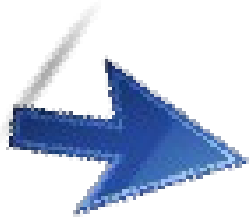
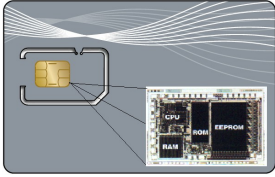


# Academic Day on Mobile Solutions for Senegal 2010 - June 7, 8 and 9 - Dakar



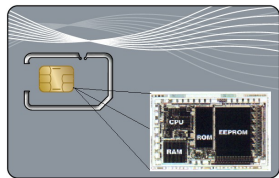
## SIM Card, SIM based Applications & Solutions

*June 8<sup>th</sup>, 2010  
Dakar, Senegal*

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



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

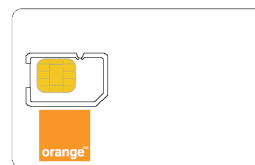


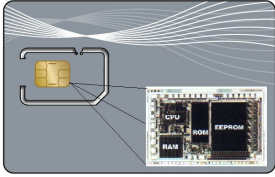
## SIM Card, SIM based Applications & Solutions

### (U)SIM Card

#### AGENDA

- **Overview**
- **Standardization (ISO-ETSI-3GPP)**
- **How (U)SIM card operates?**
- **(U) SIM card validation process**

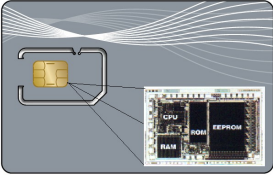




# (U)SIM Card – Overview

- **Microprocessor**
  - CPU
  - RAM
  - ROM
  - EEPROM
  - Security
  - Standards: ISO 7816 + 3GPP/ETSI
- **Result: (U)SIM card is a Smart card**





# (U)SIM Card – Description (1/2)

## (U)SIM : (Universal) Subscriber Identity Module

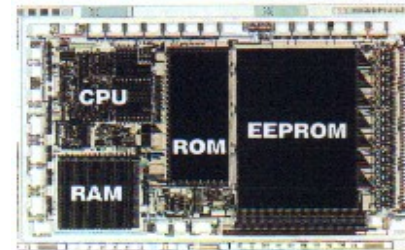
- A plastic card

→ *Branded or not*



- ... with a microprocessor

→ *CPU + memories*

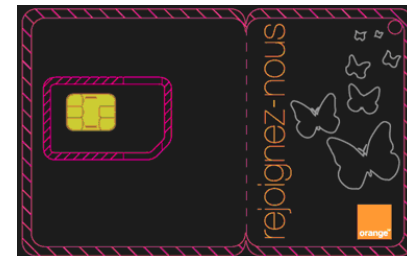


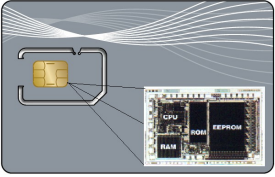
- ... and a stamp

→ *for contacts availability*



- ... Then embedding + cutting

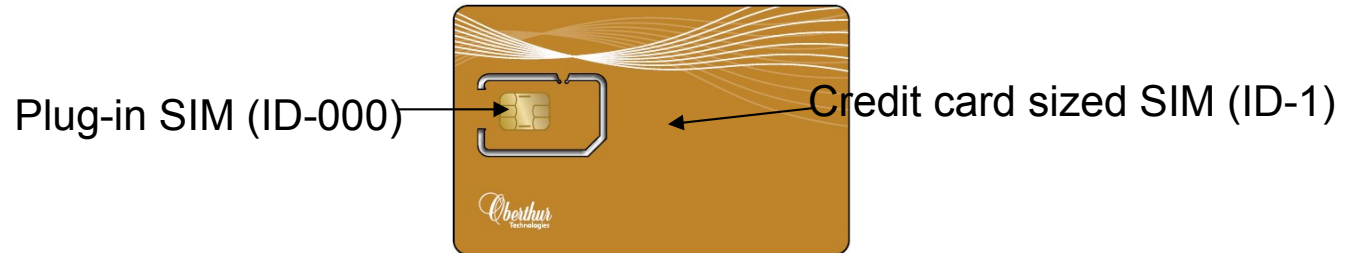




# (U)SIM Card – Description (2/2)

## How (U)SIM is used?

- To access GSM & UMTS networks



- **IMSI: International Mobile Subscriber Identity**

→ Subscription reference: 608xxxxxxxxxxxx (always 15 digits)

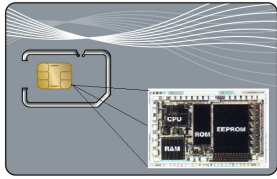
- **MSISDN: Mobile Station ISDN Number**

→ Mobile number: +221 7x xxx xx xx

- **ICCID: Integrated Circuit Card ID**

→ Card serial number: 89221xxxxxxxxxxxxxxxx (17 to 20 digits)

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

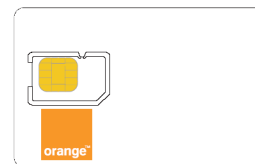


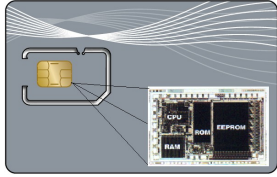
## SIM Card, SIM based Applications & Solutions

### (U)SIM Card

#### AGENDA

- Overview
- Standardization (ISO-ETSI-3GPP)
- How (U)SIM card operates?
- (U) SIM card validation process



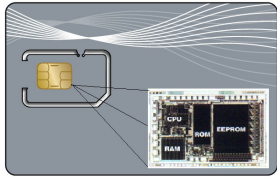


# (U)SIM Card – Standardization

---

## (U)ICC is the (U)SIM hosting hardware

- **ICC → Integrated Circuit Card**
  - SIM hosting hardware
  - Mono application
  - 2G only
- **UICC → Universal Integrated Circuit Card**
  - USIM hosting hardware
  - Multi application
  - 2G/3G



# (U)SIM Card – Standardization

- **ISO for Smart card level**

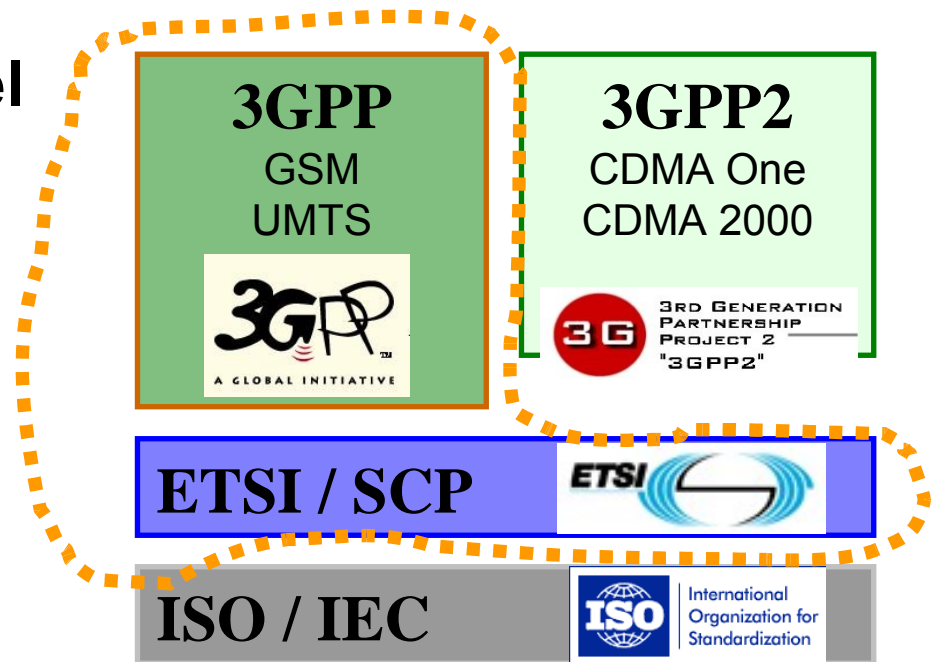
- **ETSI for (U)ICC**

Vendors, administrations, operators, research centers service providers

- **3GPP for (U)SIM**

ETSI, ARIB/TTC (Japon), CCSA (Chine), ATIS (Amérique du nord), TTA (Corée du sud)

- **3GPP2 for CDMA**

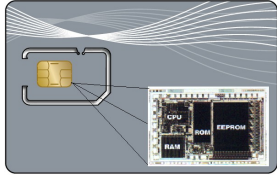


ETSI: European Telecommunications Standardization Institute (<http://portal.etsi.org>)

3GPP: 3rd Generation Partnership Project (<http://www.3gpp.org>)

3GPP2: 3rd Generation Partnership Project 2 (<http://www.3gpp2.org>)





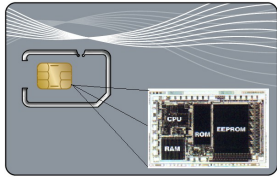
# (U)SIM Card – Standardization

---

## VERY IMPORTANT NOTE

- **(U)ICC: Universal Integrated Circuit Card**
  - Physically secure device
  - Can be inserted and removed from a terminal
  - 1 or more applications such as SIM, USIM, CDMA
- **(U)SIM: Universal Subscriber Identity Module**
  - It is an application
  - Hostable by (U)ICC
  - Provides access to GSM/UMTS networks

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

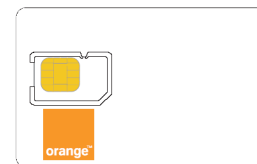


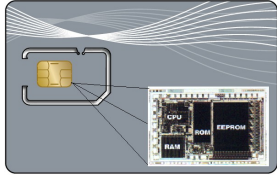
## SIM Card, SIM based Applications & Solutions

### (U)SIM Card

#### AGENDA

- Overview
- Standardization (ISO-ETSI-3GPP)
- How (U)SIM card operates?
- (U) SIM card validation process





# (U)SIM Card – Basic purpose

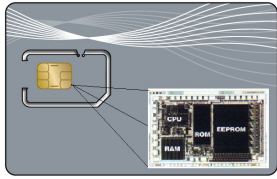
**Reliable authentication  
of subscribers**



**Subscriber – (U)SIM pairing:  
thanks to the PIN code**



**100% reliable billing**



# (U)SIM Card – GSM authentication



Visited network



VLR

Home network

AuC/HLR



IMSI

IMSI (TMSI)

IMSI

Subscriber identification

RAND

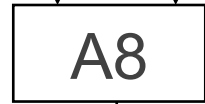
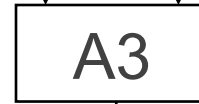
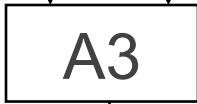
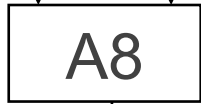
RAND



Ki



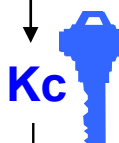
Ki



Kc

SRES

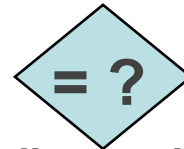
SRES



Kc



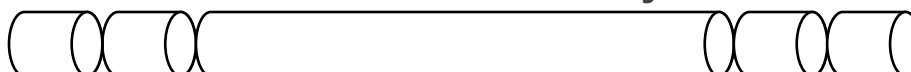
GSM Network



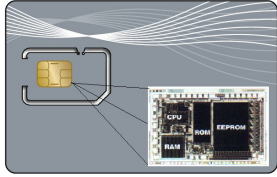
Subscriber authentication

Data confidentiality

10/06/10



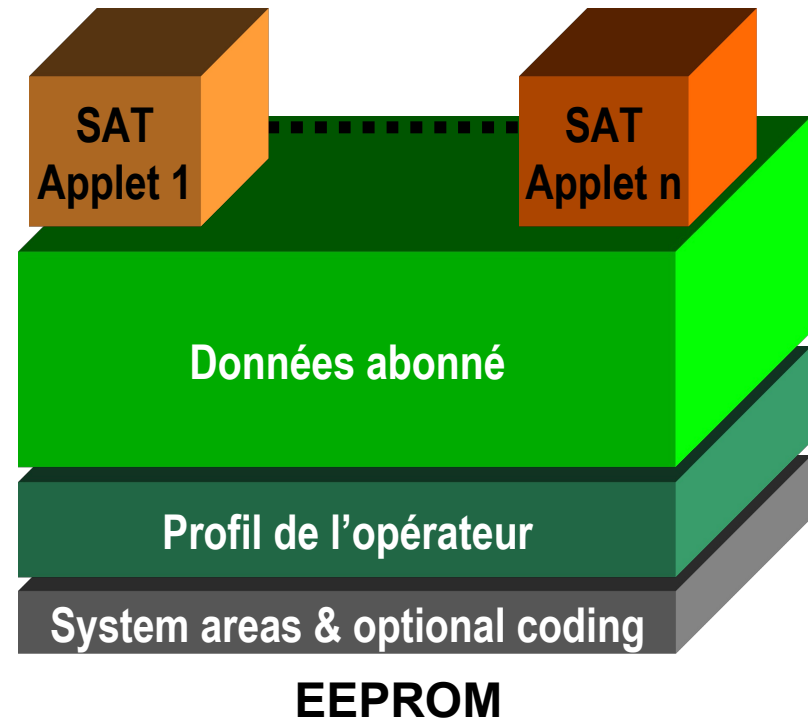
12

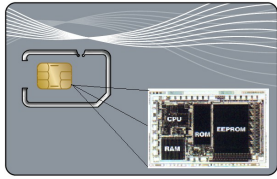


# (U)SIM Card – How does it work?

## Applicative components

- Authentication algo in OS
- Services in EEPROM/Flash
  - Operator profile (network name, SMSC number, service numbers,...)
  - Subscriber's information ( phonebook, SMS, last dialled numbers...)
  - SAT Applications (for specific services, value added services, etc...)





# (U)SIM Card – How does it work?

## Native & Java (U)SIM card

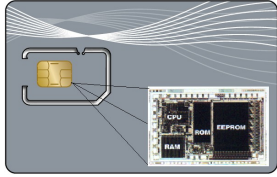
### ■ Native card

- ISO compliant → Physical and electrical
- ETSI compliant → (U)ICC i.e. multiapplication
- 3GPP compliant → running with a (U)SIM application
- Generally 16 to 32Kb
- **Vendor proprietary mechanism for everything else**

### ■ Java card

- Similar to native card apart from proprietary mechanisms
- **Built-in Java Virtual Machine**
- **Built-in Java API**
- **Capable of running java applications**
- **Standardized by JavaCard Forum**
- **Interoperable**
- **Minimum 32Kb, up to 512Kb**





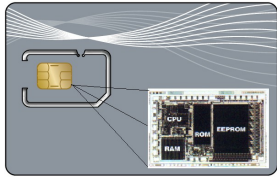
# (U)SIM Card – How does it work?

---

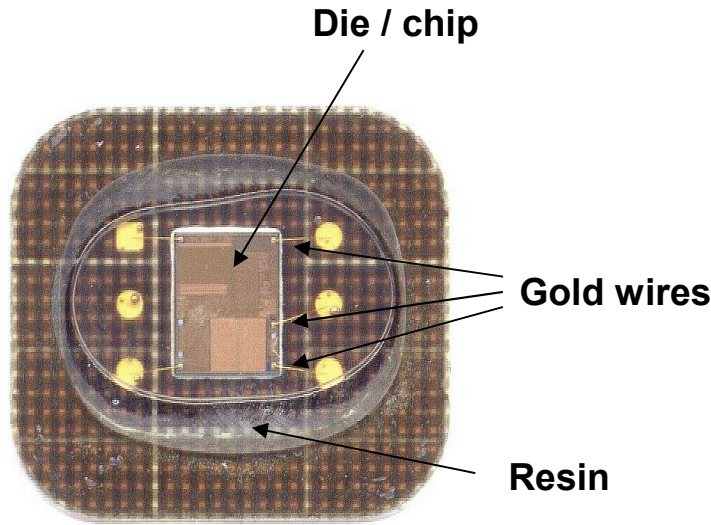
## (U)SIM card life cycle (1/2)

- **Card manufacture**
  - *OS put in ROM*
- **Initialisation**
  - *(U)SIM application in EEPROM*
- **Personalization**
  - *Operator data in EEPROM*
- **Operating**
  - *APDU commands exchange with a terminal*
- **Death**
  - *Logical invalidation*

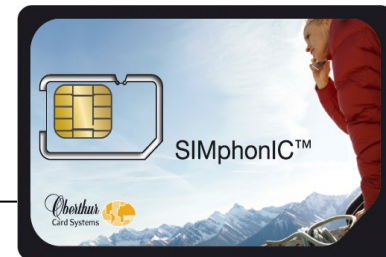
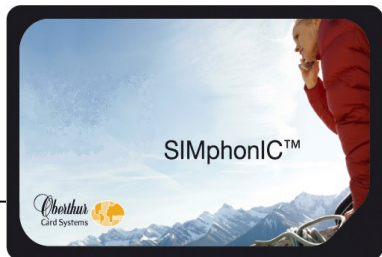
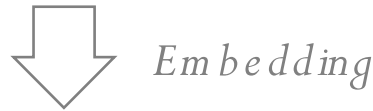
# (U)SIM Card – How does it work?



*White card*

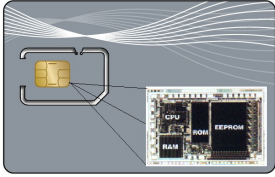


*Module*



*Plug-in Cutting*





# (U)SIM Card – Main operator issues

## **SVA: DSTK, USSD, etc**

Usability Portability  
Interoperability

## **OTA: Over The Air**

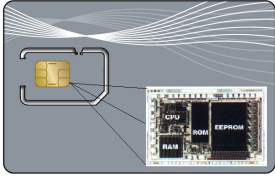
Life cycle extension  
OTA parameters  
Keysets Outputs

## **Performances**

Microprocessor, OS, Production, Card size: 64Kb is most popular in the region

## **Card packaging**

Brand promoting, better logistics  
Ecological impact : EcoSIM Pack

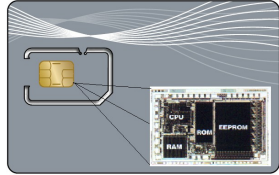


# (U)SIM Card – OTA

---

## OTA: Over The Air

- Remote access to the card
- Secure: shared keys between card and server
- SMS based
- Limited to 4Kbyte
- RFM: Remote File Management
  - File access: *READ, UPDATE, RESIZE, etc.*
- RAM
  - Application access: *INSTALL, DELETE, LOCK/UNLOCK...*



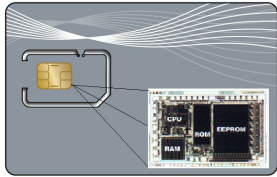
# (U)SIM Card – 2G→3G migration

## 3G card :

- Both SIM and USIM application
- Works on both 2G (GSM) & 3G (UMTS) networks
- ADN is extended
  - *secondary number, email, fax group management...*
- Security
  - *3G algo, more secure*
  - *card & network mutual authentication*



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

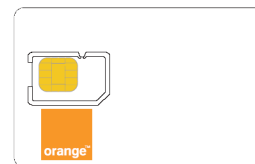


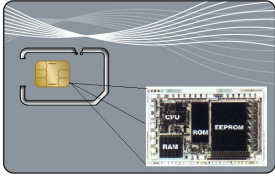
## SIM Card, SIM based Applications & Solutions

### (U)SIM Card

#### AGENDA

- Overview
- Standardization (ISO-ETSI-3GPP)
- How (U)SIM card operates?
- (U) SIM card validation process





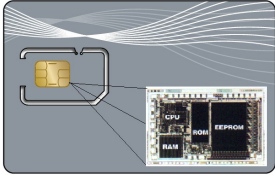
# (U)SIM Card – Validation process (1/2)

## ■ Technical Scope

### Operator's technical specifications

- *Native or Java?*
- *Authentication algorithm*
- *Transport and OP Keys*
- *SMSP, Phonebook*
- *OTA parameters*
- *Applications for Value Added Services*
- ...

Ensure card will  
operate correctly on  
operator's network



# (U)SIM Card – Validation process (2/2)

- **Brand marketing scope**

- Operator's marketing specifications**

- *Card body artwork (visual): adobe ai, photoshop files*
    - *Printing personalization*
    - *Leaflet (user guide) content and design*
    - *Packaging to be used*
    - *Packing details*
    - *Shipment details*
    - ...

Ensure operators  
marketing strategy  
is met