INTERNATIONAL JOURNAL OF EMERGING RESEARCH & DEVELOPMENT

(Volume 1, Issue 9)

Available online at: www.ijernd.com

Embedded Subscriber Identification Module

Manoj
manojmca1719@gmail.com
Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu

Ajeeth Kumar
ajithkum641@gmail.com
Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu

Rahul
rahulmca536@gmail.com
Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu

ABSTRACT

The SIM is part of European telecommunications standard that separate mobile from the network they connect to move all there necessary security and identification data into a chip into a piece of plastic, GSM Technology convert the voices at end to end encrypted digital data before send in airwaves, SIM also stores the 'key' to decrypt this data.

Keywords— *E_SIM, UIM*

1. INTRODUCTION

Consumer terminals in all types of formats including wearable terminals have been increasing in recent years, and the need has been growing for a mechanism that makes it relatively easy to load and activate a cellular communications function on those terminals. NTT DOCOMO has developed terminals that incorporate a Local Profile Assistant (LPA). Function to remotely install a profile, for using communication services in an embedded Subscriber Identity Module and has constructed a platform consisting of a network and Subscription Manager (SM). At NTT DOCOMO, we call this new platform for providing e-SIM services with the "e-SIM platform.

In this article, we describe e-SIM for consumer devices and the mechanism behind the terminals and e-SIM platform developed by NTT DOCOMO for the launch of e-SIM services.

What Is e-SIM for Consumer Devices?

Here, e-SIM for consumer devices refers to the capability of installing profiles securely from SM using terminal operations as a trigger. E-SIM embedded in a device, but its definition in GSM Association. Remote SIM Provisioning Version 2.0 includes a card form in addition to a chip form. In the rest of this section, we describe the benefits of introducing e-SIM for consumers, standardization trends, and differences with e-SIM for Machine to Machine devices.

2. BENEFITS OF INTRODUCING E-SIM FOR CONSUMERS

The conventional method of enabling communication services in a consumer device has been to use reader/writer equipment to record a profile on a User Identity Module card and to then insert that card into the user's terminal. In contrast, e-SIM for consumer devices provides the following benefits:

- The UIM function can be built into the terminal beforehand eliminating the need to insert or remove a UIM card.
- Conventionally, in the case that a UIM card had to be issued when purchasing a terminal from an online shop, the user was required to perform service-provisioning processing through a telephone-based procedure or Web-based procedure using (for example) a separate personal computer. With e-SIM, the user needs only perform simple and guided terminal operations to perform activation processing as part of initial terminal settings when starting up the purchased terminal for the first time. Since there is no need to insert or remove a UIM card, the card-slot portion of a terminal can be omitted thereby increasing the degree of freedom of terminal design. This makes it easy to support cellular communication services in even compact devices like wearable terminals.
- In short, E-SIM makes it much easier for a user to use communication services resulting in a higher level of convenience. On the other hand, conventional UIM enables simple switching of UIM information without the network as an intermediary when changing models or exchanging handsets at the time of terminal failure. Going forward, we can envision the use of both conventional UIM and e-SIM depending on the application.

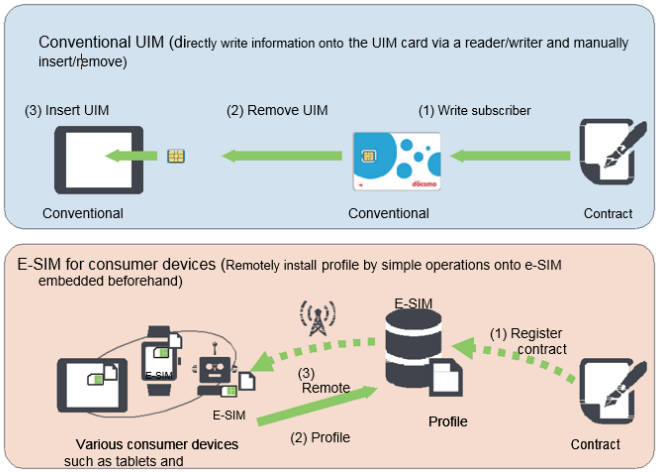

Fig. 1: E-SIM for consumers

2.1 Comparison with e-SIM for M2M Devices

The recent proliferation of M2M devices has been accompanied by increased use of embedded UIM (M2M Form Factor (MFF) that cannot be removed for the sake of device durability. In addition, companies that are expanding their M2M business globally have a growing need for greater efficiency in production and management, which can be achieved by embedding one UIM at manufacturing time and storing the M2M devices as such and then writing the communications service operator

information onto the UIM at shipping time. Against this background, NTT DOCOMO launched its "DoCoMo M2M Platform service for the corporate M2M market in June 2014.

For consumer devices, on the other hand, the user is required to perform a terminal operation to download a profile. For this reason, we load the LPA function described below on the terminal side and provide a function for downloading a profile onto the e-SIM.

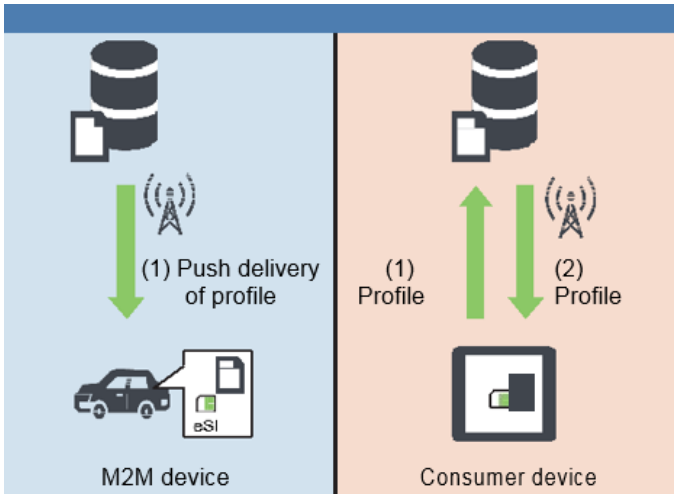

Fig. 2: E-SIM comparison

3. MECHANISM FOR ACHIEVING E-SIM FOR CONSUMER DEVICES

This section describes the E-SIM for consumer devices hereinafter referred to as "e-SIM", the terminal, and the e-SIM platform and their constituent elements.

3.1 E-SIM

Conventional UIM consists of an Operational Profile (OP) lying above the UIM chip and UIM OS. The OP, in turn, consists of various files containing information such as telephone number and International Mobile Subscriber Identity (IMSI) and various applications such as a network authentication function.

In addition, conventional UIM incorporates a Universal Subscriber identity module Application Toolkit (USAT) function for rewriting UIM Information. The purpose of this function was to enable some of the files and applications within UIM to be updated.

In contrast, e-SIM incorporates a function for remotely and securely installing an OP from SM, which makes it possible to update in units of OPs each of which includes confidential information such as a private key for network authentication.

Moreover, as many profiles as capacity allows may be stored within an E-SIM, but only one profile can be used at one time for communications. Using LPA, the user can control which profile stored in E-SIM is to be used for communications.

Another type of profile stored in E-SIM is the Provisioning Profile (PP). While the OP type of profile provides the user with services.

The same as conventional UIM software, the PP serves to download OPs. The use of PP for other than OP downloading is limited.

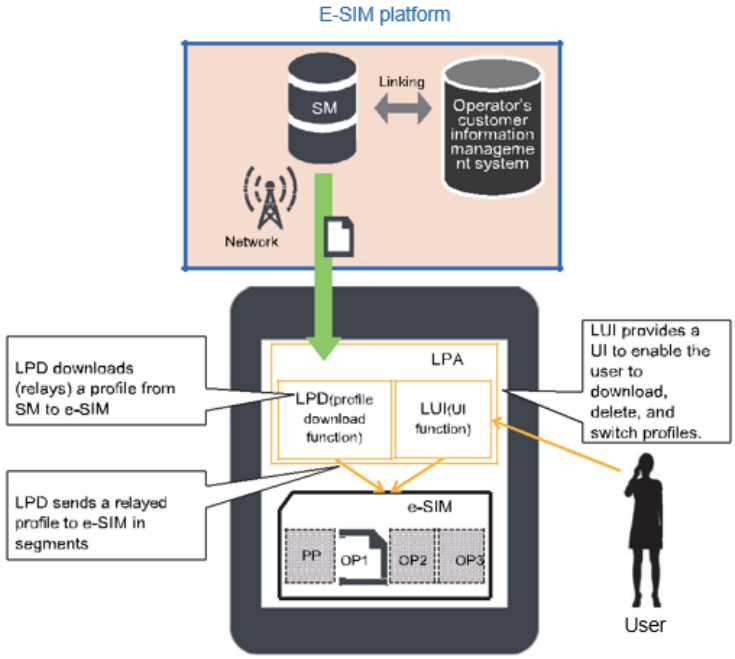

Fig. 3: E-SIM platform

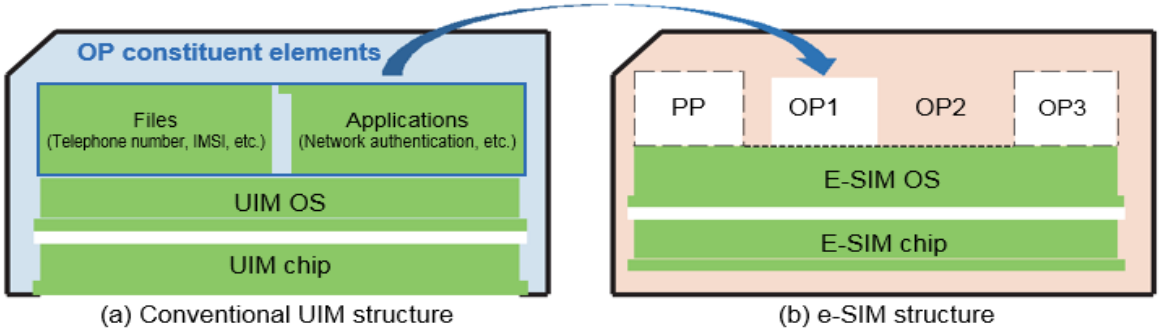

Fig. 4: Typical Structure Conventional UIM and E-SIM

3.2 Terminal (LPA)

LPA consists of the following two functions:

- Local Profile Download (LPD): This function performs a batch download of an encrypted profile from SM, sends that profile in segments to e-SIM, and installs the profile. The Interface between the terminal and e-SIM operates at low speed, so having LPD perform a batch download from SM first shortens communication time using the mobile network.
- Local User Interface (LUI): This function provides a UI for controlling the e-SIM by user operations (as in downloading, deleting, and switching profiles).

Using LPA with these functions enables efficient profile downloading from SM and profile control in conjunction with user terminal operations.

3.3 Network

Using PP to perform communications with SM and download OPs enables the provision of voice services, packet communications, and other types of services.

While an in-area state can be achieved using PP, communications at this time are handled as "not yet under contract," so voice, SMS, and other services are restricted by the network.

Restricted communications such that only packet communications are allowed with SM are achieved by establishing an Access Point Name (APN) for download communications and regulating access from that APN to points other than the SM's URL. However, it is unclear whether an APN for SM communications will be set in the user's terminal, and in this regard, it is also possible for the user to manually set an APN for SM communications, though this is an added burden.

This problem is resolved in the following way with reference to Once it is recognized at the Mobility Management Entity (MME) and Serving General Packet radio service Support Node (SGSN) that packet communications are being performed by PP, the EPC Serving and PDN Gateway (ESPGW) will forcibly convert whatever APN has been set by the terminal to an APN for SM communications and connect to that APN. The Multi Access Platform System (MAPS) will then regulate non-SM communications. In this way, the user connects only with the SM without having to consciously do so. After establishing communications with SM and downloading an OP, services can be provided according to contract conditions the same as an ordinary user.

3.4 SM

The SM for E-SIM mainly provides a function for generating and storing profiles and a function for securely installing profiles, as described below:

- **Profile generation and storage**: After a contract has been established between the user and operator, a profile needed or using communication services is prepared so that it can be downloaded to the target E-SIM from the SM server introduced here. The SM receives information such as telephone number, IMSI, and network authentication key from the operator's customer information management system, generates a profile according to specifications, and securely stores the profile after Encryption.
- **Profile installation**: The profile is encrypted so that it can be decrypted only at the E-SIM targeted for installation. This encrypted profile is installed in that E-SIM via LPA. The E-SIM platform system guarantees robust security based on the Public Key Infrastructure (PKI). The E-SIM, LPA, and SM each store a public key certificate issued by a trusted certificate authority. This certificate is used as a basis for authentication processing in inter-system communications.

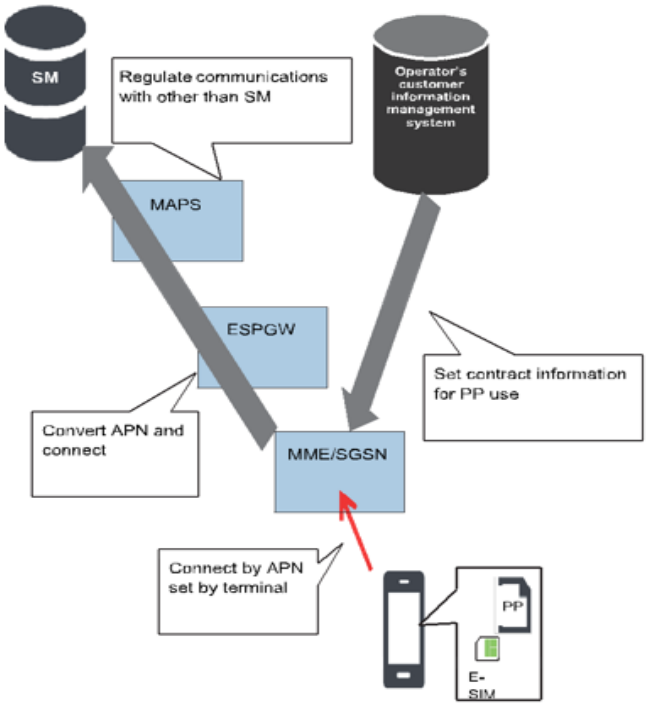

Fig. 5: Control of communications from PP to SM

3.5 Example of a Profile Download Sequence

An example of a sequence using the above mechanisms to install a profile from SM to E-SIM via the network and terminal (LPA) and summarized below:

- The terminal storing E-SIM is turned ON and a packet communications call is established using PP.
- SM is accessed by LPA in the terminal and HTTPS communications are established based on LPA and SM certificates. Only an LPA having a certificate that allows access to SM can do so.
- Once a communication channel is established between SM and LPA, E-SIM and SM perform mutual authentication via LPA. A closed, secure communication channel between E-SIM and SM is established during this mutual authentication process, and a profile is then installed in E-SIM without any leakage of profile information at the terminal or LPA. As described above, a batch download is first performed at LPD followed by segmented transmission to and installation on the E-SIM to shorten communication time using the mobile network.
- After installing a profile, profile switching, deletion, etc. becomes possible through LPA operations. A variety of communication services are available using OPs.

4. CONCLUSION

NTT DOCOMO has developed an E-SIM platform conforming to the GSMA global standard with an eye to a wide range of applications and low-cost provision. It is envisioned that E-SIM will be used in an embedded state within the terminal. However, while tests to check the terminal's network connection function, for example, can be performed by inserting/removing a test-type UIM given a terminal having a conventional UIM card slot, such a test- type UIM cannot be used if a UIM cannot be inserted/removed as in E-SIM, which poses a new problem. For this reason, parts of the previously released GSMA RSP

specifications Version 2 such as test environment setup are still under discussion. Taking the above standardization trends into account, we plan to apply this E-SIM platform to a dramatically diverse range of terminals to make communication services even more convenient for users.

5. REFERENCES

[1] GSMA SGP.21: "Architecture Specification- V2.0," Aug. 2016.
[2] GSMA SGP.22: "Technical Specification - V2.0," Oct. 2016.
[3] K. Suzuki et al.: "Standardization of Embedded UICC Remote Provisioning," NTT DOCOMO Technical Journal, Vol.16, No.2, pp.36–41, Oct. 2014.
[4] M. Minami et al.: "UIM Version 3," NTT DOCOMO Technical Journal, Vol.9, No.1, pp.25–31, Jun. 2007.
[5] Tetsuhiro Sasagawa, "control N-communications from PP to SM", NTT DOCOMO Technical Journal, Vol.19, Jun. 2017.

APPENDIX

GSM:	Global System for Mobile communications
E-SIM:	Embedded Subscriber Identification Module
LPA:	Local Profile Assistant
SM:	Subscription Manager
UIM:	User Identity Module

