

eSIM for Consumer Devices toward Expanded eSIM Usage —Secure Installation Conforming to GSMA—

Communication Device Development Department Tetsuhiro Sasagawa[†] Tomohiro Akiyama
Product Department Kensuke Ueda Akihiro Inoue
Core Network Development Department Tomonori Kagi

NTT DOCOMO has introduced Japan's first eSIM service for consumer devices conforming to GSMA. This has been achieved by adding an LPA function to consumer devices (terminals) for installing profiles triggered by user terminal operations and by constructing a platform consisting of a network and SM. This article describes the mechanism of the eSIM, LPA function, network, and SM developed for this service to achieve secure profile installation in consumer devices.

1. Introduction

Consumer devices (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)^{*1} function to remotely install a

profile^{*2} for using communication services in an embedded Subscriber Identity Module (eSIM)^{*3} and has constructed a platform consisting of a network and Subscription Manager (SM)^{*4}. At NTT DOCOMO, we call this new platform for providing eSIM services the “eSIM platform^{*5}”.

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

©2017 NTT DOCOMO, INC.

Copies of articles may be reproduced only for personal, noncommercial use, provided that the name NTT DOCOMO Technical Journal, the name(s) of the author(s), the title and date of the article appear in the copies.

[†] Currently Product Department

^{*1} LPA: Provides a relay function (LPD) for downloading profiles from SM to eSIM and a UI function enabling the user to perform profile-related functions such as downloading, deleting, and switching.

2. What Is eSIM for Consumer Devices?

Here, eSIM for consumer devices refers to the capability of installing profiles securely from SM using terminal operations as a trigger. In terms of form factor, the original definition of “eSIM” is a SIM embedded in a device, but its definition in GSM Association (GSMA)*⁶ Remote SIM Provisioning (RSP)*⁷ 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 eSIM for consumers, standardization trends, and differences with eSIM for Machine to Machine (M2M)*⁸ devices.

2.1 Benefits of Introducing eSIM 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 (UIM)*⁹ card and to then insert that card into the user’s terminal (**Figure 1 (a)**).

In contrast, eSIM 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 (Fig. 1 (b)).
- The work of service provisioning can be performed without having to physically use special equipment (reader/writer) thereby

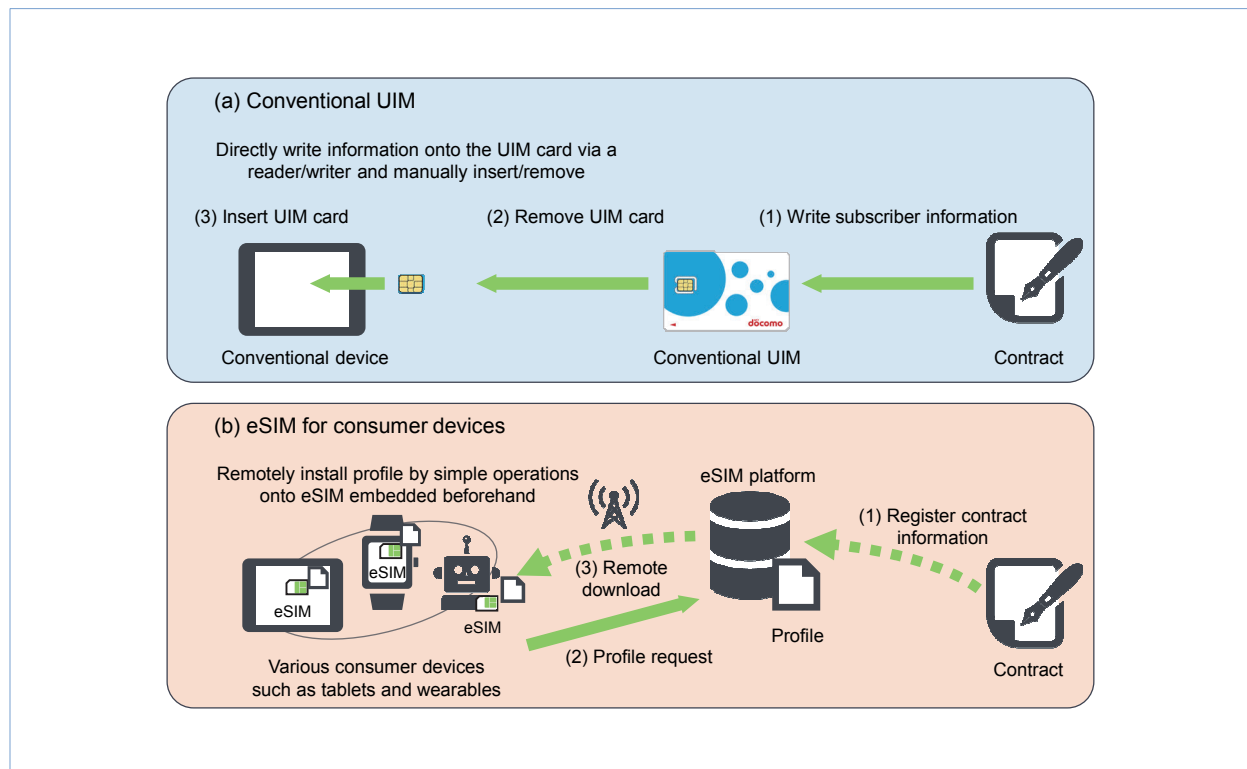


Figure 1 Differences between conventional UIM and eSIM for consumer devices

*2 Profile: UIM software running on eSIM OS consisting of various files containing telephone number, IMSI (see *12), and other data, applications such as network authentication, etc. There are OP and PP types of profiles.

*3 eSIM: Generic name for SIM that can install profiles remotely.

*4 SM: A server linking with the operator information management system. Provides a function for generating and saving profiles and a function for downloading and installing profiles

in eSIM via LPA, etc.

*5 eSIM platform: A platform consisting of a network, SM, etc. for providing eSIM services. On this platform, a compatible user terminal can install a profile via the network into an eSIM built into the terminal through a terminal operation.

enabling prompt use of communication services simply through possession of the terminal.

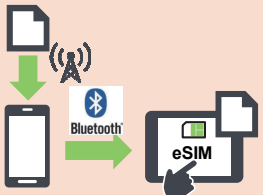
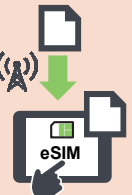
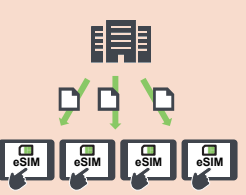
- Conventionally, in the case that a UIM card had to be issued when purchasing a terminal from an online shop, the user was required to perform service-provisioning processing through a telephone-based procedure or Web-based procedure using, for example, a separate personal computer. With eSIM, the user need 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, eSIM 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 intermediary when changing models or exchanging handsets at the time of a terminal failure. Going forward, we can envision the use of both conventional UIM and eSIM depending on the application.

2.2 Standardization Activities

Standardization activities targeting eSIM for consumer devices have been taking place mainly at GSMA RSP meetings. As shown in **Figure 2**, Version 3 specifications are currently being discussed within GSMA RSP to add to existing specifications up to Version 2 released in October 2016.

Specifications version	Version 1	Version 2	Version 3
Release period	January 2016	October 2016	Under discussion
Use case	Download profile to 2nd device 	Download profile to 1st device 	Push delivery of profiles 
Features	<ul style="list-style-type: none"> • Transfer profile to 2nd device such as a wearable or tablet via smartphone 	<ul style="list-style-type: none"> • Download profile directly to a unit device such as a wearable or tablet • Supports installation of multiple profiles 	<ul style="list-style-type: none"> • Supports kitting* for a large number of devices in corporate applications

* Kitting: The work of installing applications in a terminal such as a mobile phone, configuring and registering the terminal, etc. so that the user can begin using the product immediately.

Figure 2 Examples of GSMA RSP use cases

*6 GSMA: A global trade body of mobile operators that also includes terminal manufacturers, software companies, and other companies in the mobile industry. In addition to activities such as formulating roaming rules between operators, GSMA leads eSIM-related standardization.

*7 RSP: Generic name for remote profile writing technology for use with eSIM as defined by GSMA.

*8 M2M: Machine-to-machine communications between machines.

Systems that enable machines to communicate with each other without any human mediation.

*9 UIM: Contains information such as telephone number and network authentication key and provides a user authentication function for registering terminal location in the communications network. Synonymous with SIM.

Version 3 aims to extend these specifications to consumer devices in enterprise applications.

Taking the features and characteristics of the Japanese mobile market into account, NTT DOCOMO has made a variety of proposals at these meetings in relation to a method of designating the destination SM, specifications of profiles to be downloaded, specifications of a function for assessing terminal capabilities, etc. Many of these proposals have been reflected in released specifications. The developments described here conform to GSMA RSP specifications Version 2 [1] [2]. NTT DOCOMO is achieving early development and commercialization through its deep involvement in standardization activities.

2.3 Comparison with eSIM for M2M Devices

The recent proliferation of M2M devices has been accompanied by increased use of embedded UIM (M2M Form Factor (MFF)^{*10}) 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^{*11}” service for the corporate M2M market in June 2014 [3].

For consumer devices, on the other hand, the user is required to perform a terminal operation to download a profile (Figure 3). For this reason, we load the LPA function described below on the terminal side and provide a function for downloading a profile onto the eSIM.

3. Mechanism for Achieving eSIM for Consumer Devices

This section describes the eSIM for consumer devices (hereinafter referred to as “eSIM”), the terminal, and the eSIM platform and their constit-

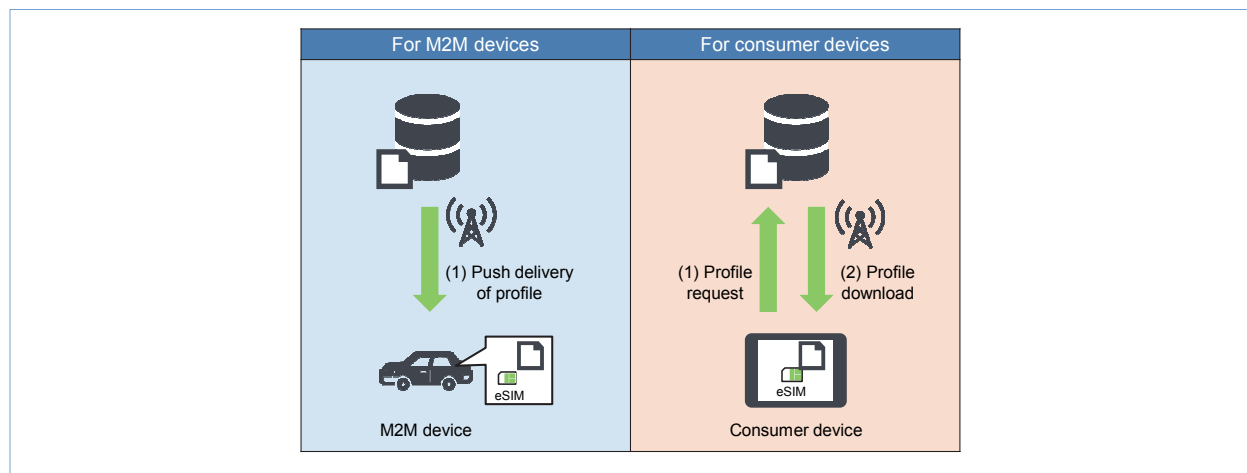


Figure 3 eSIM for M2M devices and eSIM for consumer devices

*10 MFF: Refers to the Universal Integrated Circuit Card (UICC) form factor for M2M devices as defined by the European Telecommunications Standards Institute (ETSI).

*11 docomo M2M Platform: An eSIM solution for corporate M2M devices launched by NTT DOCOMO in June 2014.

uent elements (Figure 4).

3.1 eSIM

As shown in Figure 5 (a), 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)^{*12} and various applications such as a network authentication function.

In addition, conventional UIM incorporates a Universal Subscriber identity module Application Toolkit (USAT)^{*13} function for rewriting UIM information [4]. The purpose of this function was to enable some of the files and applications within

UIM to be updated.

In contrast, eSIM 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, as shown in Fig. 5 (b).

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

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

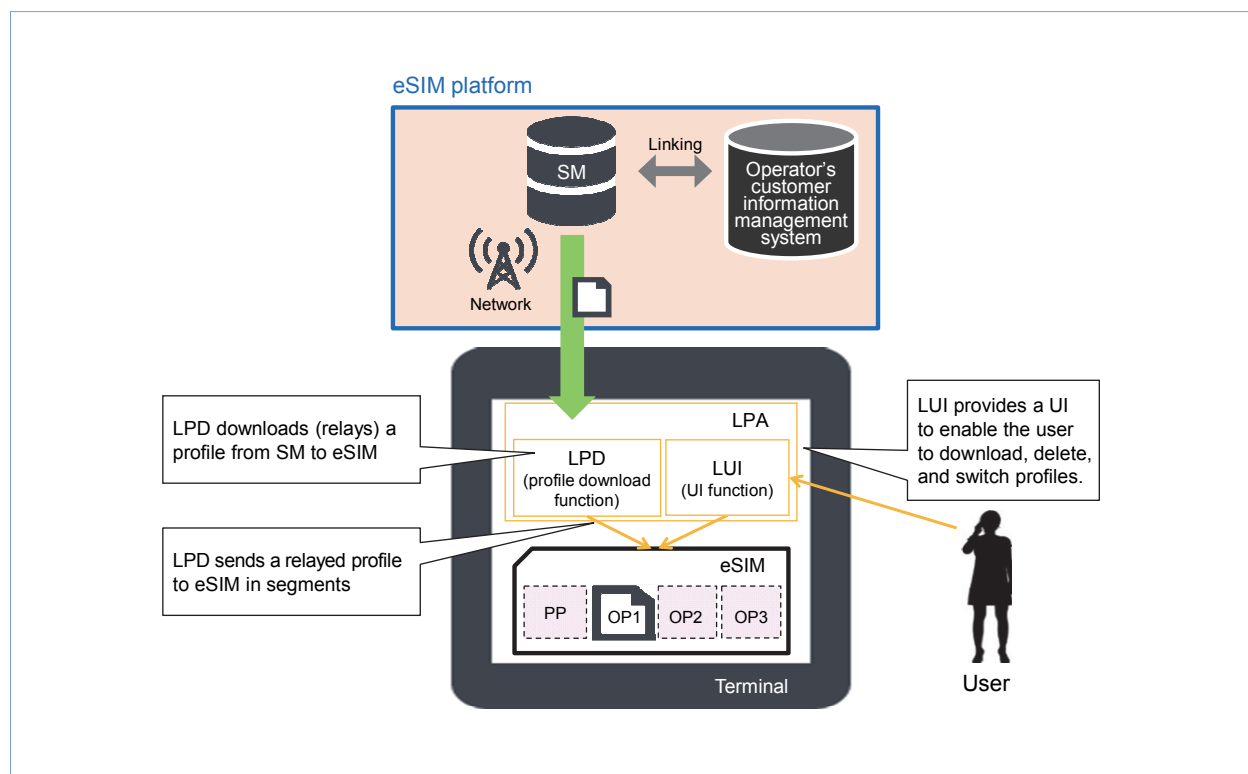


Figure 4 Constituent elements of eSIM, terminal, and eSIM platform

*12 IMSI: A number used in mobile communications that is unique to each user and stored on a UIM card.

*13 USAT: A standard specification specified by 3GPP TS31.111 for use in remotely updating information within a UIM.

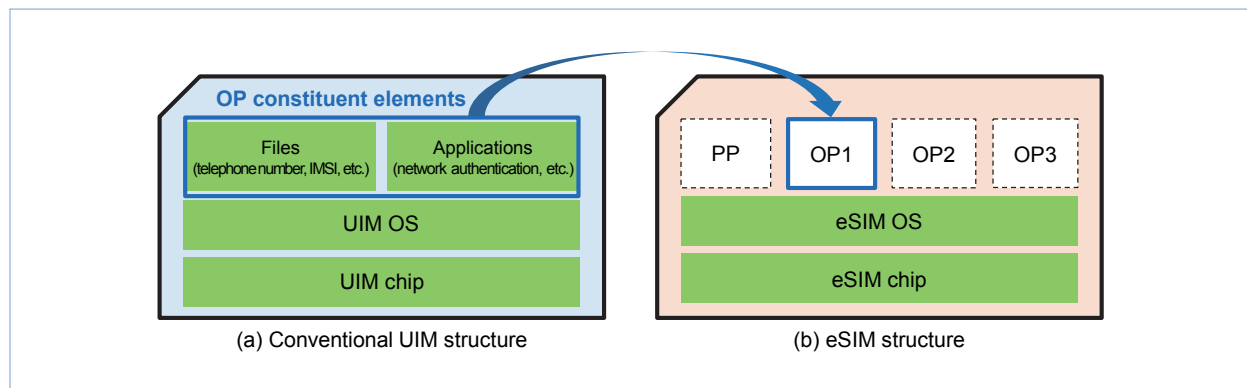


Figure 5 Typical structure of conventional UIM and eSIM

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

3.2 Terminal (LPA)

LPA consists of the following two functions (Fig. 4).

- Local Profile Download (LPD): This function performs a batch download of an encrypted profile from SM, sends that profile in segments to eSIM, and installs the profile. The Interface between the terminal and eSIM 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 eSIM 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)^{*14} 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 **Figure 6**. Once it is recognized at the Mobility Management Entity (MME)^{*15} and Serving General packet radio service Support Node (SGSN)^{*16} that packet communications is being

*14 APN: The name of a network connection point used by users to connect to the network when performing data communication.

*15 MME: A logical node accommodating a base station (eNodeB) and providing mobility management and other functions.

*16 SGSN: A logical node managing the mobility of mobile terminals that perform packet communications.

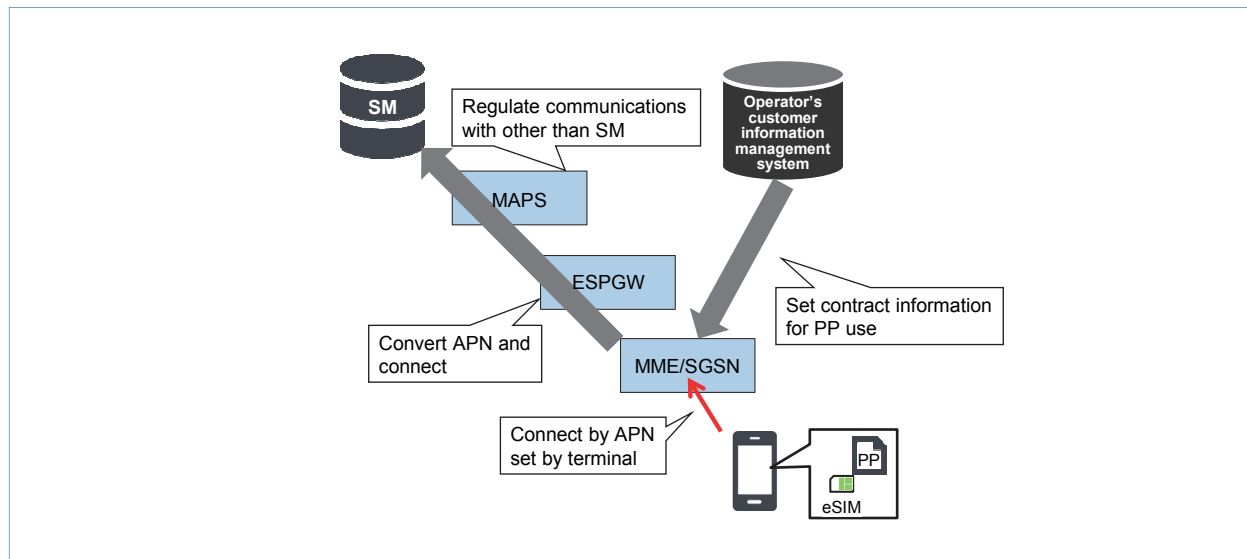


Figure 6 Control of communications from PP to SM

performed by PP, the EPC Serving and PDN Gateway (ESPGW)^{*17} 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)^{*18} 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 eSIM 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

for using communication services is prepared so that it can be downloaded to the target eSIM 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 eSIM targeted for installation. This encrypted profile is installed in that eSIM via LPA. The eSIM platform system guarantees robust security based on the Public Key Infrastructure (PKI)^{*19}. The eSIM, 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.

*17 ESPGW: Equipment having the capabilities of S-GW and P-GW.

*18 MAPS: A platform that provides Internet connections and corporate system connections from various types of access circuits.

*19 PKI: A generic term for systems, etc. built for ensuring secure communications using public key encryption technology.

3.5 Example of a Profile Download Sequence

An example of a sequence using the above mechanisms to install a profile from SM to eSIM via the network and terminal (LPA) is shown in **Figure 7** and summarized below.

- (1) The terminal storing eSIM is turned ON and a packet communications call is established using PP.

- (2) SM is accessed by LPA in the terminal and HTTPS communications is established based on LPA and SM certificates. Only an LPA having a certificate that allows access to SM can do so.

- (3) Once a communication channel is established between SM and LPA, eSIM and SM perform mutual authentication via LPA. A closed, secure communication channel between eSIM

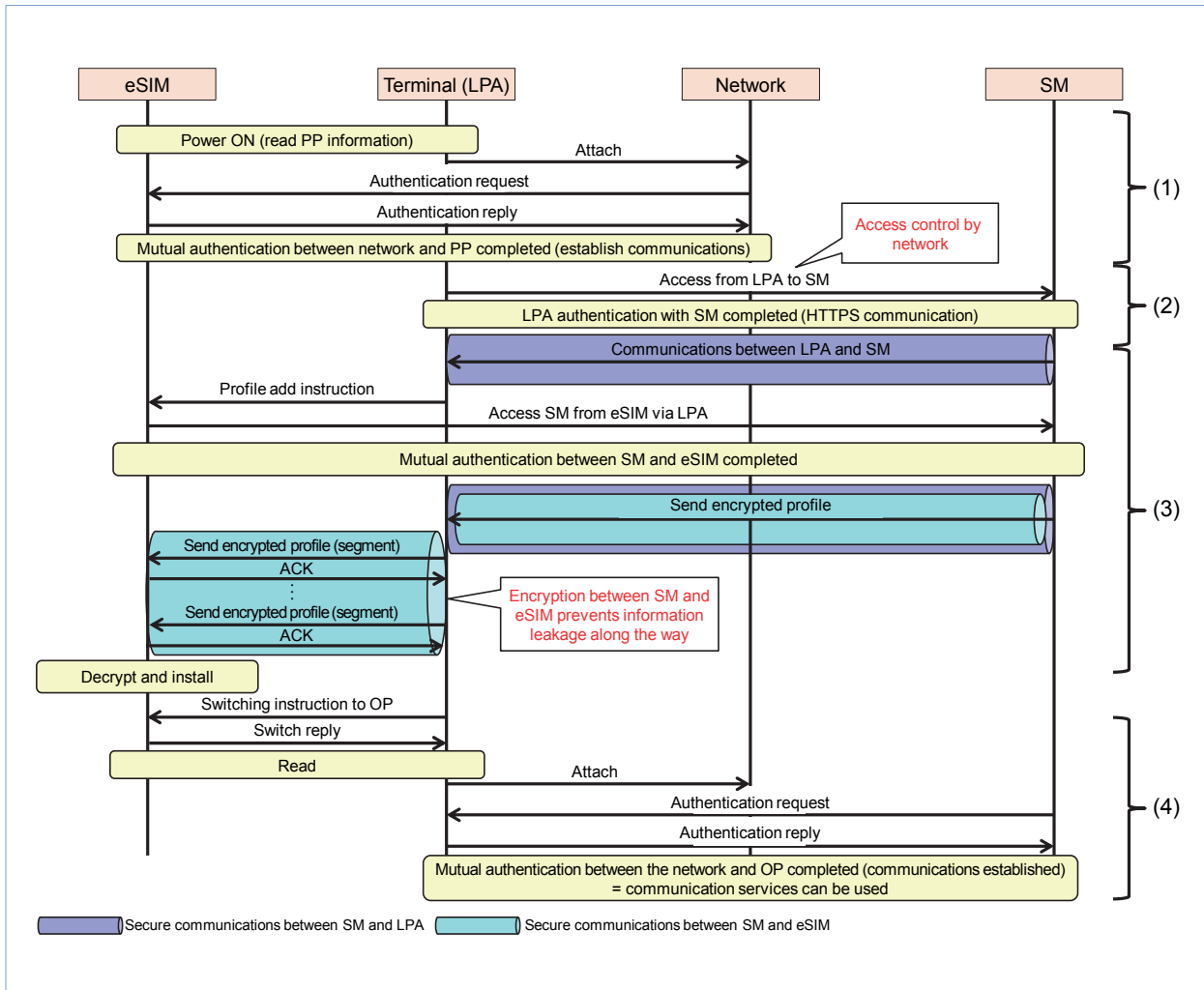


Figure 7 Example of a profile download sequence

and SM is established during this mutual authentication process, and a profile is then installed in eSIM 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 eSIM to shorten communication time using the mobile network.

- (4) 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 eSIM platform conforming to the GSMA global standard with an eye to a wide range of applications and low-cost provision.

It is envisioned that eSIM 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 eSIM, 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 eSIM platform to a dramatically diverse range of terminals to make communication services even more convenient for users.

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.