User Identity Module(UIM) for IMT-2000 systems

BoHyun Chung, Jongseog Koh
Korea Telecom
17, umyon-dong, Socho-gu, Seoul, Korea
chungbh@kt.co.kr

Abstract

User Identity Module(UIM) is widely deployed in GSM(Global System for Mobile communications), Known as SIM(Subscriber Identity Module). We can expect that UIM will be also available for ANSI based third generation systems. Removable User Identity Module(R-UIM) is UIM for ANSI based third generation systems and Universal Subscriber Identity Module(USIM) is UIM for GSM based third generation systems. This paper identifies differences between R-UIM and USIM and studies global roaming in IMT-2000 systems.

1. Introduction

User Identity Module is a kind of smart card that stores subscriber's personal information including authentication and ciphering key generation function in a secure manner with tamper-resistant module. UIM enables a user to change his/her terminal whenever needed and use same phone number in any place.

In the 2nd generation systems, UIM is specified and mandatory in GSM, called as SIM(Subscriber Identity Module)[1]. The SIM operating system, file structure and content are compliant with the ETSI GSM specifications (GSM 11.11 and GSM 11.14). All GSM carriers use SIM to store authentication algorithm and keys, as well as service and user profiles.

SIM cards were first specified to support authentication and provides an exceptional barrier to subscription cloning. With an additional local authentication by means of PIN (private identification number), the use of SIM cards has tremendously reduced wireless fraud. As of November 1st, 1999, 220 million wireless customers are using SIM cards worldwide to access to their wireless services.

SIM cards are also used to store SIM applications compliant to the SIM Toolkit as specified in the GSM 11.14. SIM Toolkit technology allows for SIM cards to monitor the phone as a peripheral (screen, keyboard, etc.) and to insert menus within the phone menus transparently to the user. SIM menu items trigger applications, which in turn can request information from the end-user (for instance a credit card account number, a dollar amount, a transaction date ...). The information received can be digitally signed or encrypted by the SIM and sent to an application server via SMS.

In 3GPP, SIM is evolving to USIM (Universal Subscriber Identity Module)[2]. ANSI based system[3] historically did not support physical UIM and they only have a concept of logical UIM. But, R-UIM is expected to apply to ANSI based third generation systems in 3GPP2.

In ITU-T, UIM was identified as one of the key

functional subsystems of IMT-2000 family systems[4][5] and technical study of UIM is ongoing toward the harmonized IMT-2000.

The scope of this paper is to study differences between USIM and R-UIM, especially, in point of authentication, and to find out problems for global roaming. In the following sections, we firstly identify what UIM is and, then find out the differences between USIM and R-UIM. Then we find out how to do inter-system roaming.

2. Characteristics of UIM

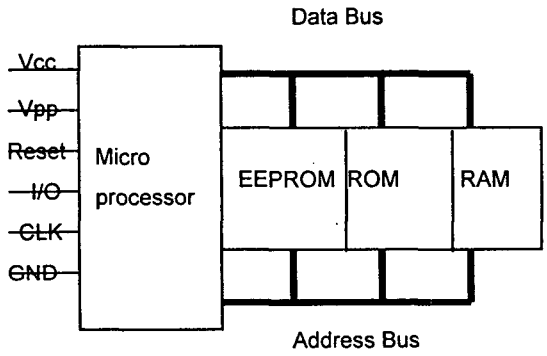

Fig. 1 Electronic Structure

A UIM is based on a micro-processor specifically designed to be tamper-resistant, composed of a Central Processing Unit, Random Access Memory, Read Only Memory, Electrically Erasable Programmable Read Only Memory (Fig. 1).

- CPU calculates security algorithm keys
- ROM stores Operating system
- RAM is working memory
- EEPROM stores customized applications and data

UIM have three kinds of file type. MF(Master File) is a mandatory root directory and DF(Dedicated File) is a Directory and EF(Elementary File) is a file. EF contains subscriber related information and network-specific information.

UIM support the following features:

- authentication algorithm and secret keys
- storage of the service profile and configuration data (preferred and forbidden roaming networks, short message service center address, available telephony services, voice mail number, service dialing number ...)
- storage of user data, such as speed dial number and short messages (SMS)
- storage of applications which can be either triggered at power-on or by specific events

3. USIM and R-UIM

In this section, we find out the differences between USIM and R-UIM for network support.

3.1 Functional assignment

ANSI based terminal must have a 32bit length unique terminal identity named ESN (Equipment Serial Number) to identify a terminal and has to show it with user ID whenever a user accesses to ANSI based system. If you want to introduce R-UIM in the ANSI based system, it is natural to allocate all personal profile to R-UIM, including ESN. But, FCC rule makes it mandate to keep ESN within a terminal. Thus, a possible allocation is the following. R-UIM has AKA (authentication and key agreement function) and user ID (MSID), and terminal has ESN. Unlike ANSI based terminal, GSM based terminal doesn't have ESN. So, USIM has all personal information and AKA.

3.2 Authentication

USIM and R-UIM have different authentication algorithms and mechanisms each other. USIM

provides mutual authentication by the user and the network showing knowledge of a secret key K which is shared between the USIM and AuC (Authentication Center). And USIM uses unique challenge.

R-UIM uses CAVE (Cellular Authentication and Voice Encryption) algorithm using SSD (Shared Secret Data) which is shared between the R-UIM and AuC, and provides only user authentication. Unlike USIM, R-UIM uses two kinds of authentication mechanisms. One is a global challenge and the other is a unique challenge.

The two mechanisms are challenge/response-based authentication in which the network authenticates an user. A unique challenge takes an user-specific random variable as a input to the authentication algorithm and the result is passed and verified by serving system. A global challenge takes time-varying random variables broadcasted by a base station and the result is verified by serving system.

3.2.1 Authentication for USIM

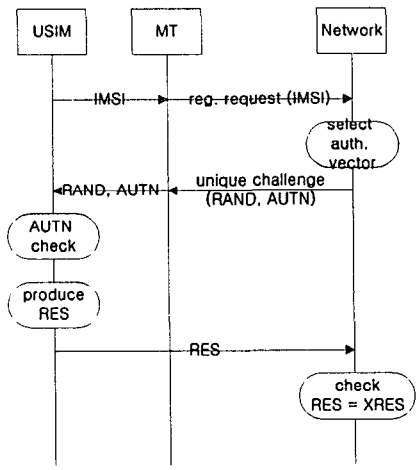

Fig. 2 AKA procedure for USIM

After network receives IMSI, it initiates an AKA. Network selects authentication vector and sends the parameters RAND and AUTN (authentication token) to the USIM. Authentication vector consists of the following components : RAND, Expected user RESponse XRES, Cipher Key CK, Integrity Key IK, Authentication Token AUTH. The USIM checks whether AUTN can be accepted and, if AUTN can be accepted, USIM produces a RES with K(secret key) which is sent back to the network. Network compares the received RES with XRES. If they match, network considers the AKA to be successfully completed. The USIM also computes CK and IK which is used by the MT to perform ciphering and integrity functions.

3.2.2 Authentication for R-UIM

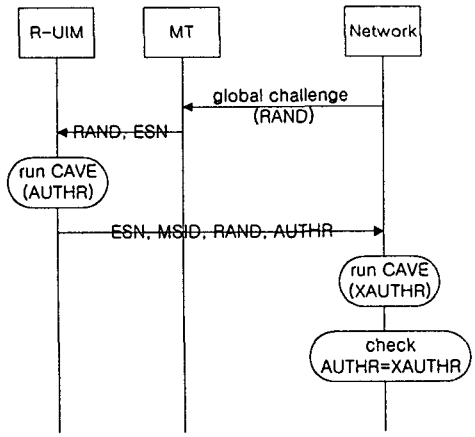

Fig 3. 2 AKA procedure for R-UIM

Receiving RAND from Network, MT sends RAND and ESN to the R-UIM. R-UIM runs CAVE function with RAND, SSD, ESN and MSID, and produces AUTHR. These parameters (ESN, MSID, RAND, AUTHR) are sent back to the network. After run CAVE function, network compares the received AUTHR with XAUTHR. If authentication fails, network (Home network) can do unique challenge.

3.2.2 Problems of global roaming

There are two kinds of roaming in 3G system. One is for same systems. The other is for different systems (3GPP and 3GPP2). In same systems, we can solve the roaming problems easily. In 3GPP, When mobile tries to register on a foreign network, it sends a LOCATION UPDATING REQUEST to the network, with its IMSI. If the foreign network has no agreement with the home network, it rejects the mobile directly. But, If the foreign network has an agreement with the home network, it sends a request to the home network asking for an authentication vector. If the home network agrees to fulfill the request, the vector is sent back to the foreign network. The foreign network asks an authentication to the terminal (sending RAND and AUTN). USIM responds with IK, CK, RES. The terminal sends the RES to the foreign network which compares it with the expected value.

To do global roaming between different systems, we have many problems to solve. The first is an authentication mechanism. 3GPP uses a unique challenge and 3GPP2 uses both a global challenge and a unique challenge, so they have different authentication procedures each other. For example, when a terminal with USIM wants to roam in a ANSI based 3G system, USIM wants to receive RAND and AUTN. But the network sends only RAND because it uses global challenge in a first attempt. The second is an authentication algorithm. USIM and R-UIM have different authentication algorithms and parameters each other. And contents of AKA messages are different each other. The third is inter-networking problems between ANSI based 3G systems and GSM based 3G systems. To solve the first and the second problem, we need to harmonize AKA between 3GPP and 3GPP2. Or we have to modify authentication procedures to do global roaming. For example, in 3GPP2, network has to be able to carry AUTN and to do a unique challenge in a first registration.

4. Conclusion

This paper identified differences between R-UIM and USIM and found out problems and solutions for global roaming in IMT-2000 systems. Harmonization of AKA between 3GPP and 3GPP2 is proceeding these days and inter-system roaming (between 3GPP and 3GPP2) will be possible with UIM in the near future. UIM cards support service mobility and user mobility as well as global roaming.

4. Reference

[1] ETSI Recommendation GSM 11.11, "Digital cellular telecommunication system(Phase 2+); "Specification of the Subsciber Identity Module",1998.

[2] 3GPP specification 3G TS 21.111, "USIM and IC card Requirements," April 1999. Available on ftp://ftp.3gpp.org/TSG_T/WG3_USIM/specs

[3] D. Brown, "Techniques for Privacy and Authentication in PCS", IEEE Personal Commun., vol. 2, no.4, Aug.1995

[4] ITU-T Recommendation Q.1701, "Framework for IMT-2000 networks", Mar. 1999

[5] ITU-T Recommendation Q.1711, "Network functional model for IMT-2000", Mar. 1999.

[6] TIA/EIA-41-D, "Cellular Radiotelecommunications Intersystem Operations", 1997

[7] 3GPP2 specification N.S0003, "Removable User Identity Module"