len)* → **`A0 B0 00 00 0A`**
- **Then update (if you have permission)**
  - *Update Binary: A0 D6 offset(2) Len Data*






# SW1 SW2: Status Word

- Coded in 2 bytes
- Gives the execution result
- 0x9000 stands for SUCCESS
- Refer to documentation
  - *ISO 7816-4*
  - *3GPP 31.102 for (U)SIM scope*