Technology Reports

IoT/M2M eSIM SM

Building of GSMA3.1-compliant eSIM Commercial System for IoT/M2M through Partnership between Operators

Solution Service Department Koji Makino Daichi Kishi
IoT Business Department Jun Bian

In view of the global trend toward IoT/M2M products, NTT DOCOMO has created the world's first multivendor eSIM linkage system enabling flexible rewriting of SIM information through partnership with overseas operators.
This article describes the mechanism for achieving this eSIM for IoT/M2M.

1. Introduction

In June 2017, NTT DOCOMO and China Mobile Communications Corporation, a Chinese telecommunications carrier, completed development of an embedded Subscriber Identity Module (eSIM)*1 linkage system between different vendors. Based on the "Remote Provisioning Architecture for Embedded UICC Technical Specification Version 3.1" (hereinafter referred to as "GSMA3.1") specification formulated by the GSM Association (GSMA)*2, this is the world's first eSIM linkage system for multivendor Internet of Things (IoT)*3/Machine to Machine (M2M)*4 in commercial environments [1].

NTT DOCOMO is introducing this technology as a Business-to-Business (BtoB) solution for developing overseas businesses with automobiles, construction machinery and industrial devices etc.

This article describes a Remote Provisioning*5 system based on GSMA3.1 standard specifications.

2. eSIM for IoT/M2M

2.1 Differences with Conventional Technology

In the world of IoT/M2M, most designs have included an unremovable SIM directly embedded in the devices*6 mounted in IoT/M2M-enabled products

*1 eSIM: The generic name for SIMs in which the communications profile information of a telecommunications carrier can be remotely rewritten using Over-The-Air (OTA) radio communications, different from normal SIM cards.
*2 GSMA: The Global System for Mobile Communications. A global standardization organization in mobile communications businesses.

as requirements for achieving miniaturization and high reliability with fewer parts. Also, with the global trend toward these IoT/M2M businesses, the demand for products usable with the communication services of local telecommunications carriers in various countries is on the rise.

However, with conventional technology, the Mobile Network Operator (MNO) information written on to the SIM is fixed and cannot be rewritten, meaning that the only solutions for overseas use were to replace the SIM with one for the local telecommunications carrier or use roaming*7 etc.

Since there are increasing demands to use local telecommunications carrier communication services in various countries without changing the SIMs inserted in products, GSMA standardized technology to flexibly change the MNO information written to the SIM [2] [3]. NTT DOCOMO is one of the operators involved in the study of this architecture [4].

2.2 Differences with Consumer eSIM

In general, technologies used with eSIM services are divided into those for consumer uses, and those for IoT/M2M [5]. The applications and standard specifications for these are not the same. **Figure 1** provides a comparison of the technologies.

Consumer eSIM technology is used to enable the user to activate the line with simple operations using the initial settings of the terminal when it was first purchased. Consumer eSIM technology is also prescribed by GSMA [6] - [9].

eSIM for IoT/M2M technology is used by applications to switch telecommunications carriers from remote servers.

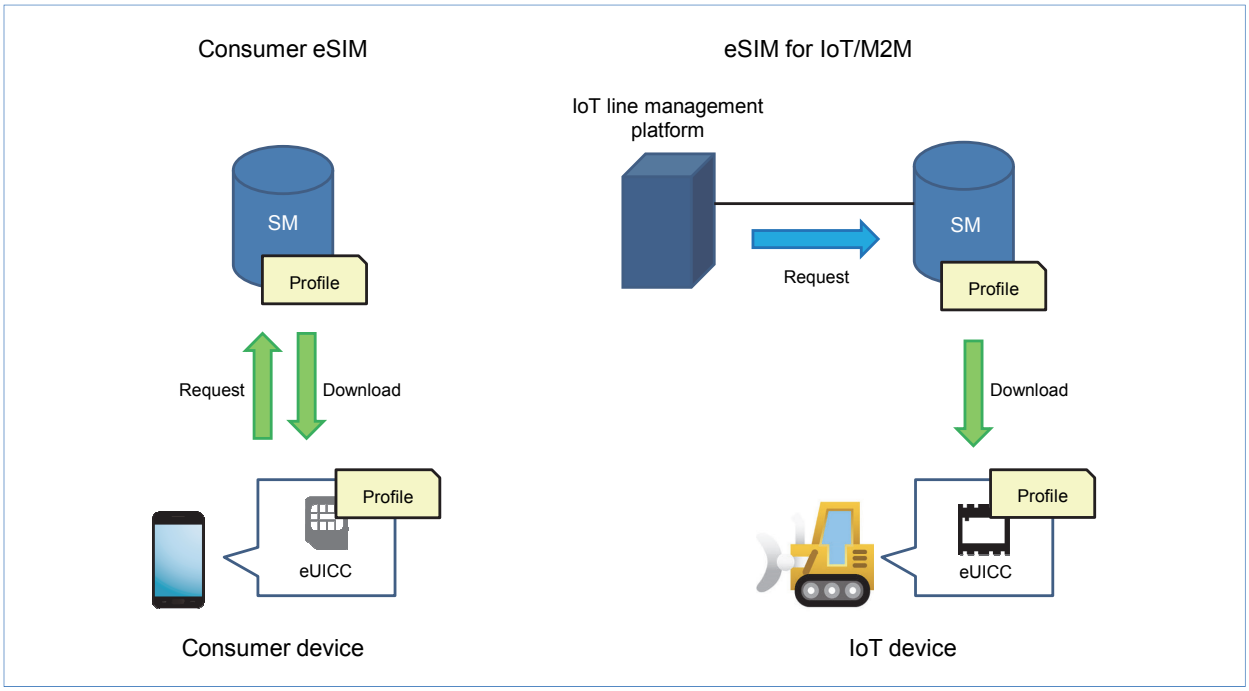

Figure 1 Differences between consumer eSIM and eSIM for IoT/M2M

*3 IoT: Mechanisms that entail various "things" connected to the Internet to enable a wide range of previously unachievable information sharing.
*4 M2M: Communications among machines.
*5 Remote Provisioning: Rewriting communications profiles remotely via OTA.
*6 Device: In this article, a "device" refers to a device such as an M2M module that has mobile communications functions.
*7 Roaming: A mechanism that enables users to use services similar to their subscribed carriers within the service areas of alliance partner carriers, but outside the service areas of their subscribed carriers.

As shown in Fig. 1, the profile[*8] is downloaded via mobile terminal operations with a consumer eSIM, whereas with an eSIM for IoT/M2M, the profile is downloaded through a request from the IoT line management platform of the telecommunications carrier.

2.3 User Experience

This section describes the use case of remote provisioning using the example of exporting a Japanese-manufactured product from Japan that uses a DOCOMO line as its default setting. There are real demands for BtoB solutions as illustrated by this example.

First of all, the user applies to NTT DOCOMO for an eSIM, and receives the eSIM issued by NTT DOCOMO. Next, the user embeds the eSIM into their product, and after enabling communications through the activation of a DOCOMO line, the user performs shipping test etc. in Japan. After the product containing the eSIM is taken overseas, roaming is commenced for the DOCOMO line. After that, the user triggers switch over to the desired line by specifying the line and telecommunications carrier, and remote provisioning is done for the specified line via roaming. When this is complete, the product is enabled for communications using a local telecommunications carrier line, and those communications services become available.

2.4 Effects of GSMA3.1 Support

GSMA3.1 [3] prescribes the following standards, which logically enable multivendor connection between components in remote provisioning architecture.

- Embedded Universal Integrated Circuit Card (eUICC)[*9] architecture
- Remote provisioning architecture interface
- Remote provisioning architecture security functions

The advantages of MNO through GSMA3.1 support include the ability to build multivendor systems for Subscription Manager (SM)[*10] and eUICC. In addition, as an advantage to the user, requirements for devices embedded in equipment to achieve remote provisioning are becoming clarified, and future increases of supporting devices are expected.

Currently, the latest version for Remote Provisioning Architecture for Embedded UICC Technical Specification is 3.2 [10].

3. eSIM for IoT/M2M Mechanism

3.1 Overview of the Structure and Operations

The system that NTT DOCOMO has built with China Mobile adopts one of the structures prescribed by GSMA3.1. **Figure 2** describes an overview of the structure and its operations.

SM is divided into two functions - SM Data Preparation (SM-DP) and SM Secure Routing (SM-SR). The following describes an overview of these functions.

- SM-DP: Securely stores the MNO communications profile
- SM-SR: Retains the eUICC Information Set (EIS) and ensures secure communications with eUICC

*8 Profile: A collection of data including information such as a phone number, subscriber ID, and network information.

*9 eUICC: An embedded UICC or UICC that enables remote provisioning. In this article, eUICC is used to describe the remote provisioning mechanism. UICC is an IC card used to record a unique ID for specifying a subscriber. UICC and SIM card are used synonymously.

*10 SM: A server that rewrites an eUICC communications profile remotely.

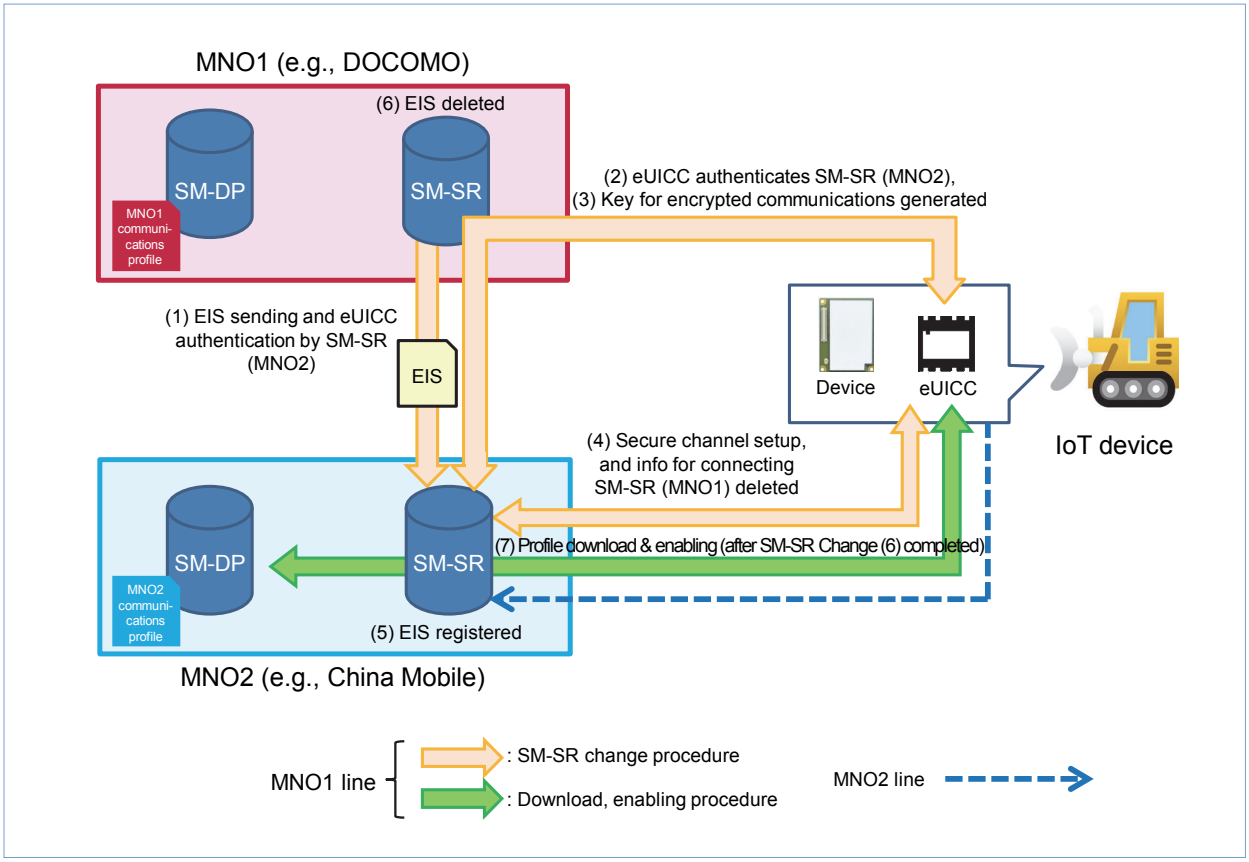

Figure 2 Overview of structure and operations

Fig. 2 describes switching communications profiles from the MNO to which the eUICC is first associated, called MNO1 (e.g., DOCOMO), to MNO2 (e.g., China Mobile).

In the figure, MNO1 and MNO2 communications profiles are stored in their respective SM-DPs.

With a structure like that in the example in the figure, remote provisioning is performed with the following procedure.

- SM-SR Change (Fig. 2 (1) to (6))
- Profile Download and Profile Enable (Fig. 2 (7))

If downloading the destination communications profile via the SM-SR associated with the destination MNO is required, SM-SR change procedures will be required in the remote provisioning procedure.

Note that in GSMA3.1 specifications, the configurations of SM-DP and SM-SR are not limited to the example in the figure.

3.2 Overview of SM-SR - eUICC Communications Routes

The following describes a general example configuration of a communications route between SM-SR and eUICC.

1) Types of Communications Routes

Figure 3 describes communications routes between SM-SR and eUICC.

GSMA3.1 prescribes communications methods with SMS and packets (HTTPS*11) between SM-SR and eUICC.

SMS is used for sending and receiving small-sized remote provisioning command, while packets (HTTPS) are used for sending and receiving large-sized remote provisioning command.

With packets (HTTPS), a Bearer Independent Protocol channel (BIP channel) is established between a device and an eUICC by sending a push-type SMS that instructs the establishment of BIP channel from the SM-SR to the eUICC before the communications route is established.

2) Configuration of the SM-SR - IoT Line Management Platform*12

Connections between SM-SR and the components of the IoT line management platform owned by the MNO are configured as follows.

- SM-SR and SMS Center (SMSC)*13 are connected using Short Message Peer to peer Protocol (SMPP)*14 to enable sending and receiving of commands via SMS between SM-SR and eUICC.
- SM-SR and the packet switch (Gateway GPRS Support Node (GGSN)*15 or Packet data network-Gateway (P-GW)*16) are connected using IP to enable sending and receiving of commands via packets between SM-SR and eUICC.

3) Structure between IoT Line Management Platform and Devices

This structure is configured with normal Global System for Mobile communications (GSM)*17/Universal Mobile Telecommunications System (UMTS)*18/LTE, so detailed descriptions are omitted.

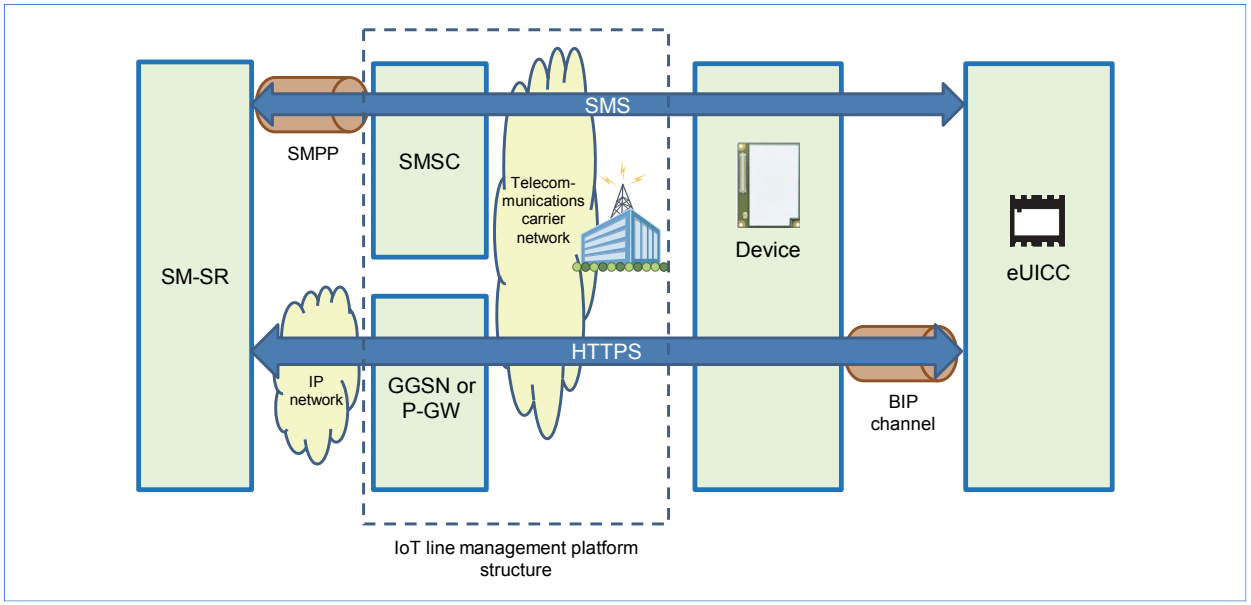

Figure 3 Overview of SM-SR - eUICC communications routes

*11 HTTPS: An HTTP communications method that uses TLS protocol to prevent attacks such as spoofing, intermediary attacks or eavesdropping. As well as HTTPS, Card Application Toolkit Transport Protocol (CAT-TP) is also prescribed in GSMA3.1 as a packet communications method.

*12 IoT line management platform: A platform that accommodates and manages IoT/M2M devices.

*13 SMSC: The SMS Center server. Stores and re-sends SMS data.

*14 SMPP: A communications protocol used between the SMSC server and applications for SMS sending and receiving.

*15 GGSN: A gateway connecting Packet Data Network (PDN) with functions for assigning IP addresses and forwarding packets to SGSN.

*16 P-GW: A gateway connecting PDN with functions for assigning IP addresses and forwarding packets to Serving Gatway (S-GW).

4) Structure between Devices and eUICC

Communications using BIP [11] [12] protocol are required between devices and eUICC to perform HTTPS communications between SM-SR and eUICC. GSMA3.1 Annex G Device Requirements including BIP support are necessary at the device side.

3.3 Remote Provisioning Sequence Overview

1) Information Elements Required for Remote Provisioning

The following describes the main information elements necessary for the remote provisioning mechanism.

- EID (eUICC ID): The eUICC serial number. The target eUICC is specified by the EID.
- EIS: A combination of eUICC authentication information and information for accessing eUICC, which is stored in SM-SR. Only the SM-SR with the corresponding EIS registered can issue commands to the target eUICC.

2) Remote Provisioning Sequence

Figures 4 and 5 describe the remote provisioning

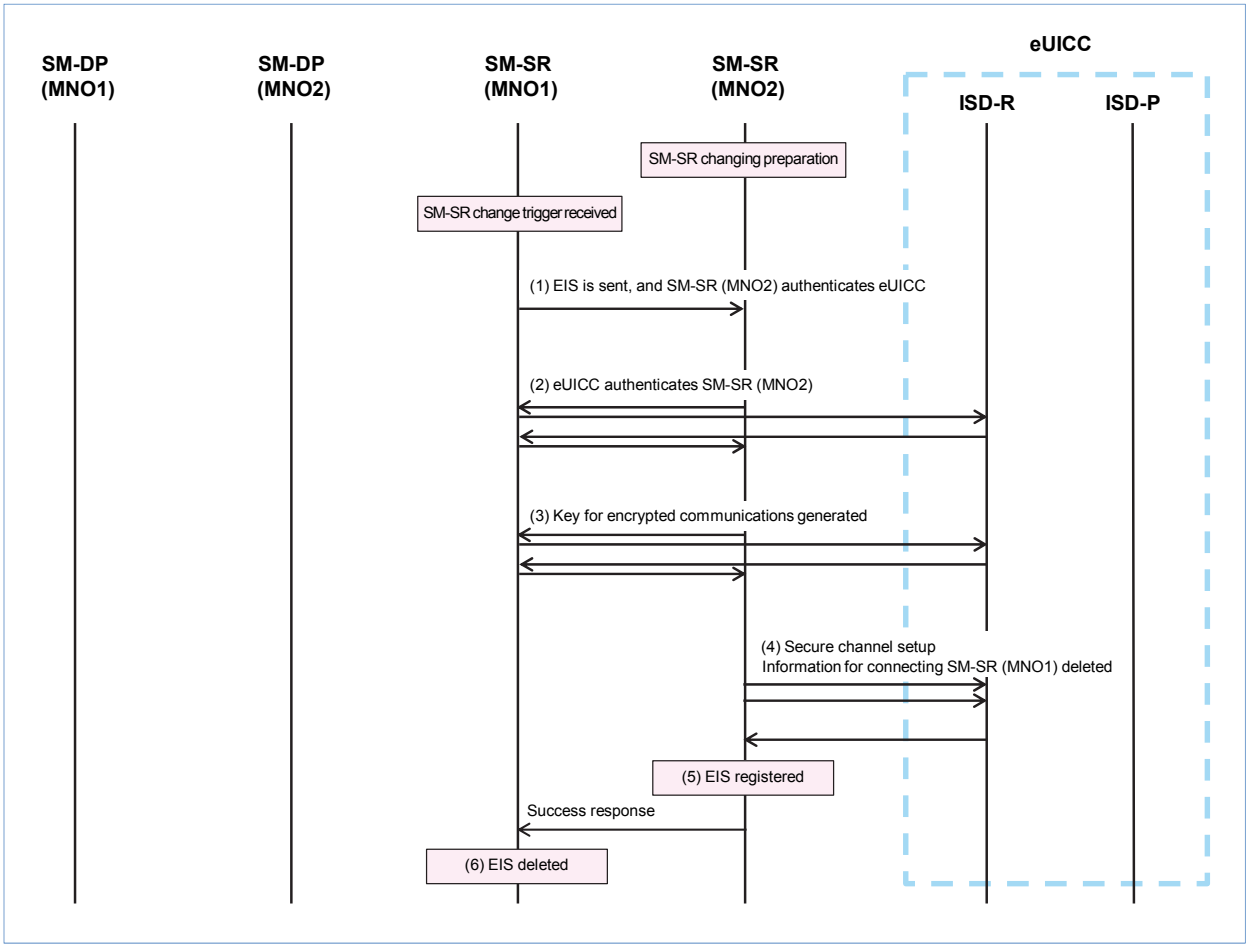

Figure 4 Overview of SM-SR change procedure

*17 GSM: A second-generation mobile communication system used widely around the world, especially in Europe and Asia.

*18 UMTS: A third-generation mobile communication system which includes W-CDMA (as used by NTT DOCOMO) and other access methods such as Time Division (TD)-CDMA.

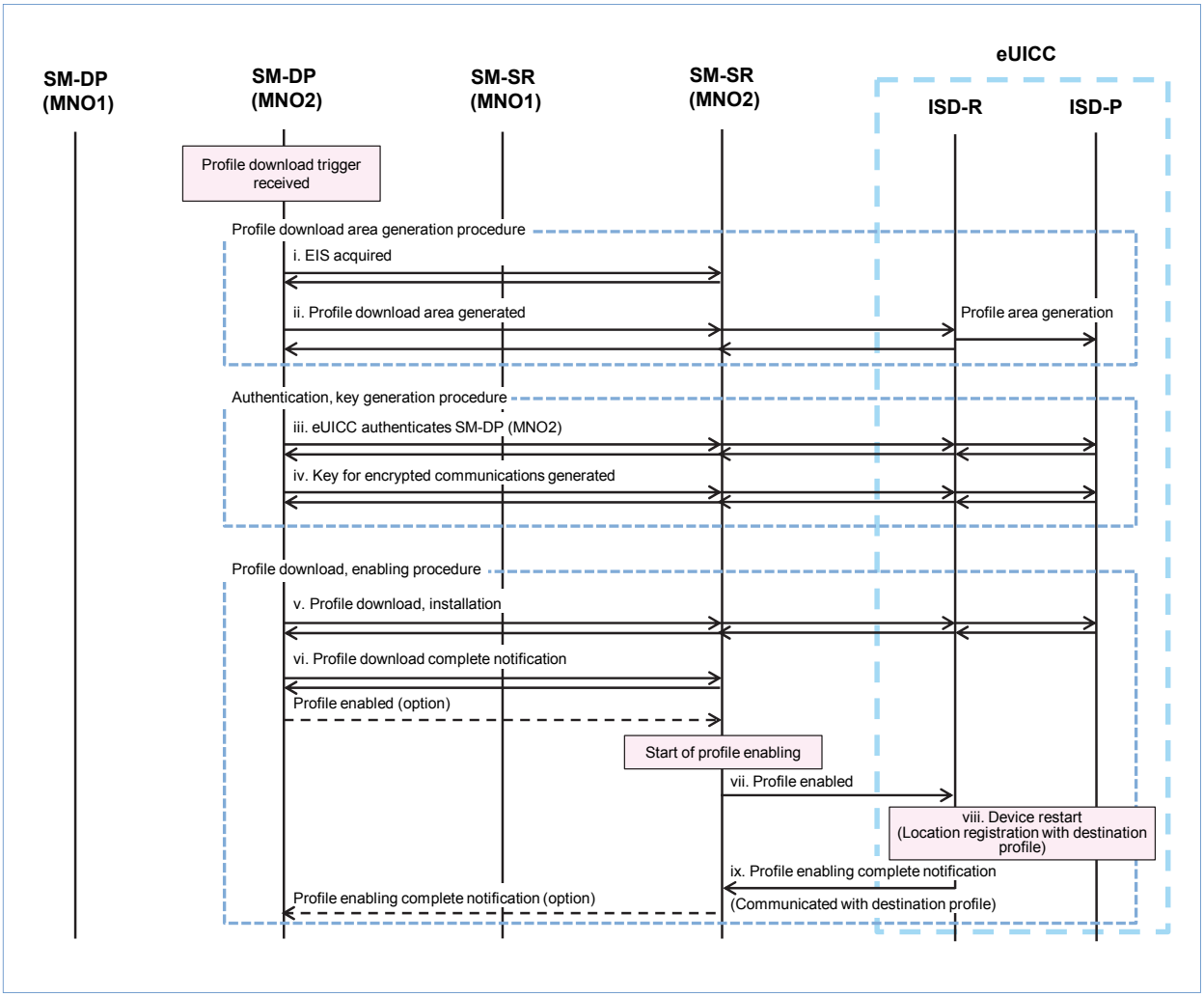

Figure 5 Overview of profile download & enabling procedures

sequence.

SM-DP/SM-SR and eUICC have preset internal authentication information verified by a common Certificate Issuer (CI)*19, and designed to enable secure mutual authentication in SM-SR change and profile download procedures.

Issuer Security Domain Root (ISD-R) and Issuer Security Domain Profile (ISD-P) areas are prescribed for eUICC.

- ISD-R: Only one exists in the eUICC for communicating commands with SM-SR.
- ISD-P: An area for storing profiles. Many exist in the eUICC for communicating commands with SM-DP.

Required authentication information is accessible by both ISD-R/ISD-P.

*19 CI: Issues electronic signatures required to achieve secure remote provisioning.

3) SM-SR Change Procedure (Fig. 4)

In the eUICC manufacturing stage, EIS is registered in the SM-SR which will be the first host, and has administrative rights to access the eUICC. The administrative rights are transferred when the EIS storage destination SM-SR is changed with the SM-SR change procedure.

As described in Fig. 4, the SM-SR change procedure entails transfer of rights to manage communications with eUICC from SM-SR (MNO1) to SM-SR (MNO2), and is executed in the sequence below.

(1) After SM-SR (MNO1) receives a trigger to change SM-SR, EIS is passed from SM-SR (MNO1) to SM-SR (MNO2). SM-SR (MNO2) authenticates eUICC based on EIS.

(2) Communications take place between SM-SR (MNO2) and eUICC ISD-R through SM-SR (MNO1), and eUICC authenticates SM-SR (MNO2).

(3) Communications take place between SM-SR (MNO2) and eUICC ISD-R through SM-SR (MNO1), and a key for encrypted communications between SM-SR (MNO2) and eUICC is generated.

(4) A secure channel is set up between SM-SR (MNO2) and eUICC ISD-R and key information for connecting SM-SR (MNO1) is deleted.

(5) EIS is registered in SM-SR (MNO2) (administrative rights are transferred to SM-SR (MNO2) at this time).

(6) EIS is deleted from SM-SR (MNO1) (eUICC can no longer be accessed from SM-SR (MNO1)).

4) Overview of Profile Download & Enabling Procedures (Fig. 5)

The destination MNO communications profile information is downloaded to the eUICC through the profile download procedure. After that, the eUICC is instructed to switch to the destination MNO communications profile through the profile enabling procedure.

As shown in Fig. 5, profile download & enabling is done in the following sequence to switch communications profiles.

i. SM-DP (MNO2) receives a profile download trigger, acquires EIS from SM-SR (MNO2), and performs necessary checks before the procedure starts.

ii. Communications are performed between SM-DP (MNO2) and eUICC, and a profile download area is generated as the eUICC ISD-P.

iii. Communications are performed between SM-DP (MNO2) and eUICC, and eUICC authenticates SM-DP (MNO2).

iv. Communications take place between SM-DP (MNO2) and eUICC, and a key for encrypted communications between SM-DP (MNO2) and eUICC is generated.

v. Communications are performed between SM-DP (MNO2) and eUICC, and the profile is downloaded and installed in ISD-P.

vi. A profile download complete notification is sent from SM-DP (MNO2) to SM-SR (MNO2).

vii. Communications are performed between SM-SR (MNO2) and ISD-R in eUICC, and a command to enable the downloaded profile is sent.

viii. Having received the commands to enable the

profile, ISD-R instructs the device to restart. Location registration with the newly downloaded communications profile is executed after the device restarts.

ix. After successfully registering location with the new communications profile, ISD-R sends a profile enabling complete notification to SM-SR (MNO2).

4. Conclusion

This article has described the mechanism of a Remote Provisioning system developed based on GSMA3.1 standards. We studied system integration by preparing environments to provide network services using SMs that support GSMA3.1 standards on commercial systems.

Multivendor connection is logically possible in GSMA3.1. In building the system, some issues with differences of interpretation of implementation occurred between various vendors, but efforts were made through NTT DOCOMO's partnership with China Mobile to quickly eliminate these issues and achieve the world's first GSMA3.1 standard specifications-compliant multivendor eSIM system.

Currently, various issues such as a lack of GSMA3.1-compliant devices required to use eSIM services are hindering full penetration of eSIM services. Also, system integration testing with devices embedded in products planned for commercial implementation will be required. Going forward, DOCOMO plans to continue working toward solving these issues.

REFERENCES

[1] NTT DOCOMO Press Release: "China Mobile Communications and NTT DOCOMO Develop World's First Multi-Vendor eSIM System for IoT," Jun. 2017. https://www.nttdocomo.co.jp/english/info/media_center/pr/2017/0627_00.html

[2] GSM Association: "Embedded SIM Remote Provisioning Architecture, Version 1.1," Dec. 2013.

[3] GSM Association: "Remote Provisioning Architecture for Embedded UICC Technical Specification, Version 3.1," May 2016.

[4] K. Suzuki et al.: "Standardization of Embedded UICC Remote Provisioning," NTT DOCOMO Technical Journal, Vol.16, No.2, pp.36-41, Oct. 2014.

[5] T. Sasagawa et al.: "eSIM for Consumer Devices toward Expanded eSIM Usage - Secure Installation Conforming to GSMA -," NTT DOCOMO Technical Journal, Vol.19, No.2, pp.5-13, Oct. 2017.

[6] GSM Association: "RSP Technical Specification, Version 2.2," Sep. 2017.

[7] GSM Association: "RSP Architecture, Version 2.0," Aug. 2016.

[8] GSM Association: "RSP Technical Specification, Version 1.1," Jun. 2016.

[9] GSM Association: "RSP Architecture Version 1.0," Dec. 2015

[10] GSM Association: "Remote Provisioning Architecture for Embedded UICC Technical Specification, Version 3.2," Jun. 2017.

[11] ETSI TS 102 226 Release 9: "Smart Cards; Remote APDU structure for UICC based applications," Jun. 2009.

[12] SIMalliance: "UICC Configuration for Mobile NFC Payments v1.0," Aug. 2014.