IIR

Internet
Infrastructure
Review

Sep.2019
Vol. 43

Periodic Observation Report

Messaging Technology

Focused Research (1)

Blockchain-based Identity Management and Distribution

Focused Research (2)

IIJ's eSIM Initiatives

IIJ
Internet Initiative Japan

Internet Infrastructure Review

September 2019 Vol.43

Executive Summary

The 30-year-long Heisei era has come to a close, giving way to the Reiwa era this past May. Heisei began in 1989, well before the Internet went mainstream, with the first commercial Internet services being launched in 1993. Windows 95, which contributed greatly to the spread of the Internet, was released in 1995. Google was founded in 1998. NTT Docomo launched i-mode, an Internet connection service for mobile phones, in 1999. NTT East and NTT West launched the BFlet's FTTH service in the year 2000. It was in 2001 that NTT Docomo launched FOMA, the world's first 3G mobile phone service. Apple released the first iPhone in 2007. And in 2010, NTT Docomo launched its 4G mobile phone service, Xi. The Heisei era's 30 year run saw substantial advances in information communications not only in Japan but across the globe.

This is our first IIR issue of the Reiwa era. While 5G mobile services are set to roll out in some countries, the monopolization of information by large platform operators has become problematic. In Japan last year, the Ministry of Internal Affairs and Communications launched a comprehensive assessment of competition rules in the telecommunications business, with an expansive scope covering not only the network layer but the platform and device layers as well. Under discussion is a vision for the country's networks with a view to 2030. Information and communication technology will continue to make immense contributions to the advancement of society, and we at IIJ hope to play our part as well.

The IIR introduces the wide range of technology that IIJ researches and develops, comprising periodic observation reports that provide an outline of various data IIJ obtains through the daily operation of services, as well as focused research examining specific areas of technology.

Our periodic observation report for this issue, found in Chapter 1, looks at messaging technologies with a focus on email. We examine deployment rates for SPF, DKIM, and DMARC sender authentication based on communications received via IIJ's email servers. Although SPF is quite well known, awareness of DMARC is yet to move forward. In light of survey data indicating that 80% of federal government domains in the United States have DMARC records, we will need to do something to raise awareness of DMARC in Japan. The report looks at deployment rates for sender authentication, discusses the encryption of email delivery routes, and describes the activities of M^{3}AAWG and JPAAWG, in which the author himself is involved.

Our first focused research report for this issue in Chapter 2 discusses identity management and distribution based on blockchain technology. The report looks at ERCs (Ethereum Requests for Comment) that use the Ethereum blockchain for credentials and touches on use cases in which credentials are used as public certifications. It also discusses the focus on blockchain-based credential management technologies, with several vendors having put forward concepts like DIDs (Decentralized Identifiers) and SSI (Self-Sovereign Identity) in the past few months.

Our second focused research report in Chapter 3 is about eSIMs. IIJ became a so-called full MVNO last year, with its own HLR/HSS systems. One feature that becoming a full MVNO enables IIJ to provide is eSIMs. The report explains why eSIMs are necessary and how they work, and then discusses IIJ's and other companies' initiatives in this area. The process of setting up communication services contracts is set for major changes in a world where physical SIM cards are not required and the profiles used to manage communications contracts are passed around as electronic data.

Through activities such as these, IIJ strives to improve and develop its services on a daily basis while maintaining the stability of the Internet. We will continue to provide a variety of services and solutions that our customers can take full advantage of as infrastructure for their corporate activities.

Junichi Shimagami

Mr. Shimagami is a Senior Executive Officer and the CTO of IIJ. His interest in the Internet led to him joining IIJ in September 1996. After engaging in the design and construction of the A-Bone Asia region network spearheaded by IIJ, as well as IIJ's backbone network, he was put in charge of IIJ network services. Since 2015, he has been responsible for network, cloud, and security technology across the board as CTO. In April 2017, he became chairman of the Telecom Services Association of Japan MVNO Council.

Messaging Technology

1.1 Introduction

The IIR has continued to report on quantitative trends in spam and its content, and as described in IIR Vol. 39, from here out we will be focusing on explaining and chronicling the spread of messaging technologies, including technologies designed to combat spam.

In this issue, we go over the results of a survey on the spread of sender authentication technologies, particularly DMARC, and explain MTA-STS, a mechanism described in an RFC last year that relates to TLS encryption connection policies for email delivery channels, as well as SMTP TLS Reporting, a mechanism for reporting of TLS connection information. In relation to messaging, we report on the JPAAWG 1st General Meeting, held last year and co-hosted alongside the Anti-spam Conference, as well as on JPAAWG itself.

1.2 Spoofed Emails and Information Breaches

Emails spoofed to appear as though they were sent by someone else cause so many kinds of problems that they are given names like phishing emails and BECs (Business Email Compromises). The damage caused by such emails is both serious and wide ranging, including financial damages and breaches of confidential and personal information resulting from the capturing of IDs and passwords, malware infections, and the like.

A number of incidents have spurred these sorts of occurrences on. A spate of information breaches from a variety of Web services have occurred, with email addresses included in the information exposed in almost all cases, making it possible for spammers to direct spam with precision. News also came of a massive breach of personal information from a major hotel chain last year, and reams of spam have subsequently made their way into the inboxes of the exposed addresses. Some such spam messages even contain a login password. Services available via the Web can be convenient, but the service provider's security cannot always be trusted. Users need to properly understand the strength of passwords and other information they set on Web services, as well as the types of services for which the same passwords are used.

1.3 Sender Authentication Rates

We have noted previously that sender authentication is an effective countermeasure against email spoofing. Settings

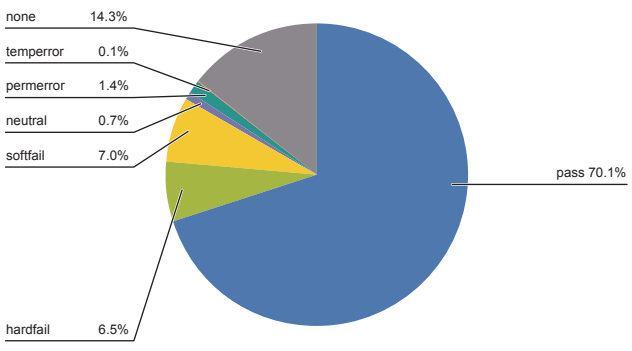


Figure 1: Breakdown of SPF Authentication Results

need to be configured on both the sending and receiving ends. Email recipients can use authentication to detect spoofed emails, while senders can configure their systems to ensure that their emails can be distinguished from spoofed ones.

If we are to promote the spread of sender authentication, we first need to understand how far it currently permeates the space. Here, we report on two sets of survey results, one looking at volume-based deployment rates among senders from a recipient perspective, and the other looking at the proportion of registered domain names on which sender authentication is implemented.

1.3.1 Volume-based Deployment rates

Here, we go over the spread of sender authentication among senders from an email recipient perspective based on email authentication data for emails received via IIJ's email services in April 2019.

Figure 1 shows a breakdown of SPF authentication results. Of all emails received, SPF authentication returned "none" for 14.3%. A value of "none" indicates that SPF authentication was not possible, so turning this around, it means that 85.7% of emails received were from senders that have implemented SPF. The year-earlier (April 2018) figure for "none" was 16.0%, around the same level, which indicates that sender authentication has spread to a point that the vast majority of received emails can be SPF authenticated.

Figure 2 shows a breakdown of DKIM authentication results. As a proportion of the total, the figure for "none" is 62.2%, which indicates that less than 40% of emails received were from senders that have implemented DKIM. The year-earlier figure for "none" was 62.4%, so DKIM deployment rates have not changed that much.

Figure 3 breaks down DMARC authentication results. And by the same measure, the figure for "none" here is 76.9%, indicating that around 20% of emails received were from domains where the sender has implemented DMARC. DMARC authentication uses the results of SPF and DKIM, so it is predictable that authentication rates here will be lower than for SPF and DKIM. That said, and although the resending of emails is an issue, emails can be DMARC authenticated via

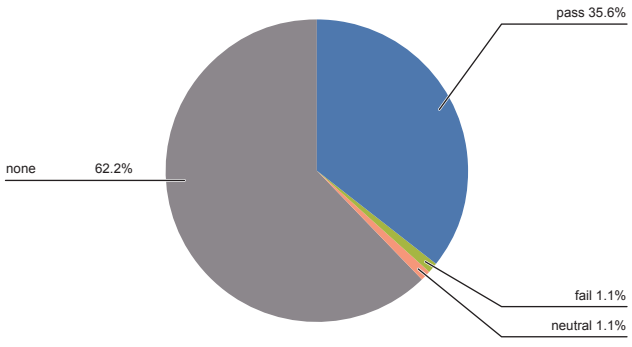


Figure 2: Breakdown of DKIM Authentication Results

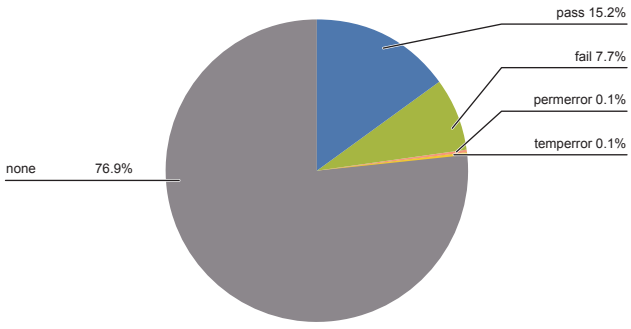


Figure 3: Breakdown of DMARC Authentication Results

SPF alone, so the figure is really quite low considering that the SPF deployment rate is above 80%.

Figure 4 shows the results for DMARC since January 2016. Initially, the figure for "none" was 87.5%, so on a volume basis, the deployment rate has risen by around 10 percentage points over almost three years. The proportion has roughly doubled. Although changes in the proportion of "fail" results have fluctuated over time, the data show that the proportion of all emails that can be authenticated, including those for which authentication fails, is gradually rising.

1.3.2 Deployment Rates Based on Registered Domain Names

Next, for registered jp domain names, we look at whether SPF or DMARC is implemented. As noted previously in Vol. 39, we have a joint research agreement with the Japan Registry Services (JPRS)—which manages jp domain names—and the Japan Data Communications Association for the purpose of gauging the spread of sender authentication technology. I am taking part in the studies as a visiting researcher for the Japan Data Communications Association.

Figure 5 shows the results for March 2018 onward. For domain names configured with an MX record, which indicates the domain name is used for email, the graph shows what proportion had a DMARC record configured, broken down by type of jp domain. According to the latest data from May, this was 0.95% of jp domains overall. By type, ad.jp tops the list, but still only with a figure of 3.4%. Next down the list with 2.1% is go.jp, which has a step-function look to it on the graph because the number of such domains registered is small.

Materials[*1] disclosed by NISC (the Cabinet Office's cybersecurity center) indicate that the use of SPF, DKIM, and DMARC on the sender and receiver sides is listed as a measure for preventing email spoofing within the information

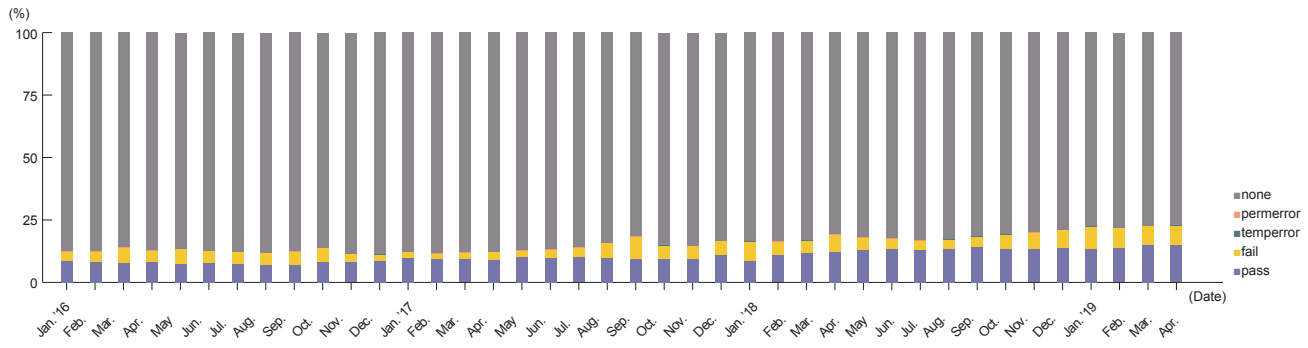


Figure 4: Breakdown of DMARC Authentication Results Over Time

*1 "Guidelines on the Formulation of Information Security Measures for Government Agencies and Related Bodies (2018 Edition)" (in Japanese at https://www.nisc.go.jp/active/general/pdf/guide30.pdf).

security strategy for government bodies. This means we can expect the proportion of go.jp domains with a DMARC record configured to increase ahead. Note also that registered go.jp domains top the list for the proportion with an SPF record configured (Figure 6).

Similarly, the proportion of all jp domain names with an SPF record configured was 59.7%. This is a 2.8-percentage-point increase vs. the previously reported figure of 56.9% (Vol. 39). The fact that this SPF adoption rate is still rising seems to indicate that awareness of SPF is quite high. Unfortunately, the rate of increase for DMARC is quite low compared with that for SPF, so we will need to boost awareness of DMARC somehow.

1.3.3 Deployment rates Overseas

According to a survey[*2] by the US-based Valimail, 80% of federal government domains in the United States have DMARC records. This was the highest rate among the industries surveyed. As I reported last time, this increase likely traces to a legally binding order[*3] issued by the United States Department of Homeland Security. And according to DMARC.org, a group that advocates for the use of DMARC technology, the number of domains in the DNS with DMARC records increased by over 2.5-fold in 2018[*4].

1.4 Encryption of Email Delivery Channels

Email is used not only to exchange simple messages but also as a means of transferring various types of data via attachment capabilities (MIME). Meanwhile, it does seem that users do not give much consideration to what route an email that contains data will take when being delivered nor to what level of data leakage risk exists. The SMTP email delivery protocol can use TLS (STARTTLS) as an extension. Here, we discuss issues with this conventional STARTTLS protocol and standards established to address those issues, namely MTA-STS and SMTP TLS Reporting.

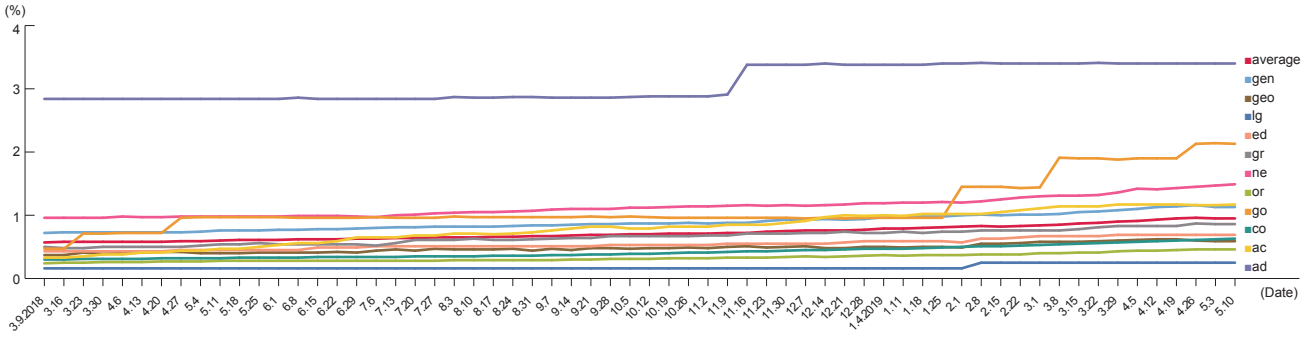


Figure 5: Proportion of jp Domains with a DMARC Record

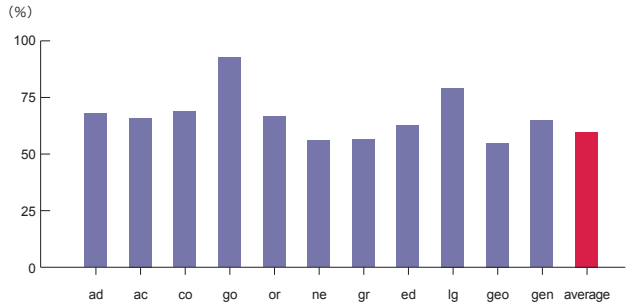


Figure 6: Proportion of Domains with an SPF Record Declaration

*2 Email Fraud Landscape, Q4 2018 (https://www.valimail.com/resources/email-fraud-landscape-q4-2018/).
*3 DHS, "Binding Operational Directive 18-01" (https://cyber.dhs.gov/bod/18-01/blank).
*4 DMARC Policies Up 250% In 2018 (https://dmarc.org/2019/02/dmarc-policies-up-250-in-2018/).

1.4.1 Issues with STARTTLS

The SMTP extension STARTTLS (TLS) is used to encrypt the channel when emails are delivered. The procedure is as follows: if the Recipient mail server supports STARTTLS (determined by the response when connecting), the sender sends a STARTTLS command to start a TLS session. So the channel cannot be encrypted under the following conditions.

- **Recipient mail server does not have STARTTLS (does not return a response to STARTTLS)**
- **The STARTTLS command is sent in order to start a TLS session but the available TLS version and cipher suites do not match**

Cipher suites are combinations of encryption algorithms, key length, and so on. Encrypted communications are not possible unless both sending and receiving ends are able to use the same cipher suite. If the STARTTLS command cannot be executed, many sending email servers will switch to conventional unencrypted plaintext email transmission. This setup exposes email to a sort of man-in-the-middle attack because by intercepting the SMTP session and deleting the intended recipient server's STARTTLS response, an attacker can force plaintext transmission and snoop the contents of email. This sort of technique is also called a downgrade attack.

1.4.2 MTA-STS and TLSRPT

MTA-STS[*5] is a mechanism in which recipient domains use a combination of DNS and HTTPS to publish their receiving policies. This mechanism allows you to determine whether TLS authentication is supported before sending an email and what action the sender should take if a TLS connection cannot be established.

Recipient domains should make the following settings.

(1) Configure an MTA-STS record
(2) Set a "well-known" path so that the MTA-STS policy can be fetched

The MTA-STS record is usually a TXT record that is named by adding "_mts-sts" to the destination domain and that starts with the string "v=STSv1". So if the mail destination domain is "example.com", the record is configured as follows.

```
_mta-sts.example.com.  IN TXT "v=STSv1; id=20160831085700Z;"
```

The id parameter is a string that can be used to determine when the policy has been updated. By first referring to this MTA-STS record, the sender can check whether the recipient domain supports MTA-STS.

*5 SMTP MTA Strict Transport Security, RFC 8461

To fetch the MTA-STS policy, the sender refers to the "well-known" path on the policy domain prepended with "mta-sts". The "well-known" path is described in RFC 5785. In the case of MTA-STS, it is fetched via an HTTPS GET request for the following path.

```
https://mta-sts.example.com/.well-known/mta-sts.txt
```

The MTA-STS policy contains line feed-separated (CRLF-separated) key/value pairs. The currently allowable parameters are shown in Table 1.

"max_age" specifies how long the policy should be cached. "mx" specifies patterns matching hostnames given in the MX record. Multiple hosts and patterns can be set. Table 2 shows the allowable values for operation mode ("mode"). The sending MTA determines whether to continue sending emails based on the value of this "mode" field.

An example of an MTA-STS policy appears below.

```
version: STSv1
mode: enforce
mx: mail.example.com
mx: *.example.net
mx: backupmx.example.com
max_age: 604800
```

The TLSRPT*6 specification is used to report to the sender if the policy verification succeeds or fails under MTA-STS or other mechanisms such as DANE*7. Senders use the DNS to publish a TLSRPT policy for receiving reports. Email recipients that support TLSRPT first determine whether this TLSRPT policy has been specified by the sender domain, and if fetchable, a report is sent to the report recipient, if specified, in that policy. The TLSRPT policy settings can be retrieved by prepending "_smtp._tls" to the target domain. The parameters are quite similar to those for DMARC*8 but differ in that "v=TLSRPTv1" specifies version 1 of TLSRPT and the "rua=" field, which specifies where the report is to be submitted, can specify the mailto schema ("rua=mailto:") as well as HTTPS ("rua=HTTPS:"). An example of a TLSRPT policy record appears below.

```
_smtp._tls.example.com. IN TXT "v=TLSRPTv1;rua=mailto:reports@example.com"
```

When emailing reports to destinations specified using "rua=mailto:", the report must contain a DKIM signature by the sender domain. The DKIM record of the sender providing the DKIM signature SHOULD contain the "s=tlsrpt" service type declaration.

Table 1: MTA-STS Policy Parameters

Parameter	Meaning
version	The version (currently only "STSv1")
mode	Expected behavior of sender if policy validation fails
max_age	Max lifetime of the policy (in seconds)
mx	Allowed MX record patterns

Table 2: MTA-STS Policy Modes

Operation mode	Meaning
enforce	Messages are not delivered to hosts that fail policy validation or TLS
testing	Report sent if sending MTA implements TLSRPT*6; messages continue to be delivered
none	Indicates that no explicit MTA-STS policy is applied

*6 SMTP TLS Reporting, RFC8460
*7 The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, RFC 6698
*8 Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC 7489

```
selector._domainkey.example.com  IN TXT
    "v=DKIM1; k=rsa; s=tlsrpt; p=MIf4qwSZfase4fa=="
```

Reports sent via email are sent as attachments (MIME) in the same manner as DMARC reports. An example of a TLSRPT policy record for sending reports over HTTPS also appears below.

```
_smtp._tls.example.com. IN TXT "v=TLSRPTv1; rua=https://reporting.example.com/v1/tlsrpt"
```

Report data should be compressed for both email and HTTPS transport. Whether applying compression or not, the media type should be consistent with the format ("application/tlsrpt+gzip" or "application/tlsrpt+json"). Reports are sent in JSON format, unlike DMARC reports. We do not go over the parameters given in the report data here, but details can be found in RFC 8460.

Based on this, Figure 16 shows plots of total traffic of the past 10 years. The data series are stacked. The outbound data are observations made at entry points, and the inbound data are observations made at exit points. Some traffic is eliminated within the backbone, such as that involved in attacks, but generally all traffic that comes into the backbone also exits at some point, so the totals are almost the same.

1.5 About JPAAWG

The IIR has mentioned the international antispam organization M^{3}AAWG[*9] several times in the past. Recently, it has also become a forum for a range of discussion on highly relevant security issues beyond that of email. It has also been supporting the establishment of regional organizations beyond North America and Europe, where many M^{3}AAWG members reside. A recently formed group is LAC-AAWG for Latin America and the Carribean. The organization is also working toward and supporting AFR-AAWG for Africa. This leaves only the issue of Asia and what to do there.

*9 Messaging, Malware and Mobile Anti-Abuse Working Group

IIJ has long been an active member in M³AAWG since it was established, but the number of participants from Japan has not really risen as much the number from the US and Europe. To increase the number of participants, we have been publicizing the M³AAWG's activities in Japan and sounding out the prospects of holding an M³AAWG General Meeting in Japan or Asia from time to time. Against that backdrop, M³AAWG has been making efforts to support M³AAWG-linked activities in other regions. And out of that process emerged efforts among M³AAWG and participants from Japan to set up JPAAWG.

As an organization, JPAAWG (Japan Anti-Abuse Working Group) is entirely independent of, but receives considerable support from, M³AAWG. The JPAAWG 1st General Meeting on November 8, 2018, was held in conjunction with the Internet Association Japan's Anti-Spam Conference, an event that has been running for over a decade, and attracted many speakers and participants. Speakers included the chair and key members of M³AAWG. With the event's success, we made preparations for ongoing JPAAWG activities, culminating in JPAAWG being formally established on May 30, 2019. We hope JPAAWG's future activities will be of interest to you.

1.6 Conclusion

In this issue, we described MTA-STS, a technical specification for reliably ensuring encryption of email deliveries, and TLSRPT as a means of ascertaining what operations have taken place. So far, the IIR has looked at sender authentication technologies including DMARC, ARC, and DANE, but email-related technical specifications continue to evolve along with new specifications such as BIMI (Brand Indicators for Message Identification) and JMAP (JSON Meta Application Protocol). Going forward, the IIR will continue to discuss new technical specifications and the background to their development.

Shuji Sakuraba

Senior Manager, Application Service Department, Network Division, IIJ. Mr. Sakuraba is engaged in the research and development of communication systems. He is also involved in various activities in collaboration with related external organizations aimed at bringing about safe and secure messaging environments. He has been a member of M³AAWG since its establishment. He is the chair of the Japan Anti-Abuse Working Group (JPAAWG). He is acting chairperson of the Anti-Spam mail Promotion Council (ASPC) and a member of its administrative group, as well as chief examiner for the Technology Workgroup. He is chairman of Internet Association Japan's Anti-Spam Measures Committee. He is a member of the Email Security Conference program. He is a visiting researcher for the Japan Data Communications Association. And he is a visiting researcher at JIPDEC.

Blockchain-based Identity Management and Distribution

2.1 Introductions

Everyday, it seems, media reports about various services based on blockchain technology appear. Among these are many unfortunate ideas that merely use blockchains as a distributed database, so much so that a number of flowcharts for determining whether you really do need to use blockchains have been published[*1]. There are several methods of classifying blockchains; broadly, they can be classified into private-use blockchains and public blockchains that underpin the security of cryptographic assets. With public blockchains, it is necessary to incentivize ongoing mining to extend the chain; for cryptoassets such as Bitcoin, it is necessary to extend the chain based on predefined rules. With cryptoassets, the main reason for using blockchain is to transfer assets from one address to another, but efforts are also being made to use this blockchain-based value-transfer platform for other applications. These are being called second layer or Layer 2 applications.

Here, we look at developments in ERCs (Ethereum Requests for Comment)[*2] used for credentials (identity information) from among the second-layer services for the Ethereum blockchain[*3]. We will also touch on use cases in which such credentials are stored in the blockchain, enabling public certifications, such as student or employee IDs, to be verified digitally. Finally, we also go over why several vendors and consortiums have put forward concepts such as Decentralized Identifiers (DIDs) and Self-Sovereign Identity (SSI), where the user is in control of managing their own identity, and take a look at the focus on technology for managing credentials based on blockchains.

2.2 IDs and Credentials as Identifiers

In focused research pieces back in 2015, we reported on trends in ID management technology at the time[*4*5*6]. Here, we consider IDs in the narrow sense of identifiers.

Real-world entities are linked with digital-world entities, and a unique identifier (which we will denote "ID") is assigned to identify the digital-world entity. The notion of an ID as an identifier must be kept conceptually separate from the various identity information that is bound to that ID. Further, because realms (the scope within which the ID is valid and can be used to identify something) are separately defined for each ID space, a single, unique entity in the real world can have multiple IDs even within the same realm.

Now the reason IDs are assigned in the digital space is that there is a need for third parties on the network to identify the entities to which IDs are assigned. The act of authentication accompanies all sorts of activities in the digital world. Authentication allows access to various resources and services, for instance.

This act of authentication can be accomplished by using pairs of tokens (secret information) and credentials (public information). According to the definition in NIST SP 800-63, a token contains a secret known to the user to which the ID in question has been assigned, and credentials bind various attributes to the ID. Cryptographic techniques are used to ensure the integrity of credentials. Credentials use cryptographic techniques to ensure content integrity. When the entity that holds the ID seeks verification of his or her attributes by a third party in the digital world, the token (secret information) can be used to verify that the holder of the ID is the entity to which it was assigned.

When a credential is presented together with an authentication operation, a receiving third party can verify what sort of entity the ID is using the attributes given in the credential. In addition to authentication in this manner, credentials are also used for authorization in some cases. An X.509 certificate is

*1 NISTIR 8202, "Blockchain Technology Overview" (https://doi.org/10.6028/NIST.IR.8202), Figure 6: DHS Science & Technology Directorate Flowchart.

*2 Ethereum Improvement Proposals (http://eips.ethereum.org/).

*3 Ethereum Project, Developer Resources (https://www.ethereum.org/developers/). In this volume, we do not cover technology related to smart contracts, a key feature of Ethereum.

*4 Internet Infrastructure Review Vol. 26, "1.4.3 ID Management Technology" (https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol26_EN.pdf).

*5 Internet Infrastructure Review Vol. 27, "1.4.2 ID Management Technology: From a Convenience and Security Perspective" (https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol27_EN.pdf).

*6 Internet Infrastructure Review Vol. 28, "1.4.3 ID Management Technology: Online Authentication Methods Not Using Passwords" (https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol28_EN.pdf).

an example of a credential because it binds a public key with one or more IDs. And in fact, SSL/TLS client authentication is one case of this. Deploying a personal X.509 certificate on the browser side allows a user to log in to a server, and this is used in applications like corporate online banking. A specification for X.509 Attribute Certificates[*7] provides a method that is closer to credential-like usage. Attribute certificates differ from ordinary X.509 certificates in that they do not contain a public key. A serial number used to identify the certificate is placed in an area for storing identifiers called the Holder so as to specify the X.509 certificate, and attributes bound to the certificate holder (subject) are then stored. Here the realm can be understood to be the certificates issued by the certification authority, the ID to be the serial number, and the credentials to be the attribute certificate. Credentials can be written to X.509 Attribute Certificates, but they are not actually implemented in applications that general users are likely to encounter, such as browsers, so there are hardly any cases of them being used at present.

2.3 Overview of ERC-725

ERC-725[*8] was proposed in October 2017 by software engineer Fabian Vogelsteller[*9], known for developing the ERC-20 token standard and web3.js. Like the IETF's RFCs, ERCs (Ethereum Requests for Comment) are documented proposals for improvements that anyone can author; the format and writing guidelines are given in ERC-1. A major feature worth noting is that authors are asked to keep their proposals compact. A similar class of documents exists in the Bitcoin community, known as BIPs (Bitcoin Improvement Proposals)[*10]. The method for reducing transaction data known as SegWit, for instance, is defined in BIP-141.

Smart contracts, a method for automatically executing contracts and performing services, are a new concept put forward by Nick Szabo in 1997 and thus predate Bitcoin. A commonly cited example of a smart contract is the vending machine. When certain conditions are met by two processes, namely that the user inserts payment for the desired beverage into the machine and the user subsequently presses the button corresponding to that beverage, a sale is automatically initiated. As well as being used for cryptoassets, Ethereum is also being viewed as a distributed application platform enabling the creation and execution of smart contracts[*11]. ERC-725 defines a Solidity interface for the behavior of a proxy account. Solidity is a language used to write distributed applications. ERC-725 refers to ERC-735[*12] and ERC-780[*13] and provides a framework for distributing credentials on the Ethereum blockchain based on these specifications. In the ERC-725 document, credentials are called claims. ERC-735 describes the format of claims, and ERC-780 describes an Ethereum Claims Registry (ECR). Under the framework specified in the Ethereum blockchain realm, an ID (identifier) is an Ethereum address (note that it is not a contract address), and the identity information of the identity holder bound to the address is certified by credentials, called claims. The claim issuer can issue a claim to any entity on the Ethereum blockchain using a private key in the claim issuer's possession. The identity holder passes the claim to be verified to the claim checker via some method, and the claim checker can verify the claim's veracity by verifying the digital signature. It is envisioned that this series of verification tasks can be performed both online and offline[*14].

Claims as specified in ERC-735 have the following simple data structure.

*7 RFC 5755, "An Internet Attribute Certificate Profile for Authorization" (https://datatracker.ietf.org/doc/rfc5755/).
*8 ERC-725 version 2: Proxy Account (https://github.com/ethereum/EIPs/issues/725) (http://eips.ethereum.org/EIPS/eip-725).
*9 Fabian Vogelsteller (http://frozeman.de/blog/).
*10 BIP (Bitcoin Improvement Proposals) (https://github.com/bitcoin/bips).
*11 Ethereum Project white paper (https://github.com/ethereum/wiki/wiki/White-Paper).
*12 ERC-735: Claim Holder (https://github.com/ethereum/EIPs/issues/735).
*13 ERC-780: Ethereum Claims Registry (https://github.com/ethereum/EIPs/issues/780).
*14 Fabian Vogelsteller, ERC Identity (https://www.slideshare.net/FabianVogelsteller/erc-725-identity).

```
struct Claim {
    uint256 topic;
    uint256 scheme;
    address issuer;
    bytes signature;
    bytes data;
    string uri;
}
```

ERC-735 claims should be implemented to enable the identity holder to present them to the claim checker, and a key characteristic is that the data are portable. ERC-735 provides a zone for writing URIs to an area that is not ToBeSigned, and it is here that data pointing to the identity information is shared via a distributed file system such as IPFS[*15]. The ERC-725 Alliance[*16] has an open-source project related to ERC-725[*17]. Also, a number of samples are available on sites[*18] built using this demo implementation, showing how the veracity of claims can be verified in the browser. It is worth noting that the specification allows you to sign your own identity information and thus make your own claims about yourself.

So under the ERC-725 framework, anyone can issue a claim. In other words, anyone can be a claim issuer, so you can issue a claim to anyone as long as you know their Ethereum address. A key issue, therefore, is how to establish trust for a claim issuer and how to value the claims issued by that issuer. There also appears to be functionality to allow, for example, claims to be revoked and the Ethereum address to be swapped out, but the specification is still incomplete in this regard. It also seems that discussion over what reputation system to use for issuers has only just begun.

So we are straddled with a problem of reputation, and we will probably need to work through a few stages before we are ultimately able to distribute claims the way we would like. My view is that the notion of claims will gradually gain traction via the following three steps. In the first stage, acquaintances in closed networks, such as SNS, will casually issue claims to one another. This phase will determine scalability. The next stage will see the formation of a framework

Table 1: Elements of the ERC-735 Claim Structure

Topic	Currently marked as ToBeDefined. A 256-bit space expected to contain information on the topic (or type) of claim.
Scheme	ToBeDefined. A 256-bit space to hold the processing method or signature algorithm to use, which would refer to separately defined schemes.
Issuer	A contract address or the Ethereum address of the key used to sign the signature.
Signature	Note that the signed data needs to be of the following structure: {identity holder's Ethereum address, topic, data}
Data	The hash of the identity information (claim data). The identity information itself is not written here, so sensitive information is not being written to the blockchain.
Uri	A URI pointing to the identity information. HTTP link, IPFS URI, or such like.

*15 IPFS (InterPlanetary File System) (https://docs.ipfs.io/introduction/).

*16 ERC-725 Alliance (https://erc725alliance.org/).

*17 ERC-725 Alliance, "Repository for code and discussion around ERC725 and related standards" (https://github.com/ERC725Alliance/erc725/tree/master/contracts/contracts).

*18 ERC 725: Demo implementation by Origin Protocol (https://erc725.originprotocol.com/); Origin Protocol, Inc. (https://www.originprotocol.com/).

for ranking issuers using existing user evaluation/reporting systems to assess whether they have issued incorrect claims or not. And finally, this will develop into a completely distributed, automated reputation system (Figure 1).

The Blockcerts[*19] project is another example of the use of portable claims in a vein similar to ERC-725; there are open-source code[*20] and verification demos[*21] available as well. Blockcerts is based on prototypes developed at the MIT Media Lab and Learning Machine. Work is ongoing to extend Blockcerts to implement multiple blockchain types, including Bitcoin and Ethereum. A smartphone app called Blockcerts Wallet has also been implemented and released, and MIT is now using the Blockcerts technology to write students' diplomas to the blockchain[*22]. And a Spanish university has also announced that when issuing degree certificates, it will use the SmartDegrees platform so that they can be managed on the Ethereum blockchain[*23]. The situation is a tad chaotic at present with multiple such second-layer platforms on the scene, so when selecting a platform, the business continuity prospects need to be taken into account.

As discussed so far here, claims embody a simple mechanism, but if the Issuer is trustworthy and the second-layer specification works properly, it is understood they can be used on a semipermanent basis so long as the reliability of the Ethereum blockchain remains intact. So the digital issuance of diplomas is one application apt for making good use of blockchain technology, and indeed, some such services have appeared in Japan. Once trusted organizations do not persist indefinitely, as attested by the closure of private schools in regional areas and the discontinuation of certifying exams by local governments. There are even cases of physical certificates issued by such organizations no longer being validatable. Hopefully, we are bound for an era in which claims distributed via an open framework, as discussed here, provide an alternative to physical certificates.

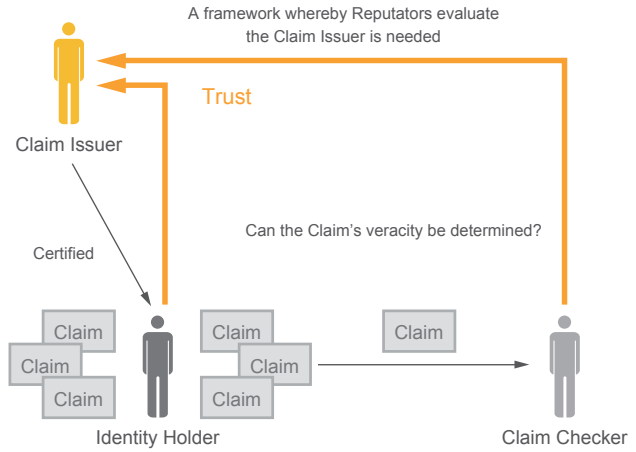


Figure 1: Framework for Issuing and Valuing Claims

*19 Blockcerts (https://www.blockcerts.org/).
*20 Repositories of the Blockcerts project (https://github.com/blockchain-certificates).
*21 Example Blockcerts (https://www.learningmachine.com/new-product/examples/).
*22 MIT News, Digital Diploma debuts at MIT (http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017).
*23 Universidad Carlos III de Madrid is issuing degree certificates with blockchain (https://www.uc3m.es/ss/Satellite/UC3MInstitucional/en/Detalle/Comunicacion_C/1371252827656/1371215537949/Universidad_Carlos_III_de_Madrid_is_issuing_degree_certificates_with_blockchain).

2.4 Decentralized Identifiers, DIDs

As identifiers, IDs are assigned within a specific realm. When it comes to authenticating across realm boundaries, the notion of the ID Federation comes into play and often appears in a single sign-on context. Credentials such as the X.509 Attribute Certificates and ERC-735 claims we have discussed only circulate within the realm in which they were issued. In reality, identity providers, whose role is also to issue IDs, do not exist in isolation. To enable the login functionality of service providers, such as SNSs, to be used from external services, that functionality is split off into the identity provider role. As such, in cases where ID linking functionality is used to log in to separate services, there is a risk that the ID will suddenly stop working because it is operated by a particular company or organization. Thus, the deactivation of one ID could result in an inability to use several other services. The deactivation—or in the worst case, deletion—of an ID because an SNS operator decided that inappropriate content had been posted can have negative impacts, and indeed there have been various real-world cases of this.

The notion of Decentralized Identifiers (DIDs) emerges from this backdrop. A feature of DIDs is that they are not valid IDs only in one specific realm and there is no centralized presence that manages the IDs. This is seen as highly compatible with the notion of Self-Sovereign Identity (SSI)[*24] proposed by the nonprofit Sovrin Foundation[*25]. SSI is similar to the idea that individuals have the right to control their own information. The term is used in recognition of the need for individuals to own and manage their own identities without going through a central managing authority. Credentials such as ERC-735 claims, as discussed above, can be passed around without the identity holder intending it. Not so with SSI; instead, the idea is that the identity holder has sovereignty over the distribution of his or her credentials.

The nonprofit ID2020 Alliance[*26] is an organization that seeks to achieve privacy protection and portable, user-centric identity management. There is also a project[*27] that looks to use claims written to a blockchain as an alternative to passports, analogous to the way people seek to use

*24 The Sovrin Alliance, "Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust" (white paper, version 1.0, January 2018) (https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf).

*25 The Sovrin Alliance (https://sovrin.org/library/rise-of-self-sovereign-identity/).

*26 ID2020 Alliance, The Alliance Manifesto (https://id2020.org/manifesto).

*27 Taqanu (https://www.taqanu.com/impact).

cryptoassets rather than legal currency in cases where the reliability of nationally issued currencies has diminished. The idea can be interpreted as follows: data corresponding to claims that everyone recognizes and that are issued by credible institutions can provide a passport-like means of personal identification. The Sustainable Development Goals (SDGs)[*28] compiled by the United Nations in 2015 state Target 16.9 as: "By 2030, provide legal identity for all, including birth registration". And the ID2020 Technical Requirements[*29] have been formulated in an attempt to assist the world's "identity refugees", thought to number over a billion. The document covers seven categories—applicability, identification, authentication, privacy, trust, interoperability, and recovery—and is highly useful as a design guideline of this type.

The intention behind DIDs, meanwhile, can be gleaned from documents developed by the W3C[*30][*31]. The W3C defines a DID as a globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network[*32]. ERC-735 claims use Ethereum addresses as the ID space, but a method has also been proposed for wrapping Ethereum addresses in the W3C DID format instead of using them as raw DIDs[*33]. So W3C DID is being promoted as a global ID capable of representing a range of IDs. The existence of DIDs alone only solves the issue of nonconflicting numbering, but in conjunction with the claim use cases[*34] and the verifiable credentials (originally called claims, the wording was later changed to credentials) data format[*35], they are poised to solve the various other issues faced.

Group work at the Web of Trust VIII event in March 2019 (RWOT8)[*36] and the 28th Internet Identity Workshop[*37] in April 2019 dealt with many topics centering on DIDs and SSI. The 2019 annual meeting of the IGF (Internet Governance Forum)[*38] will also cover DID-related technology and encompass discussion of governance. So looking ahead, many people are lining up to drive the discussion forward.

*28 Transforming our world: the 2030 Agenda for Sustainable Development (https://sustainabledevelopment.un.org/post2015/transformingourworld) (https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E).
*29 ID2020 Technical Requirements: V1.0 (https://docs.google.com/document/d/1L0RhDq98xj4ieh5CuN-P3XerK6umKRTPWMS8Ckz6_J8/edit).
*30 W3C Credentials Community Group (https://www.w3.org/community/credentials/).
*31 W3C Verifiable Claims Working Group (https://www.w3.org/2017/vc/WG/) (https://github.com/w3c/verifiable-claims).
*32 Decentralized Identifiers (DIDs) (https://w3c-ccg.github.io/did-spec/#decentralized-identifiers-dids); latest version as of this writing: v0.13, dated Jun. 3, 2019
*33 eth DID Resolver (https://github.com/uport-project/eth-did-resolver).
*34 Verifiable Claims Use Cases (https://www.w3.org/TR/verifiable-claims-use-cases/).
*35 Verifiable Credentials Data Model 1.0 (https://www.w3.org/TR/verifiable-claims-data-model/); latest version: Mar. 2019; a W3C Candidate Recommendation as of this writing.
*36 Rebooting the Web of Trust VIII: Barcelona (March 2019) (https://github.com/WebOfTrustInfo/rwot8-barcelona) (https://www.weboftrust. info/pastevents.html).
*37 IIW (The Internet Identity Workshop) Workshop Proceedings (https://internetidentityworkshop.com/past-workshops/).
*38 IGF 2019 Workshop Selection Results (https://www.intgovforum.org/multilingual/content/igf-2019-workshop-selection-results).

2.5 Other Related Developments

In May 2019, Microsoft unveiled a platform to handle DIDs based on the Bitcoin blockchain. Two blog posts on May 15 describe its future activities in this area[*39][*40]. And it has published a white paper on DID[*41]. From these sources, it is apparent that the W3C DID is being used as the ID space and that the Sidetree protocol developed by the Decentralized Identity Foundation (DIF)[*42] has been adopted. This DID system is implemented on the second layer of the Bitcoin blockchain, and source code has already been released under the name ION (Identity Overlay Network)[*43].

Finally, I will touch on credit scores and information banks. Some media reports claim services that calculate credit scores based on online activity are in the works in Japan as well. A concern is that only scoring done under the auspices of big-brother entities like GAFA and FAANG would be considered accurate, and that your score could be passed around without you intending it. As with AI, another talking point of late, there is a need to ensure transparency of not only the scoring system but the scoring algorithm as well. It is theoretically possible for people to be scored unfairly based on obscure logic because they live in a particular region or on the basis of race, religion, etc. Hence, ethical considerations must be taken into account. The same can be said for the reputation mechanisms of real-world entities, a concern I also noted in relation to ERC-735 claims.

Thus, we now find ourselves in an age in which real-world entities are subject to being evaluated by various means. From a management perspective, these measures may be necessary to ensure security, yet we still need a way to enable individuals to manage their own sensitive information based on the SSI concept. In particular, although it may not be easy to ask identity holders who have been issued a DID or claim for the first time to protect themselves in the ways required, I think the ability to do this really is part of the basic literacy we all need as denizens of the digital age.

Some people have a desire to pass their social media accounts to their children or grandchildren after they die, but this is becoming less and less advisable from a business

*39 Microsoft Security Blog, "Decentralized identity and the path to digital privacy" (https://www.microsoft.com/security/blog/2019/05/15/decentralized-identity-digital-privacy/).

*40 Azure Active Directory Identity Blog, "Toward scalable decentralized identifier systems" (https://techcommunity.microsoft.com/t5/AzureActive-Directory-Identity/Toward-scalable-decentralized-identifier-systems/ba-p/560168).

*41 Microsoft Whitepaper, Decentralized Identity—Own and control your identity (https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY).

*42 Decentralized Identity Foundation (DIF) (https://identity.foundation/) (https://github.com/decentralized-identity/).

*43 ION (Identity Overlay Network) (https://github.com/decentralized-identity/ion/).

continuity perspective. With the advance of AI, it seems, the temporary or permanent deactivation of accounts as an act of censorship against posted content is having a major impact. I think these sorts of "everyday" examples are also a factor behind the rising call for services based on DID and related technologies.

At present, I think a lot remains to be discussed in regard to how we treat temporary IDs when it comes to handling massive quantities of statistical information and with respect to cases in which credentials themselves are encrypted as part of access control. A technology does not necessarily gain traction just because the background technologies are compatible and it would have social applicability if deployed adroitly, and I have seen this many times over the years. At this juncture, it is uncertain whether the technologies I have discussed here will be deployed in applications users identify with and be of any use to the world.

With the advent of real use cases such as information banks, people have come to realize the convenience provided by mechanisms for the Internet-based distribution of information (including sensitive information) linked to real-world entities. But we face a large problem here. Privacy regulations like the EU's GDPR are not unique to the EU sphere. Countries around the world, including Japan, are also subject to such regulations. Hence, because the technologies discussed here use blockchain and the circulation of credentials is thus not limited to within any one region, use of such technologies could face restrictions according to the range of regulations that countries around the world have in place. This is a far cry from the thinking behind cryptoassets such as Bitcoin and Ethereum, and could be a major factor impeding the penetration of such technologies. The ERC-725 Alliance and ID2020 will need to undertake activities to dispel these impediments to cross-country distribution mechanisms. At present, though, no such activities appear to be underway. We need experts that can offer deep insights and broad perspectives to address these issues, including the issue of whether such problems should be dealt with by these consortiums in the first place.

Yuji Suga

Senior Engineer, Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IIJ. Dr. Suga has been in his current position since July 2008. He is engaged in investigation and research activities related to cryptography and information security as a whole. He heads up the CRYPTREC Operational Guidelines Working Group on TLS Configuration and is a member of the CRYPTREC Cryptographic Technology Promotion Committee. He also serves as secretariat of the Cryptographic protocol Evaluation toward Long-Lived Outstanding Security Consortium (CELLOS); secretary of the Information Processing Society of Japan's Computer Security Group (CSEC); assistant secretary of the ISEC Technical Committee of the Institute of Electronics, Information and Communication Engineers (IEICE); CyberSciTech2019 program co-chair; organizing committee member for IWSEC2019; and member of the Cryptoassets Governance Task Force (CGTF) Security Working Group.

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.

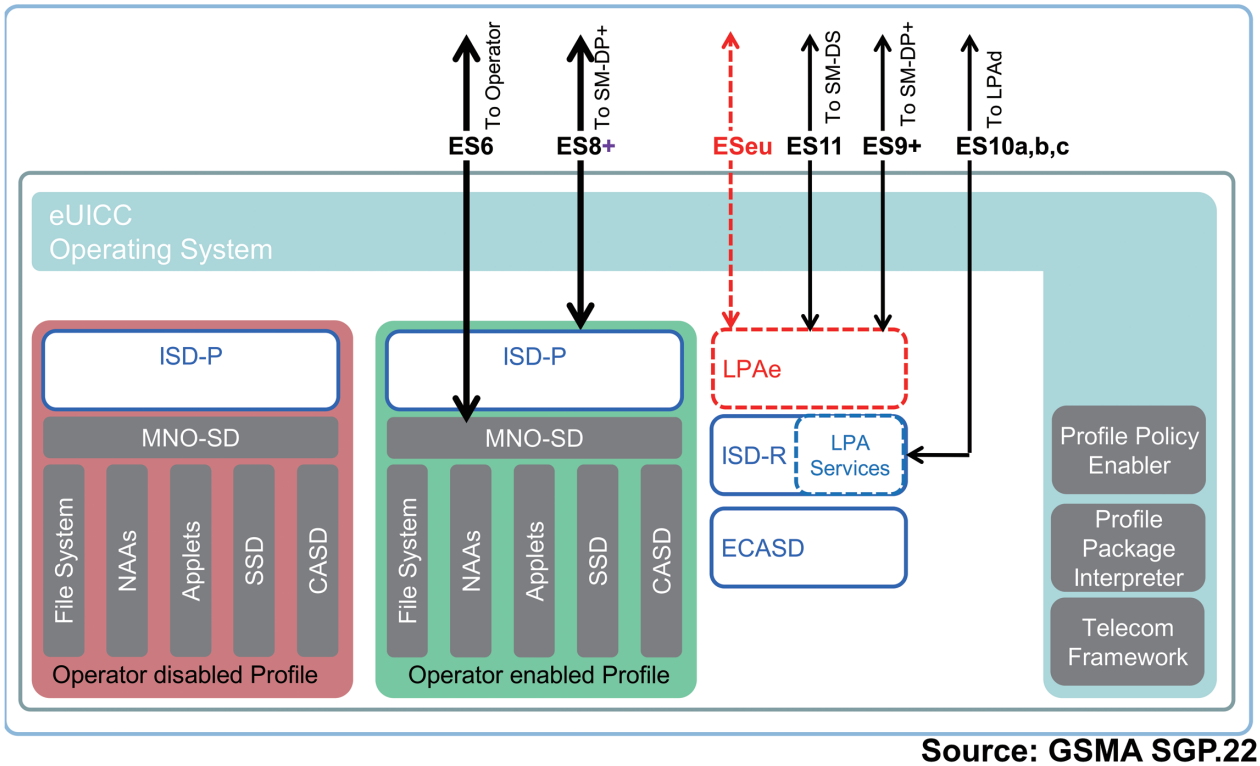


Figure 1: Internal Structure of an eSIM

*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.

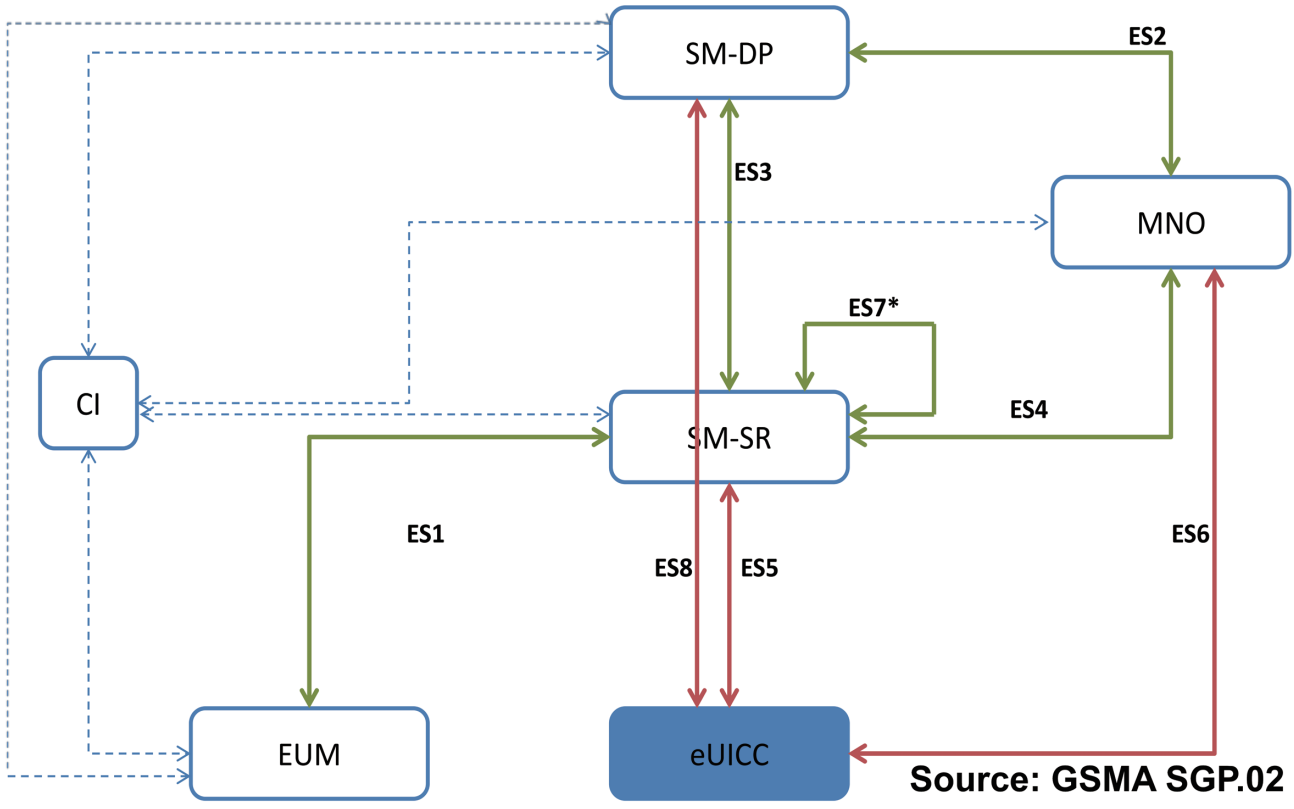


Figure 2: The M2M Model Interface

*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

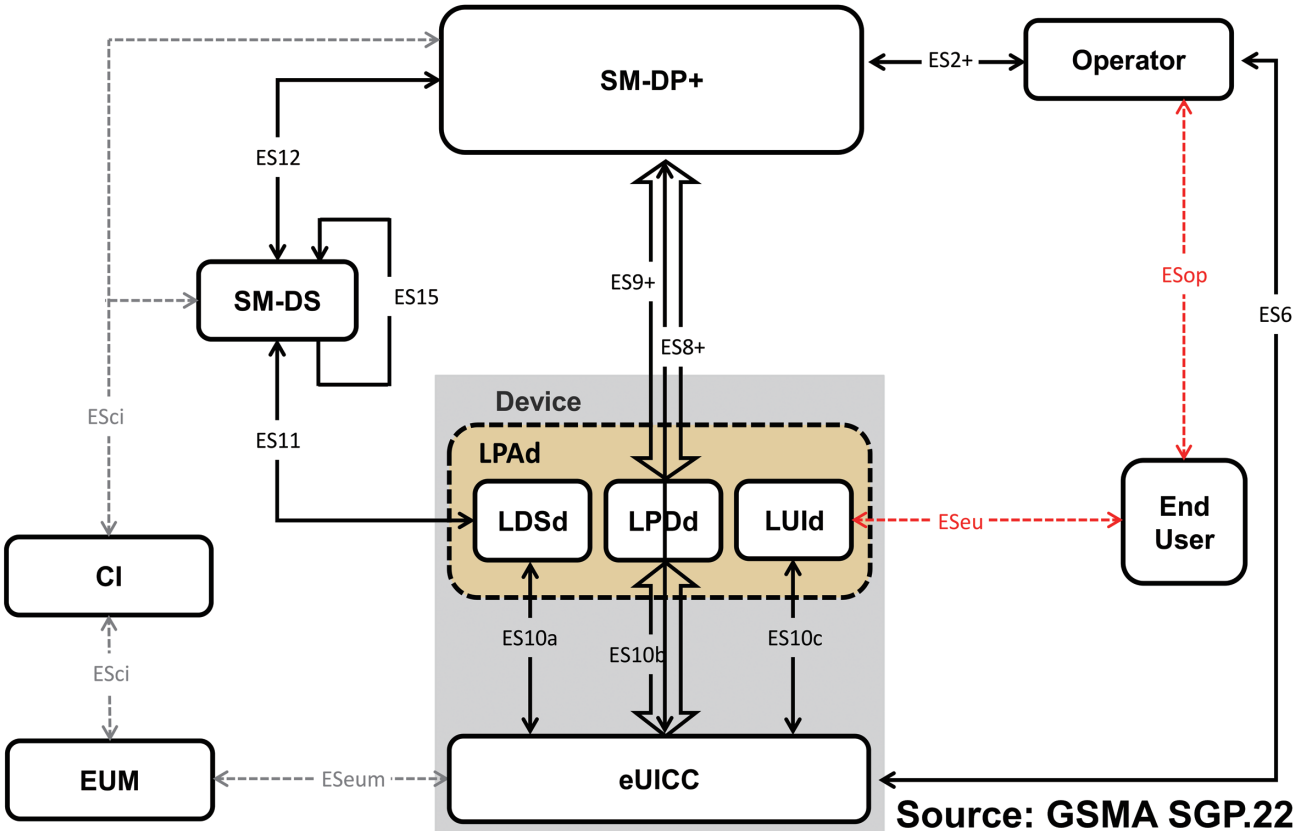


Figure 3: The Consumer Model Interface

*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

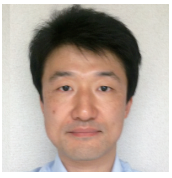
Last year, we carried out PoC testing based on the Consumer model as part of our efforts to get eSIM services off the ground. In the PoC, we installed the our full MVNO profile in a Microsoft Surface Pro LTE Advanced and accessed to the Internet with the profile successfully. We are also testing the 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

September 2019 Vol.43

Internet Initiative Japan

About Internet Initiative Japan Inc. (IIJ)

IIJ was established in 1992, mainly by a group of engineers who had been involved in research and development activities related to the Internet, under the concept of promoting the widespread use of the Internet in Japan.
IIJ currently operates one of the largest Internet backbones in Japan, manages Internet infrastructures, and provides comprehensive high-quality system environments (including Internet access, systems integration, and outsourcing services, etc.) to high-end business users including the government and other public offices and financial institutions.
In addition, IIJ actively shares knowledge accumulated through service development and Internet backbone operation, and is making efforts to expand the Internet used as a social infrastructure.

IIJ-MKTG020-0041

Internet Initiative Japan Inc.

Address: Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku,
Tokyo 102-0071, Japan
Email: info@iij.ad.jp URL: https://www.iij.ad.jp/en/