SIM Smart Card Overview
Smart Card Introduction

Java Card

Java Card Based SIM

Development Environment

Service Examples
Smart Cards?

- A smart card is a plastic card that contains an embedded integrated circuit (IC)
- Examples:
  - Student Cards
  - Credit Cards
  - Cell Phone SIM/USIM Cards
  - ...
What makes Smart Cards so smart?

Card with microprocessor capable of

- **Storing** information
- **Processing** information
- Add authentication and secure access to information

This is what makes a smart card smart

Stupid cards cannot do this
What’s in a Card?
Contact or Contact Less?

- Contact smart cards work by communicating via physical contact between a card reader and the smart card.

- Contact less smart cards communicate by means of a radio frequency signal, with a typical range of less than 2 feet.
Typical Configuration

Memory Capacity
RAM : 256 bytes to 4KB
ROM : 8KB to 64 KB
EEPROM: 8KB to 64KB
Microprocessor : 8-bit to 16-bit
Advanced Configuration

• GIGAntIC™ combines the unrivaled security features of 3G SIM cards with up to 256 MB
• Strong cryptographic algorithms will protect the value chain of digital content distributions
• Allowing operators to propose innovative high ARPU-generating services
Smart Card Introduction

Java Card

Java Card Based SIM

Development Environment

Service Examples
Architecture

- Smart card hardware
- Java Card platform (Java Card Runtime Environment)
- Java Card Virtual Machine
- Java Card API (mini OS)
- Applet
Typical Flow

Java Card Platform
(Java Card Runtime Environment)

smart card hardware

terminal

applet

applet

applet
Where is the Java?

• A subset of Java
  no threads, no doubles, garbage collector optional ...
• With some extras
  persistent and transient objects
  transaction mechanism
• And increased language-level security
  standard sandbox (cf. web-browsers)
  plus firewall between applets
Smart Cards vs Java cards

**Smart Card**
- One program (applet)
- Written in chip-specific machine code
- Burnt into ROM

**Java Card**
- Multi-application: several applets on one card
- Applet written in high-level language
- Compiled into byte code
- Interpreted on card
- Stored in EEPROM
- Post-issuance: adding or deleting applets on card
Smart Card Introduction

Java Card

Java Card Based SIM

Development Environment

Service Examples
SIM (Subscriber Identity Module)

- Mandatory in every GSM phone
- Identifies the mobile phone “user
- Enables the roaming between different networks
- Issued and managed by the operator
Information Stored By The SIM Card

- Network specific information used to authenticate and identify subscribers on the Network
- Authentications keys
- Possibly phone number (operator dependent)
Most SIM cards are Java Card™ based
Leading Vendors

- Gemalto
- NXP
- Sagem Orga
- Oberthur Card Systems
- SafeNet
- Trusted Logic
Java Card Based SIM

SIM Toolkit Framework

- GSM Applet
- Toolkit applet
- Applet
- Loader Applet

Java Card Platform
(Java Card Runtime Environment)

smart Card Hardware

Toolkit Registry
Toolkit Handler
File System
SIM Toolkit

- Set of commands which define how the card should interact with handset
- SIM initiates commands independently of the handset and the network – has a proactive role.
SIM Toolkit Session Example

Terminal Profile

91XX

Fetch

Data (SetUpMenu) + 9000

Terminal Response

9000

Envelope (Menu selection)

91XX

Fetch

Data (Proactive commands) + 9000

Terminal Response

91XX

....
Proactive Command Examples

Setup Menu

- NETWORK
- BANKING
- NEWS
- WEATHER

Display Text

- The weather today is going to be fine.

Get Input

- Please enter name:

Select Item

- BANKING
- BALANCE
- PURCHASE
- TRANSFER

Send SMS

- SMS in progress.
- Please Wait...

Setup Call

- CALLING
  01 4746 6667
- Please Wait...
Three Development Stages

1. Application Creation
2. Application Loading
   - Balance
   - Last transactions
   - Transfer
   - Invoices
   - Call Bank
3. Application Execution
Smart Card Introduction
Java Card
Java Card Based SIM
Development Environment
Service Examples
VirtuoSimo™: The Universal Wireless Development, Test and Debugging Tool
JCOP (IBM/NXP)
Smart Card Introduction

Java Card

Java Card Based SIM

Development Environment

Service Examples
NFC: Near Field Communication

For Patient ID cards
   More accurate and secure

Tracking package tags
   - Drug inventory, logistics tracking, etc.

Demo
   - ID scanning application using Gemalto’s Proximera SIM
   - Can also use J2ME
Integrated Management of Childhood Illness

- Guides health workers through the 5 leading illnesses responsible for 70% of child deaths

- SIM-based IMCI originally proposed by Dr. Alvin Marcelo (Philippines) for use in his community health projects in remote rural areas
MAC = Message Authentication Code
E = Event Counter
K = Derived DES Key

Bekoz Central

+123456789
MAC 63987455

BEAM Server (HSM)

+123456789?

Card No. Last OTP

OTP = 63987455

Bekoz - The New Way to Move Money

MAC = Message Authentication Code
E = Event Counter
K = Derived DES Key

Authenticator Algorithm

Send USD 12.32 +44987654321 63987455 MAC

SMS from Mobile No: +123456789

USD 12.32

PIN ****

$12.32 to

+44987654321
Implications For Comverse

- Discuss meeting with Oberthur

  Possible next steps:
  - Existing products:
    - Vvm

  Innovations:
  - Motion
  - Location
  - NFC
  - ...
