Mobile Subscriber Roaming on Different Mobile Networks Using UIM and PASM

Jeong-Hyun Park, Jeong-Mo Yang*

Information Technology Management Research Group,
Electronics and Telecommunications Research Institute (ETRI)
161 Kajong-Dong, Yusong-Gu, Taejon, 305-350, Korea
Email) jh-park@etri.re.kr

*Department of Information Security, Joongbu University
101, Daehack-Ro, Chuboo-Myun, Kumsan-Gun, ChungNam, 312-702, Korea
email)jmyang@joongbu.ac.kr

ABSTRACT: During a time when cellular systems are being deployed in massive scale worldwide, international roaming is becoming increasingly important. This paper presents UIM (User Identification Module) for mobility support, authentication, and service portability between different mobile systems. We also introduce network model based on PASM (Portable Authentication and Mobility Service Machine) which will support signaling protocol and user information conversions with database for roaming between different mobile networks. Stored data types and elements in UIM, logical data structure and configuration, and registration procedures are described here in the case of DCN (Digital CDMA (Code Division Multiple Access) Network System) and GSM (Global System for Mobile Communications).

Key Words: UIM (User Identification Module), Roaming, PASM (Portable Authentication and Mobility Service Machine), Personal Mobile Communications

I. INTRODUCTION

Recently, the demand for mobile communications, especially digital cellular communications, are rapidly growing and increasingly important segment of communication industry. The most important things in digital mobile communications systems are to provide interworking and service integration such as terminal (handset) mobility, personal mobility, universal roaming, access control, and the protection of user information sent via the airwaves. However, the second systems such as GSM, PDC, and IS-95 have no compatibility with each other. Each system has a different mobility management method, based on each MAP (Mobile Application Part) protocol. This means user mobility is limited within one system. In addition, since each system has different service features, service portability is not supported between different mobile systems. For next generation systems called IMT-2000 (International Mobile Telecommunications 2000) and cdma2000, the realization of global roaming is an important target. One ideal solution for global roaming is to define one global system standard. The third generation system envisages a seamless service which promotes a high degree of commonality ensuring world-wide coverage. However, due to different views and time schedules in each region, it is fairly questionable that one unified standard will be specified in IMT-2000. Another possible approach is to patch gaps between different mobile systems by intersystem roaming. Intersystem roaming provides a mobile user with an extended mobility beyond one system allowing outgoing and incoming calls. Moreover, an intersystem roaming service provides as many as possible of the service features in the visited network as in the home network. Yasuyuki et al., has proposed that the IWF (Inter Working Function) roaming approach is a quite practical approach to realize intersystem roaming. The IWF approach was mainly described from the viewpoint of mobility support in network functions. In this paper, we introduce the UIM (User Identification Module) card for global roaming supporting both intersystem

mobility support and service portability between different mobile systems, especially between DCN (Digital CDMA Network System) and GSM. We also present the architecture and data structure of the UIM card for inter-system roaming service, and introduce the PASM (Portable Authentication and Mobility Service Machine) as roaming supporting approach in the network function.

II. NETWORK MODEL FOR GLOBAL ROAMING SUPPORT

In order to allow for cellular systems complying to different standards to be interconnected, where each of the cellular systems still would use the signaling protocols of the specific standard. The solution for intersystem roaming implies that new node is
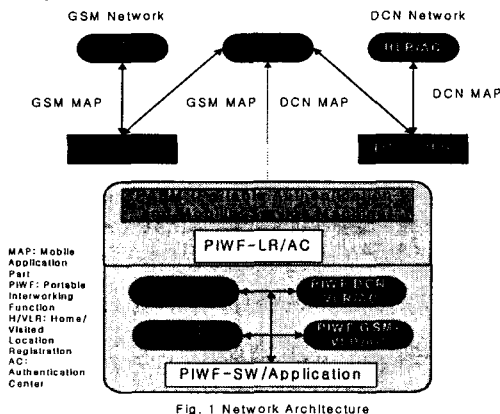

Fig. 1 Network Architecture

introduced in the network that have the purpose of providing interworking between the cellular systems of the different standards. This node will ensure that the cellular systems that should be interconnected can do this using the standard signaling of the respective cellular system, independent of the standard the interconnected system is using. The node that performs the interworking between different cellular standards is the PASM (Portable Authentication and Mobility Service Machine) as visited/home location register (VLR/HLR), authentication center (AC), and mobile service switching center for interworking. Fig. 1 shows the network architecture for roaming between cellular standards. This implies that the PASM can ensure that the two interconnected standards can cooperate with no impact on the respective standard. The home network will interface the PASM according to the home network standard, and the visited network will interface the PASM according to the visited network standard. This machine provides a simple adaptable interface to HLR/AC in the different authentication environments to allow the authentication and roaming services. The PASM is

basically considered the functions such as mobility management association, security management, routing information association, network signaling protocol translation, charging information management, and user ID (Identity) and data management association. The PASM is a portable authentication and mobility service machine which is used for authentication and global roaming services in different environments. The PASM provides the on-line access to the network for different system users and the registered data of the users. The PASM plays important role of authentication verifier, key issuer, internetworking authentication arbitrator, VLR/HLR, gateway for authentication in different service areas, and so on. The PASM also manages the secure database which includes the identities, keys, and parameters of users and network operators.

III. UIM CARD FOR GLOBAL ROAMING

Global roaming is the capability of users to roam among different networks. A user will be able to take his own terminal or UIM out of his normal service area to obtain access to the services provided in other service area, subject to the limitations of his own terminal or UIM and service profile, and service capabilities of the visited network.

A. UIM Card
The following is basic functions performed by the UIM
• Storage, execution and verification of the result of cryptographic algorithms.
• Authentication by the service provider/network operator of the user when required.
• Authentication of the service provider/network operator.
• Ciphering of user traffic when required.
• Multitasking such as sending or receiving data from the terminal whilst also engaged in a call. The UIM is a security device with logical multi mode for different networks which contains all the necessary information and algorithms to authenticate the subscriber from the networks such as GSM and DCN. It adds a new dimension of mobility to the subscriber as it is a removable module and may be used with every mobile equipments. To achieve its main task of authenticating the subscriber to the network side, the UIM contains a microcomputer with on-board non-volatile memory. In other words, the UIM is a smart card. This card comes in two formats. The IC card (UIM) is the size of a credit card, while the Plug-in UIM is obtained from this by cutting away excessive plastic and thus reducing the size to 25mm by 15mm. The latter is intended to be used mainly with handheld mobiles which are too small to support an IC card UIM. A third format, having the dimension 66mm by 33mm, has been

specified for the DECT (Digital European Cordless Telephone) authentication module. The electrical and mechanical interfaces are with the obvious exception of the two small cards, in line with the relevant international standard for IC cards. In some instances, however, more stringent conditions were agreed upon to cater for needs of the environment the UIMs are used in. These include, for instance, the temperature range the card has to satisfy and the power consumption of the microcomputer. The microcomputer consists of a CPU and three types of memory. The masked programmed ROM usually contains the operating system of the card and the security algorithms. The RAM is used for the execution of the algorithms and as a buffer for the transmission of data. The non-volatile memory, which is needed to store subscriber specific data such as secret key and IMSI, is EEPROM (Electrically Erasable Read Only Memory). EPROM, which can be written to only once, cannot be used as network and subscriber related information such as TMSI, LAI, and short message are updated frequently or have to be changeable by the subscriber. The memory space offered by present day smart card chips is typical 4 - 6 Kbyte for ROM (Max 16 Kbyte), 126 – 160 byte for RAM (Max 256), and 2 - 3 Kbyte for EEPROM (Max 8 Kbyte).

B. UIM Logical Data Structure for Global Roaming

The following is an example of logical data structure on UIM for global roaming between GSM and DCN. (Fig.2/Fig.3) Dedicated files (DF) of DF_{GSM} and DF $_{DCN}$ contain the application for GSM and DCN. All these files can coexist under a MF (master file) on a multi-application card. If a GSM user roaming to DCN inserts a GSM SIM in a DCN terminal for roaming from GSM to DCN, the IMSI EF (elementary file) of the GSM is accessed through the DCN terminal. Then, the IMSI (International Mobile Subscriber Identity) is treated as MSN (Mobile Subscriber Number) and used in the DCN network. A major consideration issue is the numbering structure between IMSI and MSN. If MSISDN (Mobile Station International ISDN (Integrated Service Digital Network)) corresponds to MSN and IMSI corresponds to MSI (Mobile Station

Fig. 2 Multi-application smart card for dual cellular systems

Identity), major consideration issues are the numbering structure between MSISDN and MSI, between IMSI and MSI, and the capabilities for multi-mode UIM and terminal multi-association services. The following is an example DCN subscriber registration at GSM system and GSM subscriber registration at DCN system.

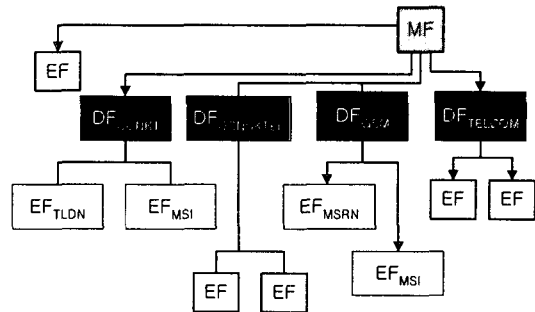## C. DCN subscriber registration at GSM System

Fig. 3 UIM Directory Structure for GSM and DCN ·

Fig. 4 is showed location registration procedure of DCN user at GSM system. Before intersystem roaming or at the service provision, the PASM generates user information through service definition association, service logic collaboration and collaborating service status control. When DCN user visits GSM network, the DCN user inserts UIM card to GSM ME, and verified by ME. DCN user requests location registration in the visited GSM/VLR. GSM/VLR requests user ID to ME, and ME sends ID to PASM via MSC/VLR. The PASM requests authentication to UIM through MSC/VLR and ME, and the UIM responses authentication response to the PASM via MSC/VLR. The PASM requests cipher mode command to UIM through MSC/VLR and ME, and the UIM responses cipher mode command to the PASM via MSC/VLR. The PASM performs location updating of DCN user through an association mapping table and the execution of collaborating service status control. If the received information is different from the stored information, the PASM adjusts the received DCN service status information with old GSM service status information to generate information. Finally, the PASM sends the MSC/VLR the new GSM service status information through Insert_Subscriber_Data_Request. GSM/MSC/VLR sends TMUI to UIM. When the user returns to the home DCN network, the home DCN network requests an intersystem location cancellation. Then, the user information is deleted at the PASM.
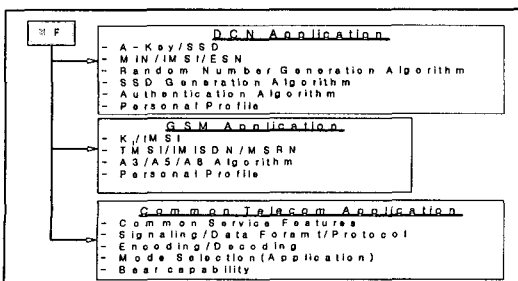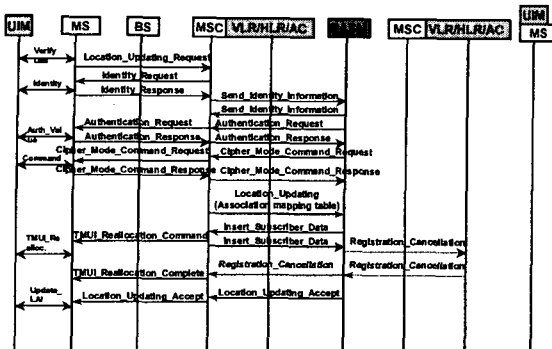
Fig. 4 DCN User Registration at GSM System

D. GSM subscriber registration at DCN System

When a GSM user roams into a DCN network he has to make location registration for provision of DCN services. Firstly, the roamed DCN network requests his subscriber information available in interworking function blocks (PASM) by using DCN MAP operations. The PASM converts this requested message to GSM MAP format. Then, it sends this GSM MAP request message to the GSM operator by GSM MAP operations. The GSM sends back the subscriber information to the PASM. This information is converted form GSM MAP to DCN MAP format and replied to the DCN operator. Then, the subscriber is verified by using this information and his location information is registered in DCN GLR/PASM.

IV. CONCLUSIONS

To meet the increasing demand for international roaming, this paper presented UIM for roaming between different mobile networks. Data types and elements, logical data structure, and configuration in UIM were shown. We also showed the network model based on PASM as HLR/VLR (Home/Visited Location Register) and AC (Authentication Center) with MAP (Mobile Application Part)/database which deals with mobility and authentication service for roaming between different mobile networks, and registration procedure between GSM and DCN networks. Third generation system will be an evolution of second generation networks, and maintain backward compatibility considering the growing second generation markets. Standardization of UIM card and relevant terminal specifications would be expected to implement such roaming services. It should noted that the considerations mentioned in this paper could be applied to not only cellular systems but also digital cordless systems or mobile satellite systems.

REFERENCES

[1] ETSI-GSM, "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface; (GSM 11.11)", Version 5.3.0, 1996.

[2] TIA/EIA/IS-95-A, "Mobile Station-Base Station Compatibility for Dual-Mode Wideband Spread Spectrum Cellular System", July 1993.

[3] ITU-T Draft Recommendation Q.FIF, "Information Flows for IMT-2000 Ver.7.1", March 1997.

[4] Yoshihiko Ito et al., "Global Personal Roaming - beyond regional system boundaries", KDD R&D Labs. 1997.

[5] Hitachi, "Hitachi Single-Chip Microcomputer H8/3048 Series Programming Manual – Smart Card Interface", 1995.

[6] ISO, "Identification Cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics", ISO 7816-1, July 1987.

[7] ISO, "Identification Cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts", ISO 7816-2, May 1988.

[8] ISO, "Identification Cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols", ISO 7816-1, September 1989.

[9] J. H. Park and K. J. Lee, "Authentication Scheme for Global Roaming on Digital Mobile Communications", Wireless'98 Proceeding, Canada, July 1998.