Lecture 26: SIM Card and Interface, eSIM Concept and Advantages

Mobile Device

DI05011011: Mobile Communication

Agenda for Today

- 1. Introduction to SIM (Subscriber Identity Module)
- 2. SIM Card Physical Evolution
- 3. SIM Card Architecture
- 4. Security in SIM (Ki, PIN, PUK)
- 5. SIM Card Interface
- 6. What is eSIM? (Embedded SIM)
- 7. eSIM Architecture (eUICC)
- 8. Remote SIM Provisioning (RSP)
- 9. Advantages of eSIM
- 10. Traditional SIM vs eSIM Comparison

Introduction to SIM

- **SIM** stands for Subscriber Identity Module.
- It is an integrated circuit (IC) that securely stores the International Mobile Subscriber Identity (IMSI) number.
- The IMSI uniquely identifies a subscriber on a mobile network.
- Without a SIM card, a GSM or LTE phone cannot authenticate and connect to a carrier's network.
- It also stores SMS messages, contact information, and network-specific data.

SIM Card Physical Evolution

- Over the years, the physical size of SIM cards has drastically reduced to save space in mobile devices.
- **Full-size SIM (1FF):** Credit card size, used in early cell phones.
- **Mini-SIM (2FF):** The 'standard' SIM used in early 2000s.
- **Micro-SIM (3FF):** Introduced with smartphones like iPhone 4.
- **Nano-SIM (4FF):** Currently the most common physical SIM, with almost zero plastic border around the chip.

SIM Card Architecture

- A SIM card is a smart card containing a microcomputer.
- **CPU:** A microprocessor for executing security algorithms.
- **ROM (Read-Only Memory):** Contains the operating system of the SIM.
- **RAM (Random Access Memory):** Used for temporary data processing during execution.
- **EEPROM (Electrically Erasable Programmable Read-Only Memory):** Non-volatile memory storing user data (IMSI, contacts, SMS, Ki).

Security in SIM

- **Ki (Authentication Key):** A 128-bit key stored securely on the SIM. It never leaves the SIM card. It is used to authenticate the user to the network.
- **PIN (Personal Identification Number):** Protects the SIM from unauthorized use. User must enter it when turning on the phone.
- **PUK (Personal Unblocking Key):** Used to unblock a SIM if the PIN is entered incorrectly too many times.

SIM Card Interface Pins

- A standard SIM card has electrical contacts (pads) that interface with the mobile phone.
- **VCC (C1):** Power supply voltage.
- **RST (C2):** Reset signal.
- **CLK (C3):** Clock signal for timing.
- **GND (C5):** Ground reference.
- **VPP (C6):** Programming voltage (rarely used in modern SIMs).
- **I/O (C7):** Serial Input/Output for data transfer.

Example: SIM Interface Communication

- **Scenario:** Mobile phone powers on.
- 1. Phone applies **VCC** (Power) to the SIM.
- 2. Phone provides **CLK** (Clock) signal.
- 3. Phone sends **RST** (Reset) to initialize the SIM.
- 4. SIM responds on the **I/O** line with an ATR (Answer To Reset) string, indicating its capabilities.
- 5. Phone and SIM begin exchanging APDUs (Application Protocol Data Units) for authentication.

What is eSIM? (Embedded SIM)

- **eSIM (embedded SIM)** is a programmable SIM card that is permanently soldered into the device's motherboard.
- It eliminates the need for a physical, removable SIM card.
- Standardized by the GSMA (Global System for Mobile Communications Association).
- Allows users to change service providers over-the-air (OTA) without swapping physical cards.

eSIM Architecture (eUICC)

- The hardware component of an eSIM is called **eUICC (embedded Universal Integrated Circuit Card)**.
- Unlike a traditional SIM which holds a single network profile, an eUICC can hold multiple profiles simultaneously.
- Only one profile is typically active at a time, but switching is instant.
- Contains strong cryptographic enclaves to securely download and install operator credentials.

Remote SIM Provisioning (RSP)

- **RSP** is the GSMA specification that allows a device to securely download a SIM profile over the internet.
- **SM-DP+ (Subscription Manager Data Preparation):** The server that securely encrypts and delivers the operator profile to the eSIM.
- **LPA (Local Profile Assistant):** Software on the device that interacts with the SM-DP+ and user interface to manage profiles.
- User typically scans a QR code or uses a carrier app to trigger RSP.

Advantages of eSIM

- **Space Saving:** Tiny footprint compared to a Nano-SIM tray mechanism, allowing for larger batteries or thinner devices.
- **Water/Dust Resistance:** Removing the SIM tray removes a major point of ingress for water and dust.
- **Easy Switching:** Users can switch carriers instantly, beneficial for international travel.
- **IoT Enabler:** Ideal for connected cars, smartwatches, and industrial IoT where swapping physical SIMs is impractical.
- **Logistics:** Carriers don't need to manufacture and ship plastic cards.

Traditional SIM vs eSIM Comparison

- — Feature — Traditional SIM — eSIM (eUICC) —
- ——————
- — **Form Factor** — Removable Plastic Card — Soldered IC (MFF2) —
- — **Provisioning** — Pre-programmed by carrier — Remote SIM Provisioning (OTA) —
- — **Profiles** — Single Profile — Multiple Profiles —
- — **Device Design** — Requires slot/tray — Saves space, better sealing —
- — **Logistics** — Physical shipping required — Digital delivery (QR code/App) —

Summary

- The SIM card is a smart card that securely authenticates a mobile subscriber to a network.
- It contains a CPU, memory, and interfaces via standardized pins (VCC, CLK, I/O).
- eSIM (eUICC) replaces the removable card with a soldered, programmable chip.
- Remote SIM Provisioning (RSP) allows for OTA carrier switching.
- eSIMs offer significant advantages in device design, IoT scalability, and user convenience.

Next Lecture Preview

- In the next lecture, we will explore the internal architecture of the smartphone itself:
- **1. Smartphone Architecture:** System on Chip (SoC)
- **2. Mobile Sensors:** Accelerometer, Gyroscope, etc.
- **3. Introduction to Mobile OS:** Basics of Android architecture.