IIJ's eSIM Initiatives

3.1 What is an eSIM?

eSIM has become an oft-heard keyword ever since the iPhone XS was announced in September 2018. Here, we provide a technical explanation of eSIM and go over IIJ's initiatives in this area.

Traditional SIM cards consist of the following and are produced in tamper-resistant packages.

- Subscription Data for the mobile service
- Applets for valued-added services
- Secure storage for the subscription data and applets
- A processor that performs authentication, encryption key generation, etc.

Of particular note, authentication and encryption keys themselves cannot be read off of the SIM.

With eSIM, on the other hand, these elements are split into two parts: the profile, which contains the data and applets, and the eSIM card, which contains the storage and processor. In addition, the profile can be installed on the eSIM card from a dedicated server over a network. The specification was developed by GSMA[*1]. The mechanism for installing a profile via a network is called RSP (Remote SIM Provisioning). RSP itself is also used with traditional SIMs as a means of remotely changing data on the SIM using OTA (Over-the-Air) technology. As a full MVNO, IIJ also uses OTA to write phone numbers to some SIMs when activating the lines.

The term eSIM stands for embedded subscriber identifier module, or embedded SIM. At present, it mostly refers to SIMs to which profiles can be installed over a network using RSP. They were developed because a mechanism for installing profiles over a network was required for SIMs used in embedded applications.

Some embedded applications employ SIM chips that are soldered directly to the circuit board instead of the more common card-type SIMs. The following advantages of SIM chips explain why.

- Targeted at industrial equipment and thus offer high durability
- Soldered to the board and thus resilient to the loosening of connections caused by vibration
- Soldered to the board during manufacturing, thus obviating the SIM insertion process
- Small size enables device miniaturization

To take advantage of these benefits, IIJ added SIM chips to its full MVNO SIM lineup in February 2019.

Although SIM chips offer such advantages, it is virtually impossible to change the SIM once it has been embedded into the device during the manufacturing process. This means that the SIM's mobile line needs to be determined at manufacture, which raises the following problems.

- Inability to standardize inventory of products for different export destinations
- An active phone line needs to be used to check operating status at the time of manufacture
- Mobile line cannot be switched even if the location where the product is used changes
- Mobile line cannot be switched to, e.g., reduce communication costs

*1 Short for the GSM Association, an industry group that represents mobile operators. Formed in 1995 to promote the spread of the GSM 2G standard. It is the largest group in the industry, encompassing over 1,000 companies across 220 countries, including around 800 mobile operators. Also known as the organizer of Mobile World Congress (MWC), the world's largest exhibition for the mobile industry, held every February.

While the use of SIM cards solves these problems, there are on-site work costs associated with swapping out cards.

So eSIMs were developed to solve the above problems. The profile can be installed after manufacture, eliminating the need for a mobile line contract to be set up when the SIM is embedded. Because profiles can be installed remotely, there are no on-site costs associated with exchanging SIMs.

3.2 How eSIM Works

3.2.1 eSIM Internal Structure

Figure 1 depicts the internal structure of an eSIM. Among the elements shown, ISD-R, ISD-P, and ECASD are what characterize eSIMs.

The ISD-R*2 is a direct interface between the inside and the outside of an eSIM and is what manages the eSIM. Operations like downloading a profile, installing a downloaded profile, and switching to or deleting an installed profile are all performed via the ISD-R.

The ISD-P*3 is the equivalent of a traditional SIM card and is created for each installed profile. Profiles downloaded from servers are formatted so as to describe the procedure for creating the ISD-P. The profile is interpreted during installation to create the ISD-P. Once the ISD-P to be used for communications is activated, the eSIM looks like a normal SIM from the device's perspective.

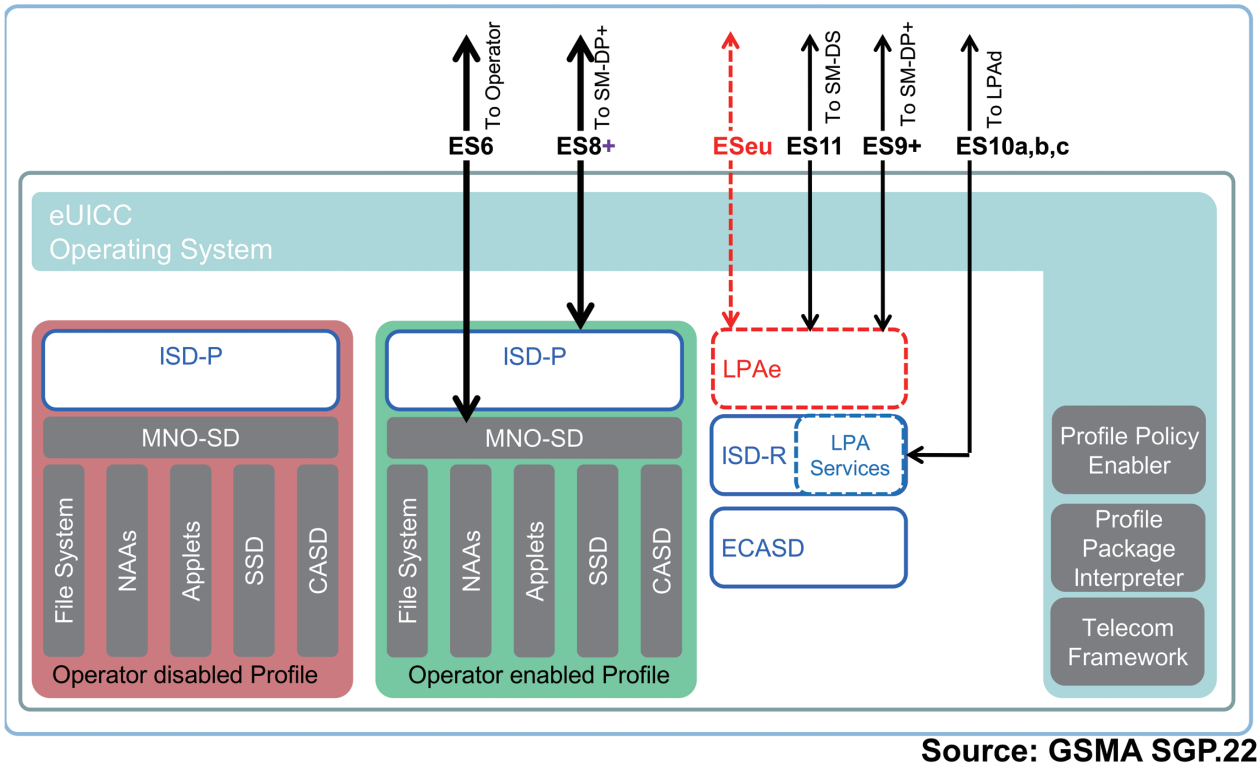


Figure 1: Internal Structure of an eSIM

*2 ISD-R: Issuer Security Domain Root
*3 ISD-P: Issuer Security Domain Profile

The ECASD[*4] stores the keys used in protecting the data when downloading a profile. A stored key is used for authentication between the server and the eSIM card. A stored key is also used to decrypt the downloaded profiles, which are encrypted by the server.

The data protection keys stored in the ECASD are signed using Public Key Infrastructure, and a similarly signed key is stored on the server side. To ensure SIM security, GSMA signs these keys as the root certificate authority, and keys signed by other certificate authorities are treated as invalid.

To obtain a GSMA signature, suppliers need to obtain SAS accreditation for each of their eSIM production sites and profile storing server sites. Because of the high cost of SAS accreditation, accredited eSIM production and server sites are limited in number. In most cases, operators do not have their own servers but instead use the services of SAS-accredited suppliers.

As of June 2019, there are broadly two specifications for eSIMs that support the remote intallation of profiles in this manner.

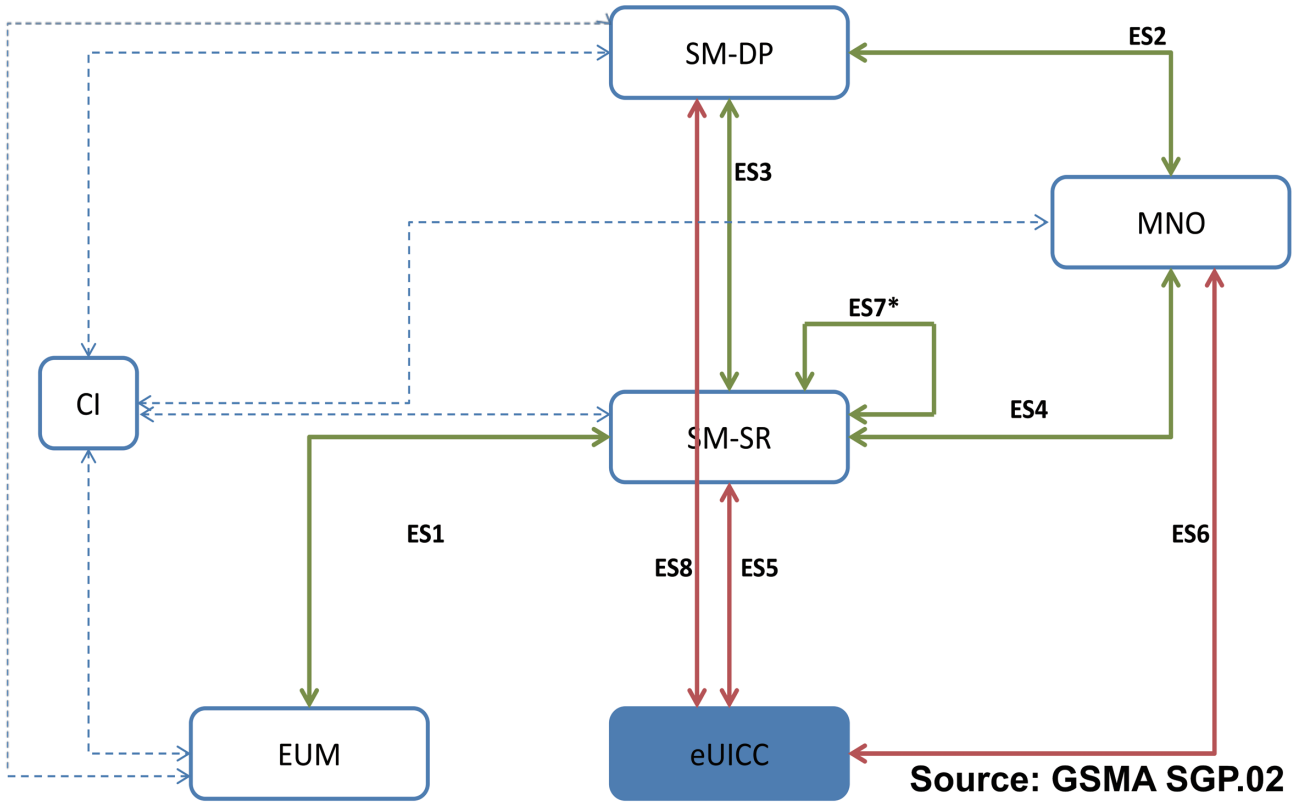


Figure 2: The M2M Model Interface

*4 ECASD: eUICC Controlling Authority Security Domain

■ **The M2M model**

Under this standard developed for M2M devices, eSIMs are controlled remotely. It is aimed at embedded devices, the original purpose of eSIMs.

■ **The Consumer model**

Under this standard developed for end user-managed devices, eSIMs are controlled via the device. The specification improves on parts of the M2M model that are difficult to deal with when it comes to end user-managed devices.

3.2.2 The M2M Model

The M2M model was the first eSIM specification developed. Since it is aimed at IoT devices, it allows profiles to be installed, switched, and deleted remotely. Figure 2 shows the elements of the M2M model. The main ones are as follows.

- eSIM card
- Device with an embedded eSIM card
- SM-SR[*5] server for secure routing to the eSIM card
- SM-DP[*6] server to provide profiles

In the M2M model, control of the eSIM card revolves around the SM-SR server. An SMS is sent from the SM-SR server to the eSIM card, a secure route between the SM-SR server and the eSIM card is opened, and the following operations are performed.

- Profile download and installation
- Profile switching
- Profile deletion

The eSIM card communicates with the SM-SR server directly, and only SMS and packets are transferred on the device in which the eSIM card is embedded. The device itself does not need much in the way of functionality; an ordinary modem of recent incarnation is generally fine. The specification is geared to environments where only limited functionality can be implemented, like embedded devices.

Since the SM-SR server controls the eSIM card in the M2M model, the eSIM card only communicates with a specific SM-SR server. Since they are set up to only communicate with a specific SM-SR server, the platform operator that manages the SM-SR server also supplies the physical eSIM card. And since all profiles are installed via the SM-SR server, the platform operator that manages the SM-SR server also obtains the profiles to be installed. Hence, profile choices depend on the platform operator.

Communication between the eSIM card and SM-SR server uses the IP protocol, but SMS is first used to trigger eSIM access by the SM-SR server. A mobile line is needed to send SMS messages, so eSIM cards that use the M2M model have a factory-installed profile called the bootstrap. Since all eSIM operations are performed remotely, bootstrapping requires connectivity in all countries, so one challenge is how to obtain this profile. Also, bootstrapping is unnecessary in cases where profiles do not need to be switched. There is no need to replace profiles in products used only in the domestic market, so traditional SIM chips are generally fine in this case.

*5 SM-SR: Subscription Manager - Secure Routing
*6 SM-DP: Subscription Manager - Data Preparation

3.2.3 The Consumer Model

The Consumer model specification was developed following the M2M model. It is aimed at end user-operated devices, such as smartphones, and enables all eSIM operations to be performed on the device. Figure 3 shows the elements of the Consumer model. The main ones are as follows.

- eSIM card
- Device with an embedded eSIM card
- LPA[*7] for managing the eSIM card on the device
- SM-DP+ server, which provides the profile
- SM-DS[*8] server, which searches for profiles provided to the eSIM

Unlike the M2M model, there is no SM-SR server for managing eSIM card profiles remotely. Instead, an application called the LPA manages profiles on the device. Another addition is the SM-DS server, which is not present in the M2M model. And because the SM-DP server has been modified to meet requirements for consumer devices, it is called the SM-DP+ in this model.

The LPA, added in the Consumer model, provides an interface to enable end users to do the following on the device.

- Enter the address of the SM-DP+ server where the profile is stored and the profile identifier
- Download profiles and install them on the eSIM chip
- Switch profiles
- Delete unnecessary profiles

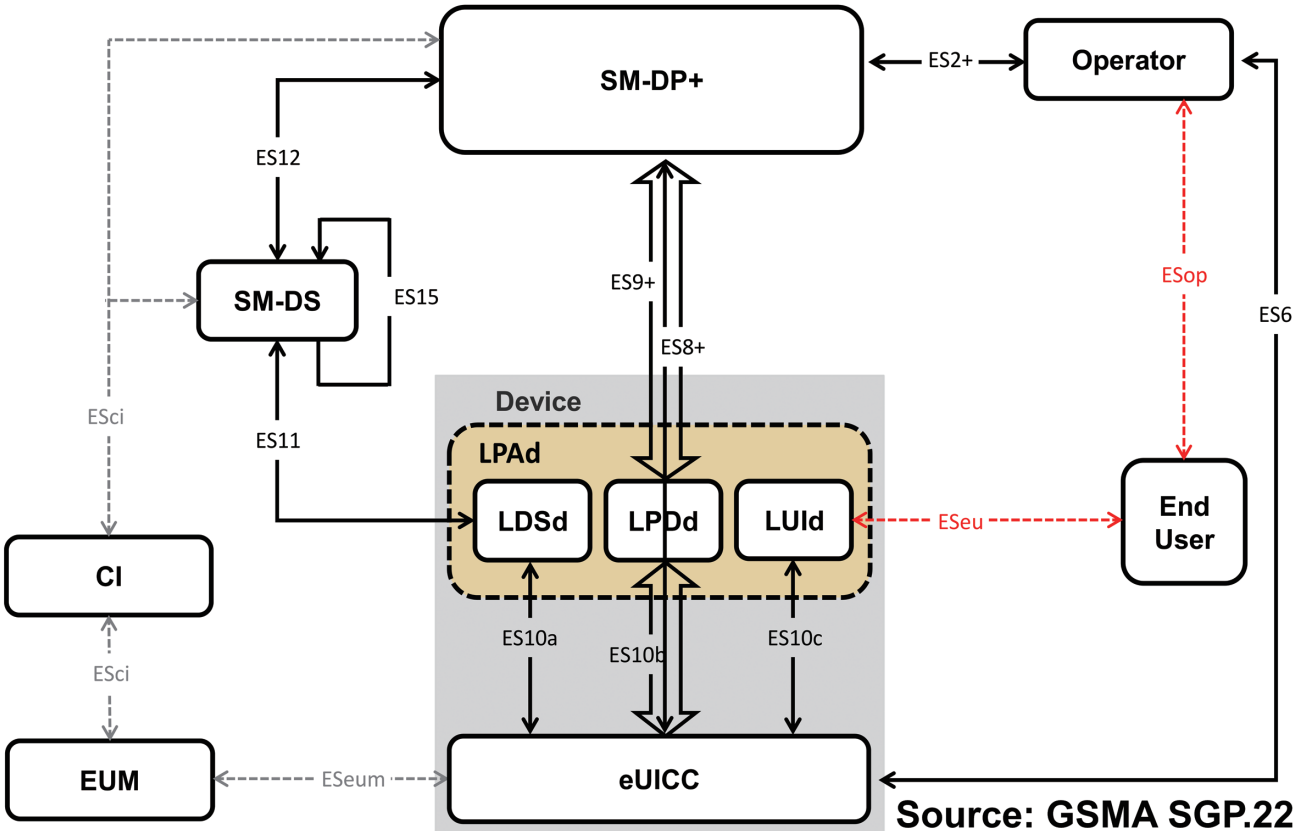


Figure 3: The Consumer Model Interface

*7 LPA: Local Profile Assistant

*8 SM-DS: Subscription Manager - Discovery Server

Two implementations for the LPA are defined: LPAd, where the LPA runs in the device, and LPAe, where it runs in the eSIM card. When device vendors develop Consumer model eSIM devices, they need to choose whether to use an eSIM that supports LPAe or to implement LPAd on the device. Because LPAe compatible eSIMs are not yet widespread, device vendors need to implement LPAd, so this is one hurdle to clear when developing Consumer model devices at present.

With this model, everything is done on the device by the LPA, so SMS is not needed the way it was in the SMS model. And since profiles can also be downloaded via Wi-Fi, there is no need for something like the M2M model's bootstrap profile. Because no extra mobile contracts are required, LPA is also implemented and the Consumer model adopted for IoT devices in some cases. On the other hand, in the interests of end user convenience, some eSIMs are supplied with a mobile line profile installed so as to enable the downloading of profiles.

To install a profile, the following must be passed into the LPA: the SM-DP+ server address and a Matching ID to identify the profile to be installed. A string called an activation code (like the one below) is used to do this.

```
1$SM-DP-PLUS.EXAMPLE.COM$MY-MATCHING-ID-0123456789
```

The string consists of the version number (currently fixed at "1"), SM-DP+ server address, and Matching ID, delimited by a "$" character. Entering these strings by hand is difficult, so they are usually converted to a QR code and read into the device (Figure 4).

Figure 4: An Activation Code in QR Code Form

3.3 Moves by Major Vendors

3.3.1 Apple

Apple was an early mover in this space, providing eSIM-like functionality in the form of its Apple SIM. Details of Apple SIM are not public, but it is thought to employ an M2M-model eSIM. Yet it is very much a custom service; for example, because end users each enter into their own phone line contracts, it incorporates a mechanism for activating mobile services via the device. Although Apple only provides the platform, the strength of its brand has seen it successfully obtain profiles from mobile operators in many countries.

A feature of the Apple SIM is that it offers users worldwide connectivity in a single SIM card. That said, only data plans, not voice call contracts, are available with an Apple SIM. Possibly this comes down to voice contracts requiring more in the way of identity checks than data contracts and the varying regulations from country to country making it difficult to provide a solution within a single platform.

Apple has continued to use the Apple SIM for the iPad but adopted a standard consumer-model eSIM for the iPhone XS, released in 2018, probably because it was not possible to uncouple the iPhone, which is a phone after all, from voice contracts. Given that the Apple SIM is still used on non-voice devices like iPads released after the eSIM-compatible iPhone XS, it would seem that Apple has only given up on voice contracts being provided via the Apple SIM. The reasoning behind the decision was probably that adopting a standard eSIM would mean that mobile operators create the platform, making it possible to meet the voice contract regulations.

With the Apple SIM, the contracts went through Apple, which made it difficult for an MVNO like IIJ to offer services. With the consumer-model eSIM on the iPhone XS and later models, there are no limitations on the profiles installed, so IIJ's full MVNO profile fits the bill. Users of the iPhone XS/XR are one major target of the IIJ eSIM services.

3.3.2 Microsoft

Microsoft included a standard LPA in Windows 10 version 1703, probably because it believes that eSIMs will be useful in realizing its Always-Connected PC concept. The inclusion of an LPA service in the OS obviates the need for device vendors to implement their own LPA, meaning it is now

easy for vendors to make eSIM-compatible devices so long as they obtain eSIM cards and compatible modem modules. So we can expect this simplification of device manufacturing to help fuel the spread of eSIM-equipped devices ahead. One sign of this is that Microsoft itself has released eSIM-equipped Surface Pros.

Microsoft also provides an app called Mobile Plans that lets users sign up for mobile plans via their device, like with the Apple SIM. In Japan as of June 2019, profiles can be purchased from KDDI, GigSky World Mobile Data, and Ubigi.

On another front, at Microsoft Ignite 2018, held at end-November 2018 in the US, Microsoft revealed plans to integrate eSIM support into enterprise MDM[*9]. Enterprise customers need device management for their PCs, and bringing the management of mobile subscriptions into the MDM fold will give enterprise device managers control over the eSIM profiles used in their devices as well.

3.3.3 Google

Google seems to be lagging Apple and Microsoft when it comes to eSIM support. Although it defined APIs related to eSIM in Android Pie, the OS itself does not have LPA functionality, so each vendor needs to implement an LPA app. Google itself does offer eSIM-compatible, LPA-equipped devices like the Pixel 2, Pixel 3 and Pixel 3a. But as of this writing in June 2019, the devices sold in the Japanese market are equipped with NFC[*10] instead of eSIM support, so it looks like Japanese users are unable to use an eSIM with these Google offerings.

Google has launched its own eSIM-based MVNO service called Google Fi, providing connectivity around the world. While the range of supported Android devices is limited, the iPhone is also supported. Given that the service is available for devices Google itself does not manage, like the iPhone, one can infer that it uses consumer-model, rather than M2M-model, profiles. However, the service is only available to US residents; access does not extend to end users around the world. Yet while it is limited to US residents, it does provide voice services, unlike with the Apple SIM. Google was probably able to achieve this because it provides the service as an MVNO and because it zeroed in on US-resident users, so that it only had to deal with the US regulations relating to end-user voice services.

3.3.4 Similar Services

While not the same as eSIM, some vendors are selling profiles based on proprietary specifications, mainly in Greater China. They provide a proprietary SIM along with an OTA service for installing profiles on the SIM, allowing end users to download and use profiles from mobile operators in a wide range of countries. Outbound travelers are the end-user target group, and the objective is to provide less expensive connectivity on the road than roaming services. An example of this type of service in Japan is the Henn na SIM series sold by H.I.S. Mobile.

With the appearance of eSIM-equipped devices like the iPhone XS, though, these services also seem to be transitioning away from proprietary specifications to open eSIM platforms.

3.4 IIJ's Initiatives

As a full MVNO operator, IIJ can provide its own profiles for installation on eSIMs. We have already launched an eSIM service providing our full MVNO profiles as one of our full MVNO service sales channels.

As discussed, eSIMs come in two forms: the M2M model and the Consumer model. IIJ has started targeting the Consumer model first with its eSIM services. The reason for this is that because IIJ's own profiles only provide connectivity in Japan, we believe the Consumer model is more suitable for our full MVNO services than the M2M model, which is geared to overseas deployment. Additionally, it can be difficult to ensure connectivity outside of the Japanese market with full MVNO profiles, and they cannot be used to bootstrap.

*9 MDM: Mobile Device Management
*10 NFC: Near-Field Communication

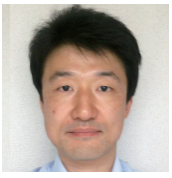
Last year, we carried out PoC testing based on the Consumer model as part of our efforts to get eSIM services off the ground. In the PoC, we installed the our full MVNO profile in a Microsoft Surface Pro LTE Advanced and accessed to the Internet with the profile successfully. We are also testing the operation of other target devices and building up our knowledge base. One thing we learned is that compatibility issues between profiles and eSIM cards can arise. As described earlier, eSIM card profiles have a specific format. A template notation is defined to simplify the profile descriptors, but we discovered that certain patterns result in installation errors with certain eSIM cards. We also discovered installation problems triggered by the absence of certain optional parameters in the profiles. Unlike the M2M model, which assumes control over the eSIM card, the Consumer model targets a wide range of eSIM cards, so building this sort of knowhow is crucial to providing services under this model.

On July 18, 2019, we commercially launched our eSIM Plan (beta version). Unlike eSIM services offered in Japan (Docomo's dtab, KDDI's prepaid plans for Windows), our service is broadly available and not restricted to a particular subset of devices. Building our own SM-DP+ server is not much of an option since it would require SAS accreditation from the GSMA, so we will use other companies' services like other mobile operators do.

3.5 eSIM Use Cases and Future Trends

What does the future have in store for eSIM usage?

The big difference between eSIMs and traditional SIMs is the elimination of the physical SIM. Eliminating the physical card and handling profiles as electronic data obviates SIM card delivery costs (not only money but distance and time). There is a tendency to focus on price when it comes to costs, but with eSIMs, there is no need to travel to a store or wait for a SIM to be delivered. This means end users can purchase profiles anytime, wherever they need them. Long-term contracts may not play to this benefit, but it makes purchasing prepaid contracts easier, especially for travelers looking to temporarily make use of services at their destination. Plus, there is no need to swap out physical SIM cards, the advantages of which include mitigating the risk of loss. And with DSDS[*11] devices like the iPhone XS, the main voice contract SIM card can go in the SIM slot while prepaid data SIMs can be purchased as and when needed. But within the context of the Japanese market, fully adopting eSIMs and the high degree of mobility they afford consumers would not be directly beneficial to the mobile operators. So it is difficult to see eSIMs gaining traction unless device makers take the lead in offering SIM-free devices. By making eSIM services available as soon as possible, IIJ hopes to set the stage for device makers to roll out eSIM-compatible devices.



Daisuke Maruyama
MVNO Service Development Section, Technology Development Department, MVNO Division
Mr. Maruyama joined IIJ in 2018. He is working on the development of service infrastructure for full MVNO services. Most recently, he has been developing eSIM service infrastructure of the type discussed in this volume.

*11 DSDS: Dual SIM Dual Standby