Introduction to SIM Cards

Contents

Part 1 : SIM Concepts

1. Overview of GSM Networks
2. SIM in GSM Networks
3. Introduction to GSM 11.11

Part 2 : SIM Applications

1. Anti-Cloning and Authentication Counter
2. Local Applications
3. Point to Point Applications

Overview of GSM Networks

What is GSM?

Original name:

Groupe
Spéciale
Mobile

GSM now stands for:

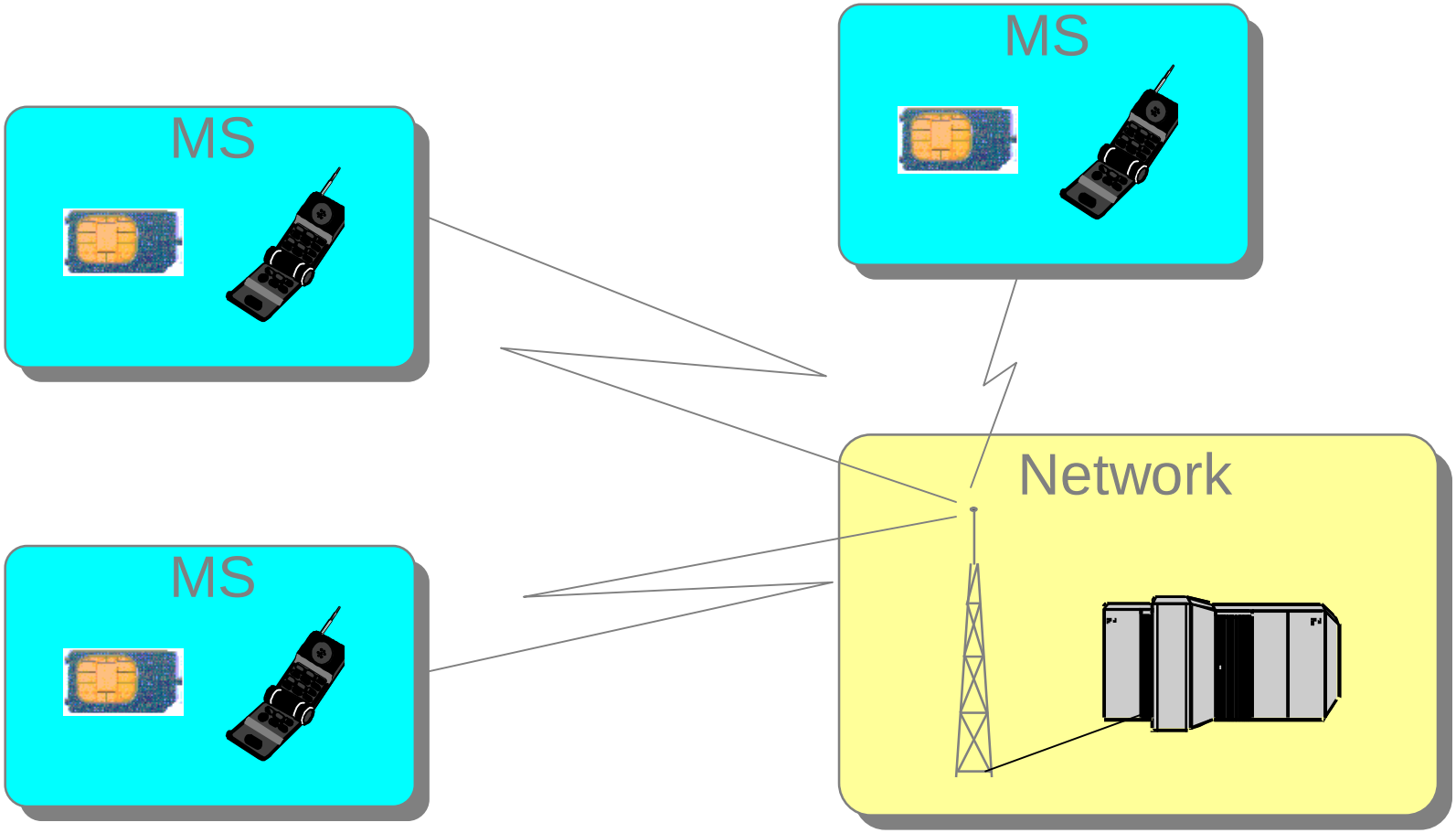
Global
System for
Mobile communication

Key Features of GSM

GSM properties:

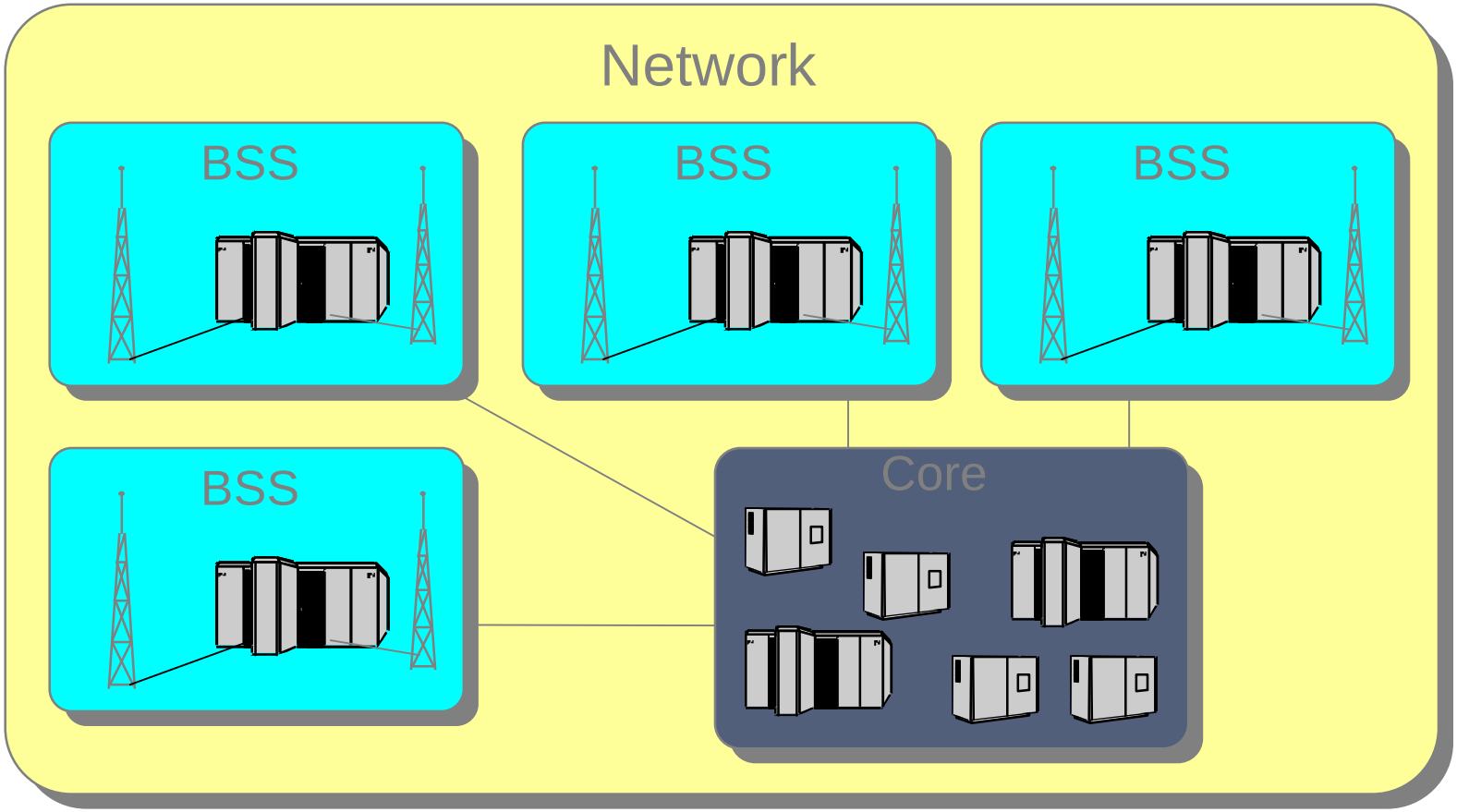
- **Open standard**
- **Provision of roaming**
- **SIM**
- **Digital (ISDN compatible)**
- **TDMA (Time Division Multiple Access)**

Network Elements



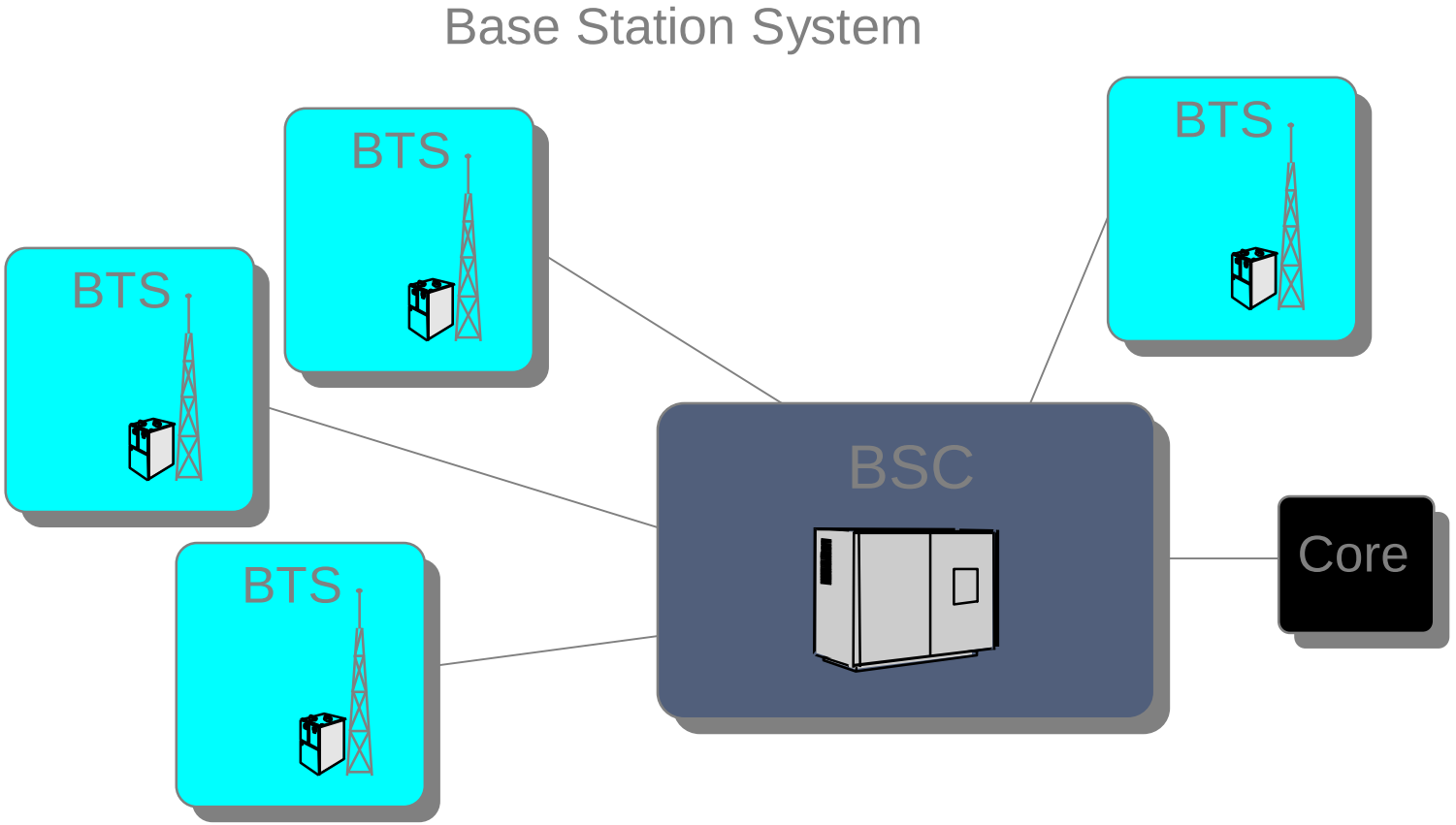
MS: Mobile Station = Mobile equipment + SIM

Network Elements



BSS: Base Station System

Network Elements



BSC: Base Station Controller
BTS: Base Transceiver Station

Network Elements

Abbreviations:

HLR: Home Location Register

VLR: Visiting Location Register

AUC: Authentication Center

EIR: Equipment Identity Register

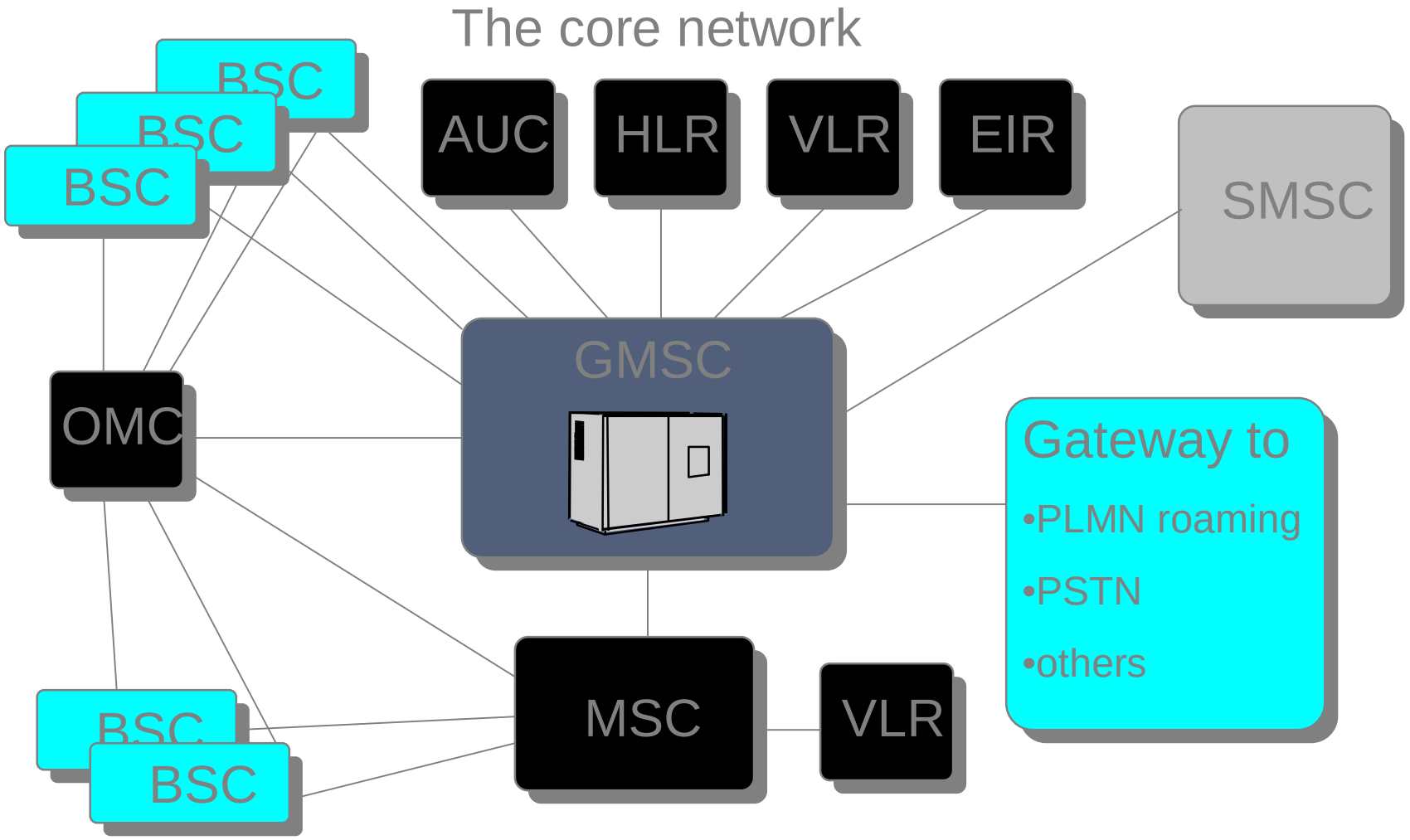
MSC: Mobile Switching Center

GMSC: Gateway MSC

OMC: Operational and Maintenance Center

SMSC: Short Message Service Center

Network Elements



SIM in GSM Networks

What is a SIM?

SIM stands for:

Subscriber

Identity

Module

What is a SIM?

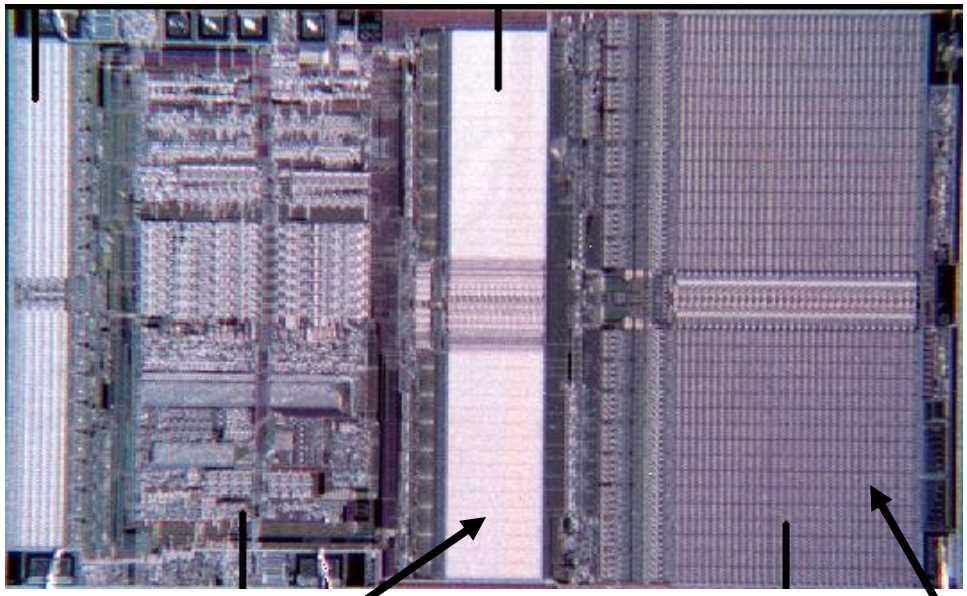
The purpose of a SIM:

- **Identify a user**
- **Authenticate a user**
- **Data storage**
- **Marketing tool**
- **Portable**

What is in a SIM?

Hardware:

- CPU
- I/O devices
- ROM
- RAM
- EEPROM



ROM :

- Basic OS functionality
- GSM functionality
- SIM vendor functionality
- Network operator functionality (optional)
- Fixed data (optional)

EEPROM:

- Setup for OS
- Patches to the OS
- Extensions to the OS
- Data

Architecture of standard SIM

Architecture of first Generation SIM

APDU Dispatch

ISO 7816-4 APDUs

GSM 11.11
Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface

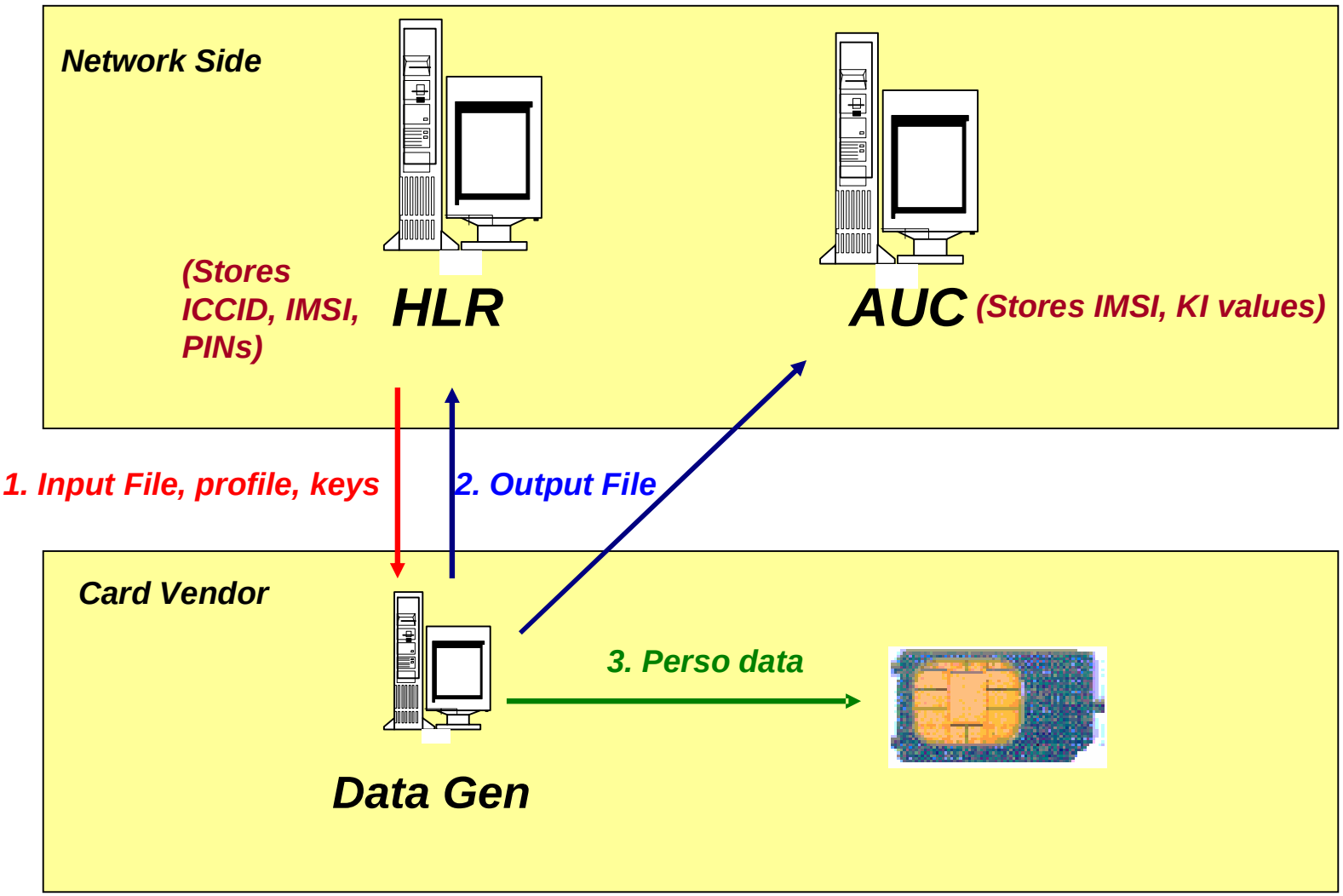
ISO 7816-4 File System

SIM in GSM networks

What is required to activate the SIM in the GSM network?

- Input file
- Output file
- Transport Key (Optional)
- SIM Card (with network profile)
- Algorithm Type

SIM in GSM networks



Input file format

```
*    HEADER DESCRIPTION
****************************************
Customer:   TELCO
Quantity:   4500
Type:       PLUG IN
Profile:    5.0
Batch:      00045
*
Transport_key:          001
*
Address1:   TELCO
Address2:   COUNTRY
****************************************
*    INPUT VARIABLES
****************************************
var_in_list:
IMSI:       238993210070000
Ser_nb:     894502300000070000
****************************************
*    OUTPUT VARIABLES
****************************************
var_out:PIN/PUK/PIN2/PUK2/Code_ADM/KI
```

Quantity

Transport Key Index

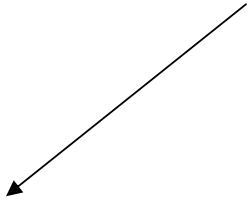
Start IMSI

Start ICCID

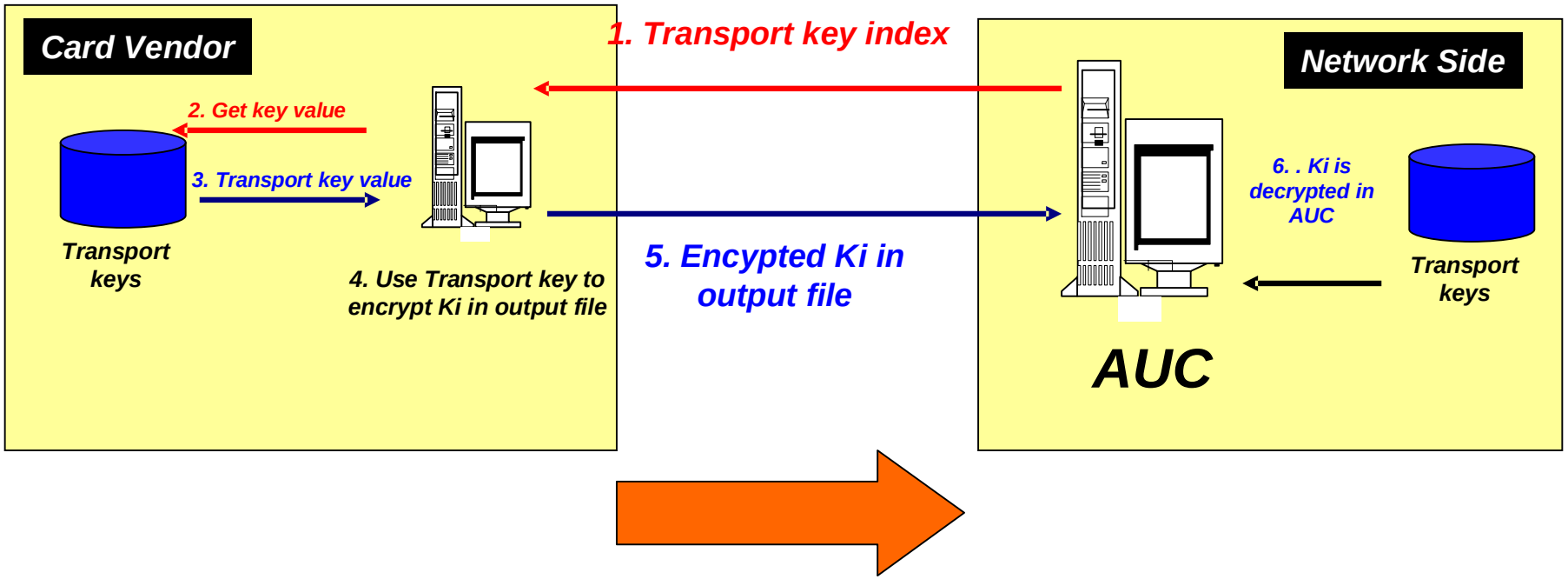
Output file format

```
*     HEADER DESCRIPTION
****************************************
Customer:    TELCO
Quantity:    4500
Type:        PLUG IN
Profile:     5.0
Batch:       00045
*
Transport_key:          001
*
Address1:    TELCO
Address2:    COUNTRY
****************************************
*     INPUT VARIABLES
****************************************
var_in_list:
IMSI:        238993210070000
Ser_nb:      894502300000070000
****************************************
*     OUTPUT VARIABLES
****************************************
var_out:PIN/PUK/PIN2/PUK2/Code_ADM/KI
894502300000070000 238993210070000 1234 12345678 0000 12345678 88888888
12345678901234567890123456789012
```

Subscriber data



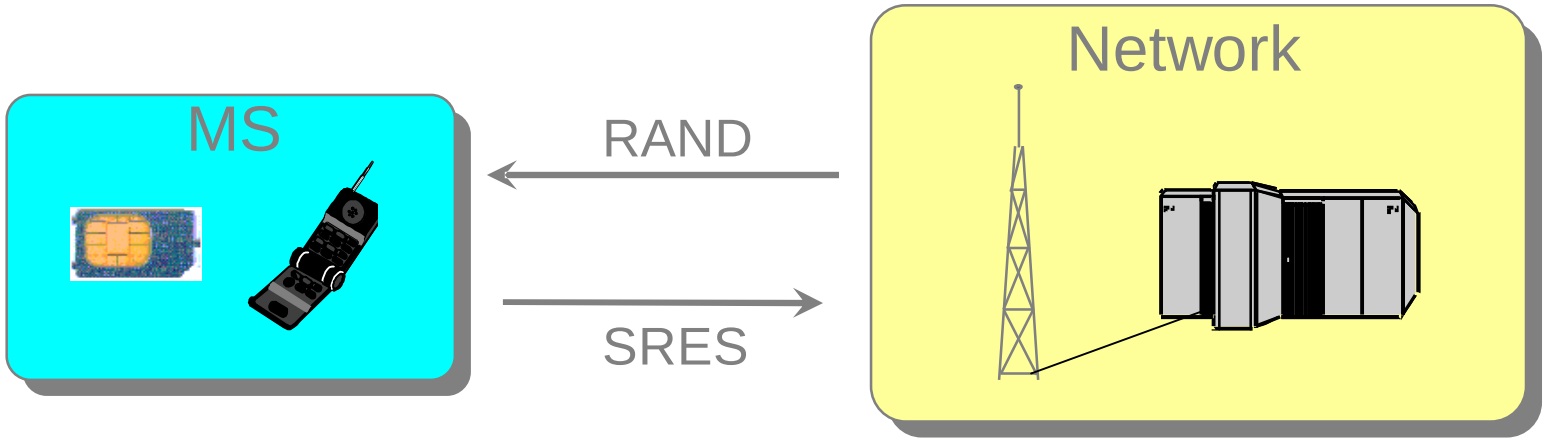
How transport key is used?



Objective : To protect the KI value during transport of file from SIM vendor to Network Operator

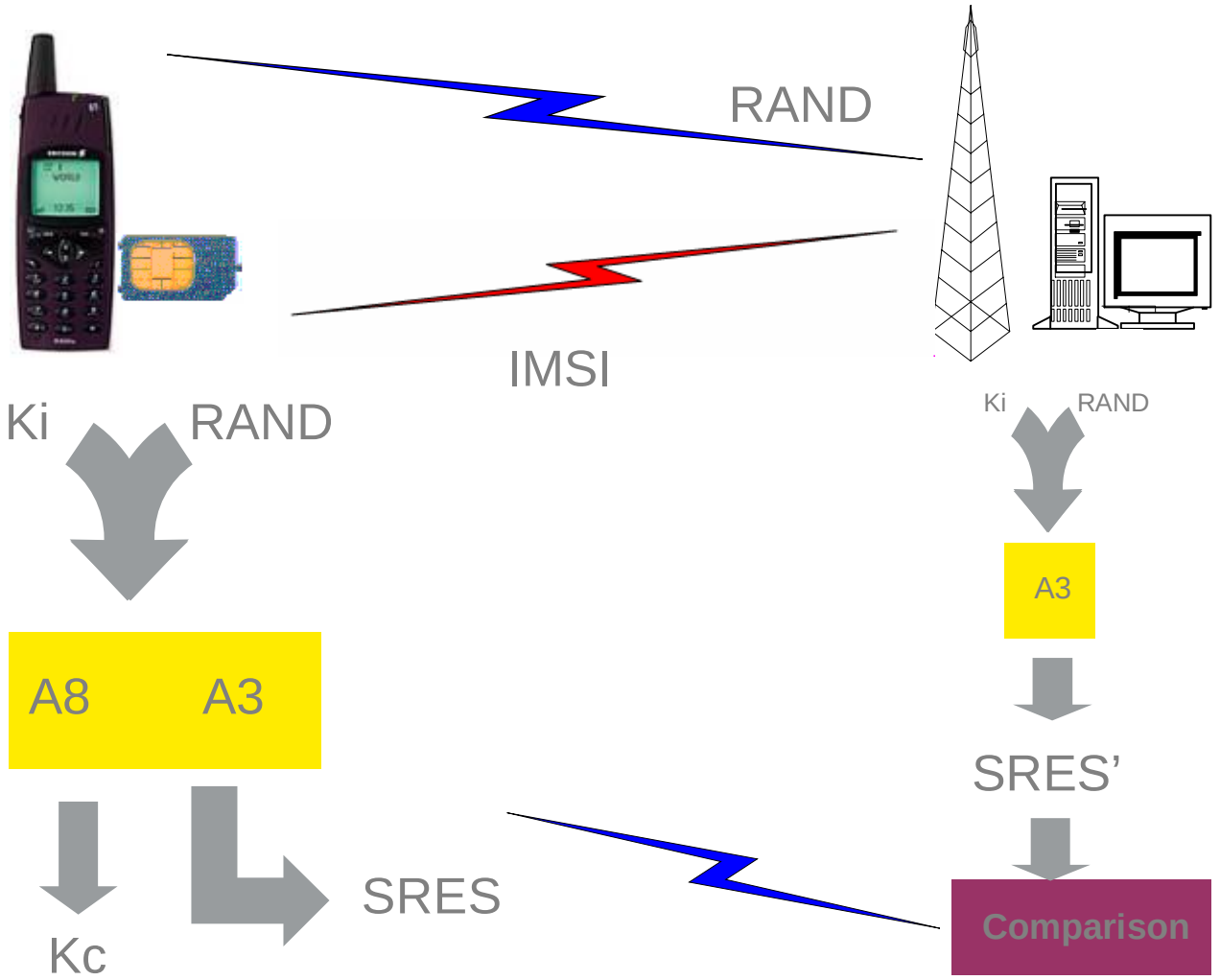
GSM Authentication Process

The action on the air interface

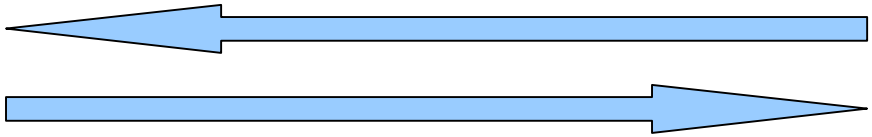


RAND: random value
SRES: response for authentication

GSM Authentication Process



Confidentiality in GSM



Encrypted Voice Data Channel

$A5_{K_c}$[Data]

$A5_{K_c}$[Data]

Comp 128 algorithm

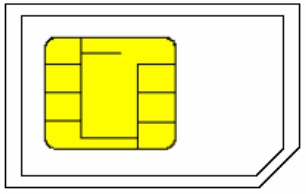
SIM Process	Comp 128 consists of •A3 ð Authentication Algorithm •A8 ð K_c Calculation Algorithm
ME Process	•A5 ð Voice Data Encryption Algorithm

- To use the Comp 128 command, ME calls SIM command: RUN_GSM_ALGO

- RUN_GSM_ALGO returns a 12-bytes response, of which 4 bytes are the SRES, and 8 bytes are the K_c.

Security in GSM

- K_i is never revealed in the network
- K_i is never passed from SIM card to Mobile Phone
- All Authentication Calculations including K_c are done in the SIM card



Introduction to GSM 11.11

GSM Specifications

- Defined by ETSI
  - AKA European Telecommunications Standards Institute
  - All the specs can be downloaded at http://www.3gpp.org/ftp/Specs/

GSM Specifications

Functions of a SIM card

Phase 1	Phase 2	Phase 2+
ØSubscriber Authentication to the network ØPIN protection to Subscriber Data ØPhonebook Storage ØSMS Storage	ØMore Security PIN2 ØFixed Dialing Numbers (FDNs) ØPublic Land Mobile Networks (PLMNs)	ØService Dialing Numbers (SDNs) ØBarred Dialing Numbers (BDNs) ØOver The Air (OTA) ØSIM ToolKit (STK)

GSM 11.11 Basic SIM Specifications

File System

- Purpose of each file
- Default Contents
- Access Conditions

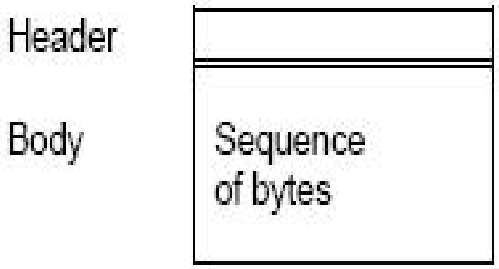
Command Set

- APDU Coding of commands
- Coding of responses
- Communication Protocol

Power Up Procedure

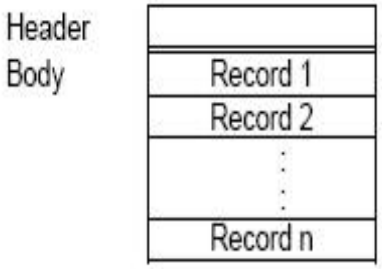
Types of Files

1. Transparent File



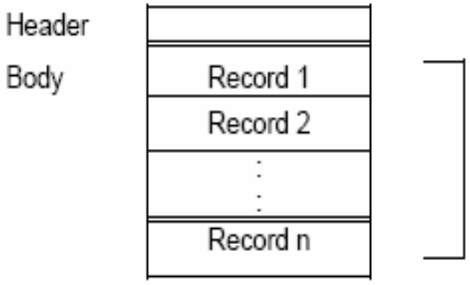
- Ø Consists of sequence of bytes
- Ø Total length of file is defined in the header
- Ø Relative address is used for reading or updating data in file

2. Linear Fixed File



- Ø Consists of sequence of records all having same fixed length
- Ø First record has index number 1
- Ø Number of record and length is defined in the header
- Ø Record Number is used for reading or updating data in file

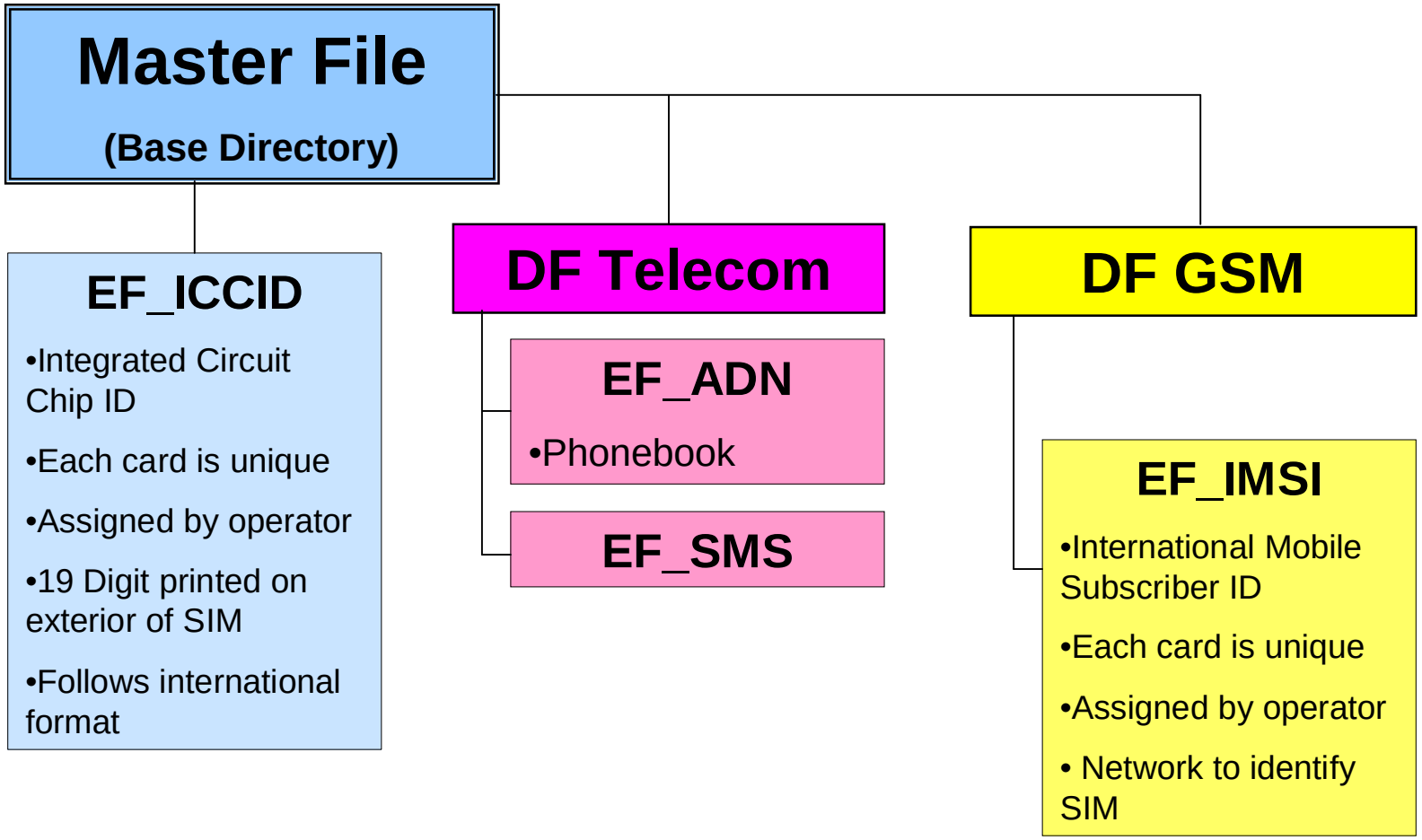
3. Cyclic File



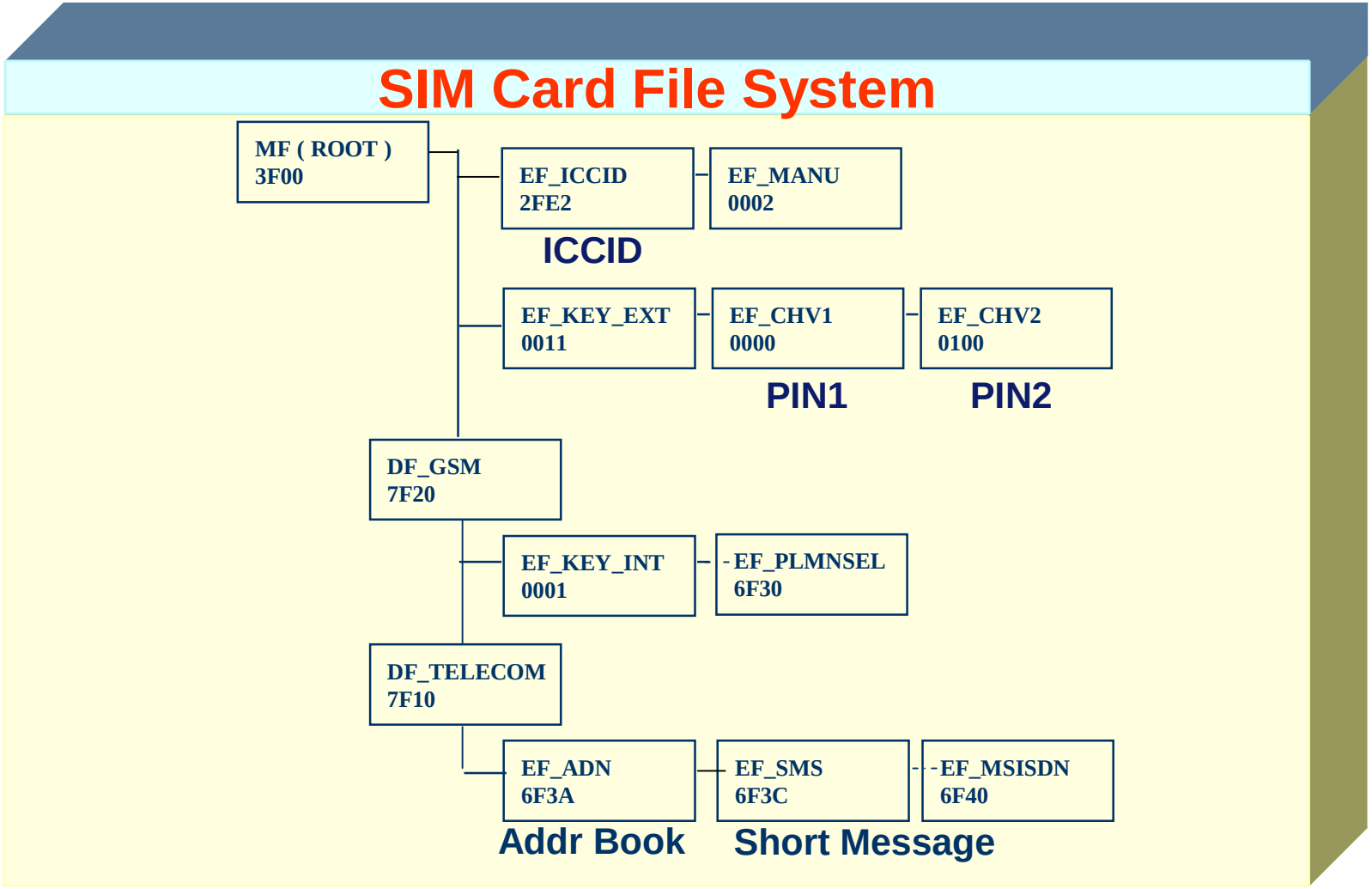
- Ø Consists of sequence of records all having same fixed length
- Ø Number of record and length is defined in the header
- Ø Stores data in chronological order
- Ø When record pointer is at last record, record 1 will be used next

SIM File System, Data and Algo

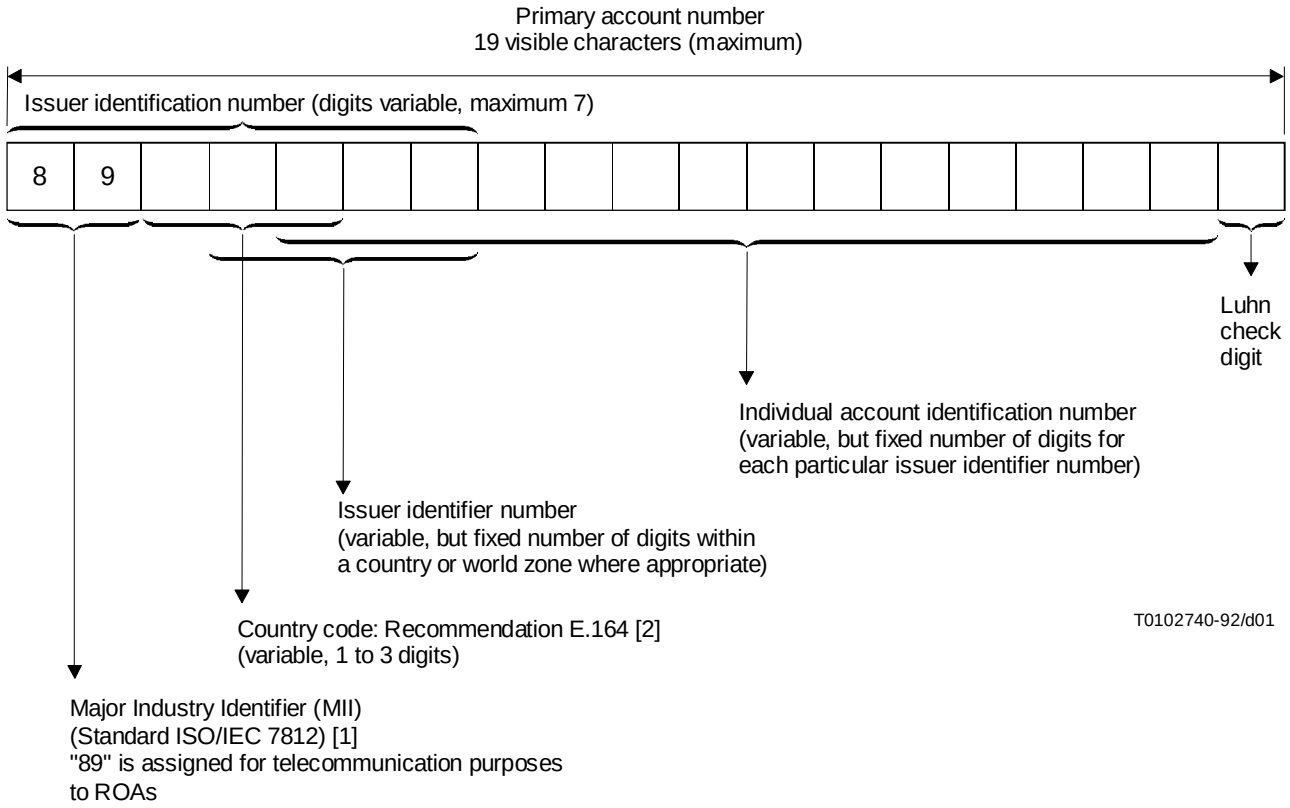
More important Files (EF) and Folders (DF) includes:



SIM File System



Format of ICCID



.

Charge card numbering system

ICCID -format

ICCID is the SIM cards unique identification number and is coded in accordance to ITU-T recommendation E.118 (18).

Format : 89 66 15 XTH YYYYYYYYY C

Number of digits ICCID : 19 digits including check digit

89 : Telecom Application Code

66 : Mobile country Code (eg. Thailand)

18 : Mobile Network Code (eg. DTAC)

X : Card Manufacture Code

T : Type of card (ID-1=1 and Plug-in=2)

H : HLR ID (HLR1=0,HLR2=1,HLR3=2)

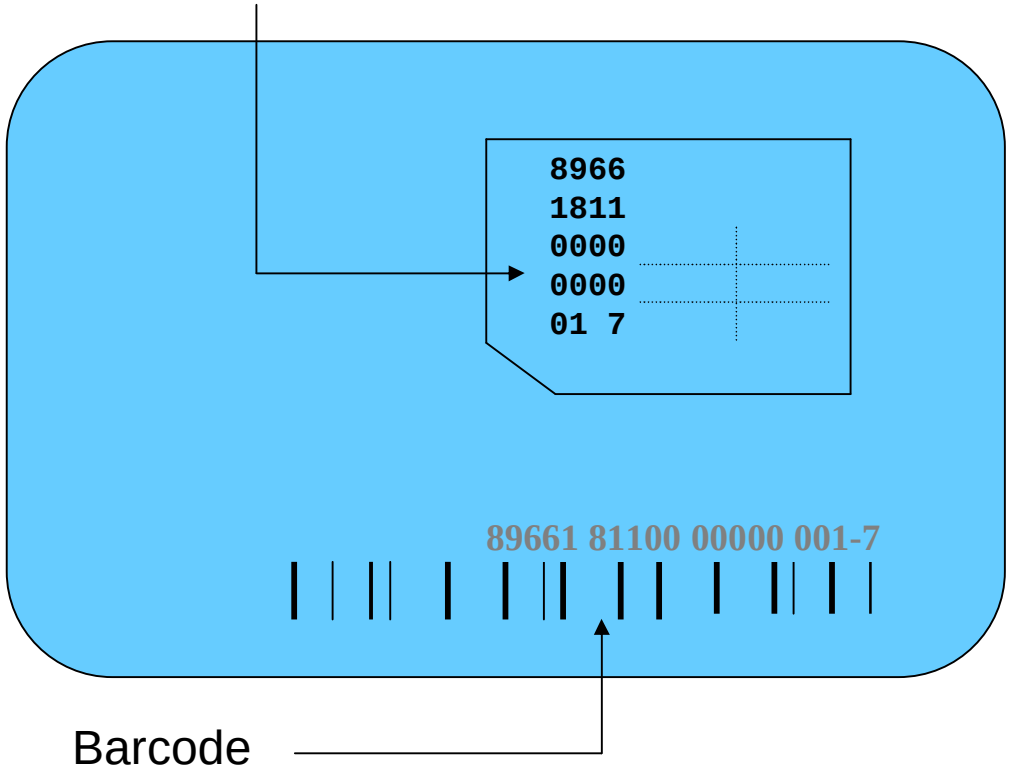
YYYYYYYYY: Sequential Number

C : Luhn key computed from the 18 previous digits (1 nibble)

Example : 89661 51100 00000 001 -7

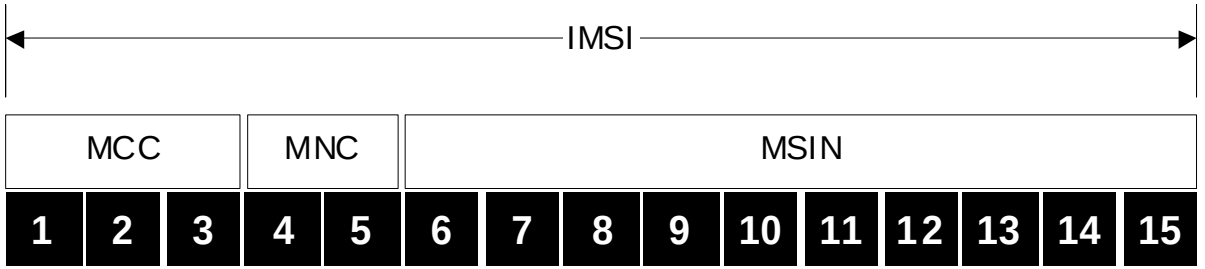
Use of ICCID in Graphical Personalisation

2 rows vertical x 10 digits each row or
5 rows horizontal x 4 digits each row



SIM Data

Format of IMSI



IMSI - format

IMSI Format IMSI is the International Mobile subscriber Identity. Length of IMSI coding must be according to GSM 04.48 [15]. IMSI is coded on 15 digits, according to the following structure:

MCCNCXXXXXXXXXX e.g. 520181000000001

MCC	Mobile network country code defined by GSM11.11. ‘520’ for Thailand.
NC	Network code registered in ITU for the operator. ‘18’ for DTAC.
XX..X	Running number of serial number , included HLR ID

Note : The running number taken from the input file and automatically incremented from the initial value.

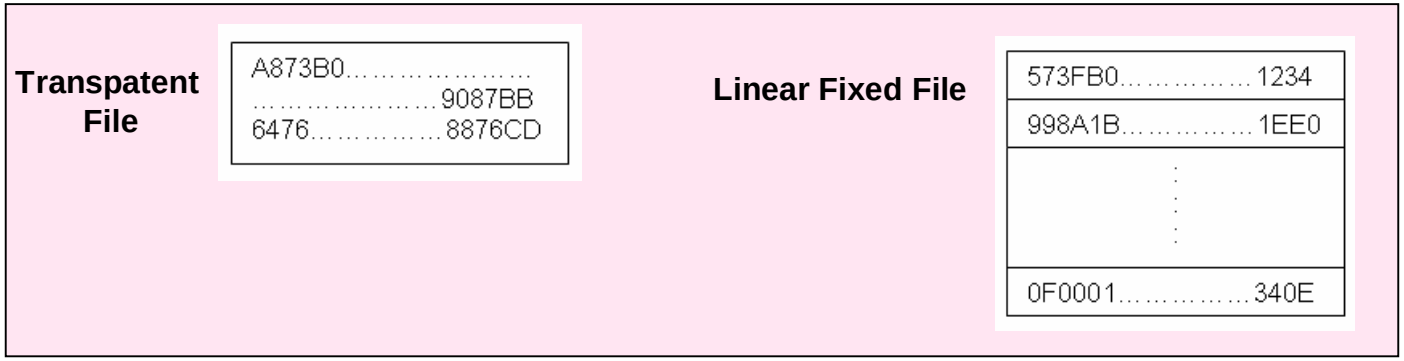
SIM File System, Data and Algo

- Important Data
  - Ki
    - Unique 16 byte secret key used for authentication
    - Usually encrypted with transport key
  - PIN / PUK (Max 8 bytes)
    - Personal Identification Number (3 tries)
    - PIN Unblocking Key (10 tries)
    - Can be fixed or random specified by operators
  - ADM (Max 8 bytes)
    - Administrative PIN (5 tries)

- Important Algo
  - A3/A8 (COMP128)
    - Authentication algorithm
    - Version 1, 2 and 3

GSM Command Set

- Basic GSM 11.11 command set includes
  - Select MF/DF/EF
  - Read Binary
  - Update Binary
  - Read Record
  - Update Record
  - Verify PIN/PUK/ADM
  - Run GSM Algo



Part 2 : SIM Applications

Anti Cloning & Authenication Counter

Hacking of K_i

- Cloning Kits call RUN_GSM_ALGO command many times with a series of Fake RAND
- Analyze SRES returned by the RUN_GSM_ALGO commands
- Ki can be found in 40000 to 80000 RUN_GSM_ALGO commands
- Only Comp128-1 can be hacked now. Comp128-2 and Comp128-3 are safe from hacking

Methods to curb hacking

Authentication Counter

1. SIM Solution

How	Limit the Number of times RUN_GSM_ALGO command can be called
Advantages	Effective in reducing possibility of SIM cloning
Disadvantages	Life Span of SIM compromised Difficult to find optimal limit

Strong Ki

2. Non SIM Solution

How	Software generates K_i values that can withstand Cloning Kits Analysis Only these K_i values are used in Perso
Advantages	No SIM technology needed Easy to Implement Does not compromise SIM Life-Span
Disadvantages	K_i values may still be hacked with new analysis algorithm in the future Customers may not feel safe

Pattern Recognition

3. SIM Solution

How	Detect Fake RAND – eg: Running numbers Detect unusually high percentage of RUN_GSM_ALGO commands received by the SIM card Once Hacking Pattern is detected, return a Wrong SRES value, which will thwart the Analysis Wrong SRES value generation §Random Number Generation §Dummy K_i

3. SIM Solution

Advantages	**Does not compromise SIM Life-Span** **Very effective as it will not be affected by new Cloning Kits**

Comparison of Methods

Comparison table

	Authentication Counter	Strong K_i	Pattern Recognition
SIM Solution	ü	û	ü
Easy to Implement	ü	ü	ü
Maintain SIM Life Span	û	ü	ü
Protection against New Cloning Kits	û	û	ü

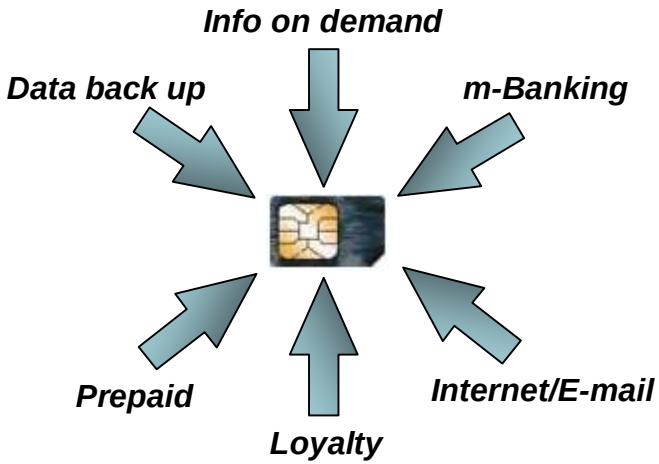
User Applications

Value-Added Applications

Applications Portfolio

§Eastcompeace Applications Portfolio may be divided into 2 main categories:

- üLocal
- üPoint to Point



Value-Added Applications

Local Applications

§Local Applications are stand-alone applications, running into the Mobile Station without producing traffic.

§Eastcompeace offer of Local Applications includes:

- üDual IMSI
- üPhonebook plus
- üEnhanced Phonebook
- üMulti-Inbox
- üPassword Manager
- üWelcome Note

Value-Added Applications

Dual IMSI

- Dual IMSI application allows the operator to offer two different accounts on the same SIM card without any impact on the network side.

- Applications:
  - Private/Business
  - Roaming

- Operator Benefits:
  - Differentiate the product
  - Increase customer satisfaction
  - Target specific subscribers segment

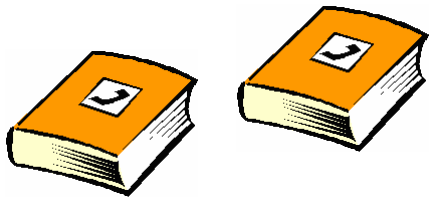
Phonebook Plus

§Phonebook Plus application provides the SIM card with an increased phonebook, up to 500 entries.

§The standard phonebook is duplicated, the user can access by menu two phonebooks, pbook1 and pbook2, each up to 250 entries.

§Phonebook is the unique solution that allows increasing SIM phonebook without changing the user experience.

§Operator Benefits:
- Differentiate the product
- Increase customer satisfaction



Value-Added Applications

Enhanced Phonebook

- USIM:
  - Enhanced Phonebook for USIM allows to access all the 3G Phone Book functionalities (more than 250 entries, second name, additional number, e-mail, …) even from a 2G handset.
  - Enhanced Phonebook makes smoother the 2G migration toward 3G.
- SIM:
  - Enhanced Book for SIM makes 3G Phonebook functionalities (more than 250 entries, second name, additional number, e-mail, …) available on a 2G SIM card.
- Operator Benefits:
  - Differentiate the product
  - Increase customer satisfaction

Mr. White
principal number
second number
email address
second name
group

Value-Added Applications

Multi-Inbox

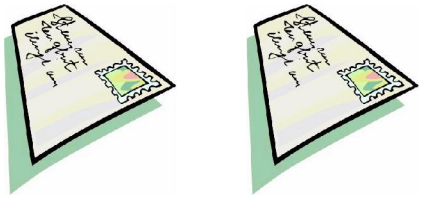
§Multi-Inbox application satisfies the need to store as many SMS as possible.

§The standard Inbox is duplicated, the user can access by menu two Inbox, Inbox1 and Inbox2.

§Once an Inbox is selected, it is managed as the standard SIM Inbox folder, through the ME commands, without changing the user experience.

§Operator Benefits:

- ü Differentiate the product
- ü Increase customer satisfaction



Value-Added Applications

Password Manager

§Password Manager application allows the operator to dedicate a certain amount of memory to the user, where he can store his highly sensitive personal data (credit card number, access codes, …).

§The dedicated space can only be accessed by code presentation.

§The secured data can be stored into a secure application server and securely retrieved in case of the SIM card is lost or stolen.

§Operator Benefits:

- ü Differentiate the product
- ü Increase customer satisfaction
- ü Increase ARPU

Value-Added Applications

Welcome Note

§This application provides a personalized welcome note when the phone is powered up. This application can be used by the operator to display the service branding and the customer ŝ subscription plan, which will help our customers to guarantee loyalty by improving the user experience.

§Welcome message can be modified via OTA, which is a perfect marketing tool to inform each customer of relevant new services or offers available!

Value-Added Applications

Point-to-Point Applications

§Point to point applications provide end to end connections to the users. The aim is to offer value added services, generating traffic and revenue for the operator.

§Eastcompeace offer of Point to Point applications includes:

- üSmart Lock
- üGroup SMS
- üMy Secret SMS
- üFlash SMS

Smart Lock

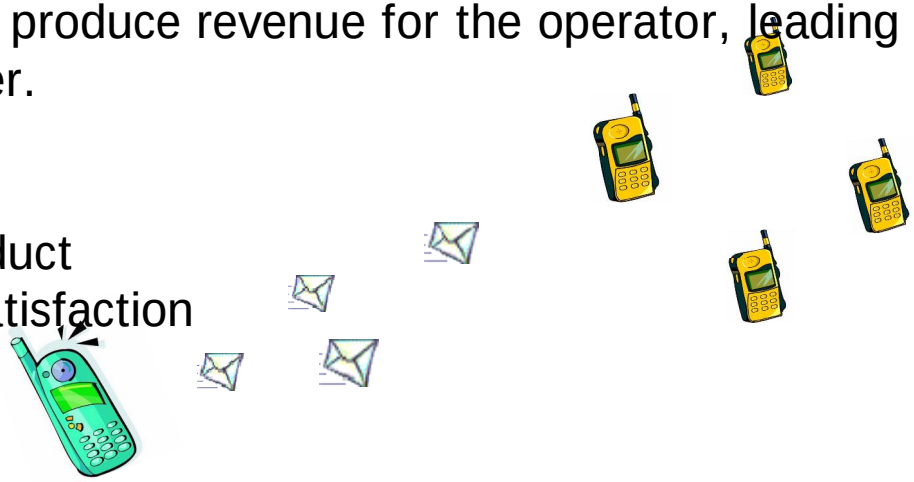
§Smart Lock application provides a feature to prevent unauthorized use of your mobile phone. If the user forgot to carry his/her mobile phone or lose it, the user can send a special SMS to his/her phone to lock the SIM card with PIN1.

- ü The STK-SMS must follow a special format and include a password
- ü The password can be set through your SIM card ś STK menu
- ü The SIM card can be unlocked by presenting the password again through the STK menu

Value-Added Applications

Group SMS

- Group SMS application assists the user to broadcast information.
- Once a group is defined, the application allows to send a SMS to the entire group by single operation.
- Definitely, this application produce revenue for the operator, leading to increase SMS traffic per user.
- Operator Benefits:
  - Differentiate the product
  - Increase customer satisfaction
  - Increase ARPU



Value-Added Applications

My Secret SMS

- My Secret SMS application allows the user to send/receive anonymous SMS, protected by PIN.

- Upon the arrival of a secret SMS, the user experience is to receive a standard SMS, the text of which, configurable by the same user, represents the notification of the arrival of a secret SMS.

- The "Secret Inbox "can be accessed via menu after a PIN code presentation.

- Operator Benefits:
  - Differentiate the product
  - Increase customer satisfaction
  - Increase ARPU

Flash SMS

§ Flash SMS application offers mobile subscribers the following features:

- ü Upon receiving SMS, the contents of the SMS are displayed on the mobile phone screen
- ü the SMS will not be stored in inbox directly
- ü User scroll down to read the SMS
- ü At the end of the SMS, the user shall be prompted to save or discard the SMS

Thank you J




We are always willing to grow with you.