SIM BLE Authentication

Technology Reports

Portable SIM: Empowering the User in the IoT Era

The recent widespread use of smartphones is driving the rapid development of new services that use smartphone applications to enhance the user experience. At the same time, the development of devices towards the post-smartphone is accelerating with systems and services that use those devices. NTT DOCOMO has developed a novel SIM-based authentication mini device called Portable SIM that physically separates the SIM function from the smartphone. In this article, we explain the basic configuration and operation of Portable SIM and describe the new ecosystem that Portable SIM will help to create.

Communication Device Development Department
Akira Shibutani
Kazuma Nachi
Yuta Higuchi
Takashi Okada

1. Introduction

Smartphones are becoming increasingly popular and the development of next-generation (post-smartphone) devices is already underway. Amid this trend, wearable devices such as watch-type, glasses-type, and healthcare-related smart devices are already becoming popular and most of them can be linked to smartphones. If this trend continues, multi-device usage in which an individual uses a full range of multiple devices including wearable devices will become a reality.

In addition, the concept of seamlessly connecting various kinds of devices such as sensors, smart meters, and automobiles on the Internet, i.e., the Internet of Things (IoT), has been proposed [1], and many kinds of IoT devices are now being developed. We can expect an explosive increase in communication devices of diverse types.

On the other hand, the market for mobile IT services such as social networking services (SNS), online shopping, electronic payment services, and content viewing has been growing in much the same way as the use of smartphones. In these services, the ID and password has been used as an essential means of identifying the user. However, the risk of leaking such information is becoming greater as these services come to handle highly confidential information such as payments, and the wide variety of services available to users means that they have to manage a large number of IDs. A more secure and straightforward ID management method is therefore needed.

Against this background, we reevaluated the concept of the post-smartphone. What we found was that the recent evolution of mobile phones has been focused on an "all in one" concept in which a large number of functions can be sequentially added as needed to a smartphone to encourage the user to use a variety of services. To realize the post-smartphone era in which various types of devices

are used, we concluded that enabling the user to connect to diverse services regardless of device type (in a multi-device environment) will be of more importance.

Based on this conclusion, we reassess the functions of current smartphones. First, for example, the User Interface (UI) and the cellular-network access function, which are the core functions of the smartphone, are not always needed for the post-smartphone era. In other words, the user identification function as can be achieved by a Subscriber Identity Module (SIM)*1 is essential and all other functions can be activated within a device as needed by the user. In short, this means an authentication mini device with SIM is one solution for multi-device usage in the post-smartphone era.

Based on the above idea, NTT DOCOMO has developed a SIM-based authentication mini device called Portable SIM that physically separates the SIM function from smartphone (**Figure 1**). In this article, we present the hardware configuration of Portable SIM and the software configuration on the smartphone side and describe the basic operation of this novel device. We also introduce the new ecosystem that Portable SIM will help to create.

2. Configuration of Portable SIM

An external view and main specifications of a Portable SIM prototype are shown in **Photo 1** and **Table 1**, respectively.

To realize the Portable SIM, it was necessary to add wireless communication functions since a SIM card itself does not have them. Furthermore, to achieve a pocketsize mini device with a smaller battery, low power consumption was essential. Ease of connection with a variety of communication devices also had to be considered. With these requirements in mind, we selected Bluetooth®*2 for connecting Portable SIM with diverse communication devices, and in particular, Bluetooth v4.0 (commonly known as Bluetooth Low Energy = BLE), which enables low power consumption. We also mounted Near Field Communication (NFC)*3 functions in Portable SIM to simplify ID management and

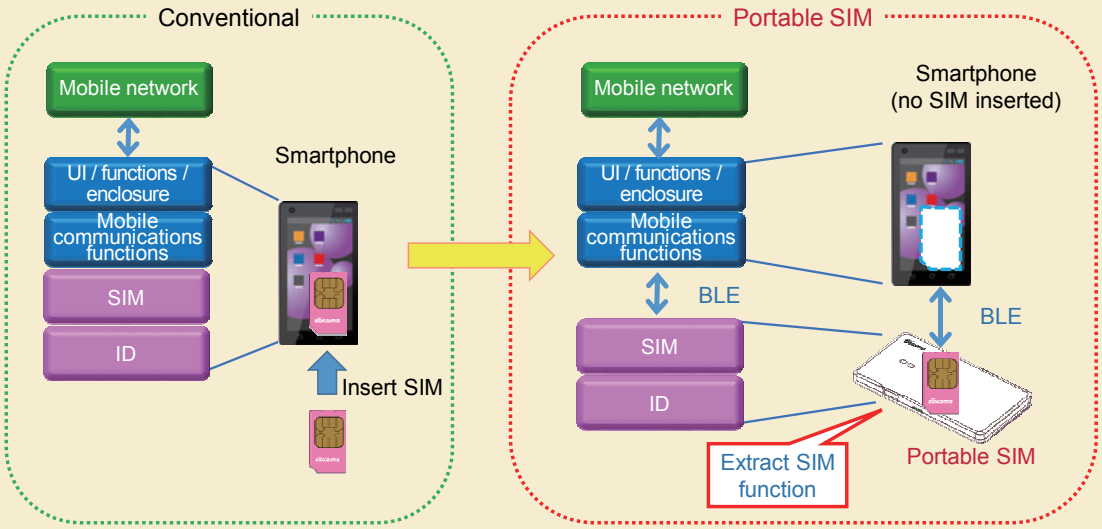

Figure 1 Concept of Portable SIM

*1 **SIM:** A smart card that stores subscriber information associated with a mobile phone.

*2 **Bluetooth®:** A short-range wireless communication standard for interconnecting mobile terminals such as mobile phones and notebook computers. A registered trademark of Bluetooth SIG Inc. in the United States.

*3 **NFC:** A short-range wireless communications standard using the 13.56 MHz band and initiated by NXP Semiconductors Inc. and Sony Corp. Provides unified support for FeliCa, Mifare, Type A/B (ISO14443), and IC tags (ISO/IEC 15693).

the establishment of a BLE connection (**Figure 2**).

When connecting SIM with an external device, a high-reliability protocol is essential to exchange SIM information in a secure manner. Bluetooth features SIM Access Profile (SAP) as a protocol that meets this requirement [2]. However, differences between the Bluetooth and BLE specifications prevent SAP from being directly applied to BLE, so we developed a new profile*4 to apply to BLE (SAP on BLE) following SAP policy.

SAP on BLE is essentially SAP constructed on BLE, which involved the one-to-one redefinition of Bluetooth commands as BLE commands. Moreover, as BLE itself is not capable of transmitting a response after the server has completed processing of a request received from the client, response processing was achieved by allocating the appropriate commands on BLE. In addition, while the encryption method used by SAP is Triple Data Encryption Standard (3DES), SAP on BLE achieves encrypted communications through Advanced Encryption Standard (AES)*5 defined on BLE.

The software configuration on the smartphone side to support Portable SIM is shown in **Figure 3**. On the smartphone side, it must be possible to exchange SIM information to the modem via BLE. The need for ensuring the security of this information given the presence of other applications on the smartphone and for facilitating the addition of functions for creating new services must also be considered. In light of the above, this software configuration places the SAP on BLE smartphone-side software (Application for Portable SIM) on the Java layer and connects with the modem via daemon software on the native layer (Daemon for Modem Comm.). As a result, those sections dependent on the modem and OS can be absorbed by daemon software, which means that support can be easily provided for a variety of communication devices without having to make extensive changes to SAP on BLE. Finally, SIM has been removed from the smartphone and connection from the outside has been achieved by

Photo 1 External view of Portable SIM prototype

Table 1 Main specifications of Portable SIM prototype

Dimensions (height × width × thickness: mm)	approx. 80 × 40 × 5.6
Weight	approx. 20 g
Communications method	NFC/Bluetooth (4.0)
Power method	USB charging

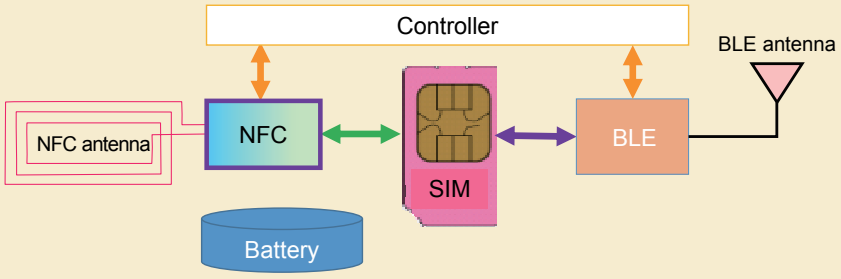

Figure 2 Hardware configuration of Portable SIM

*4 **Profile:** Inter-device protocol formulated on a service-by-service basis for use in communications by Bluetooth and Bluetooth Low Energy.

*5 **AES:** A symmetric key encryption method that has been adopted as a new encryption standard by the U.S.A. One of the cryptosystems used in 3GPP.

assigning Portable SIM the peripheral*6 role and the smartphone the central*7 role in SAP on BLE.

3. Basic Operation of Portable SIM

Basic operation of Portable SIM when using a service in conjunction with a communication device such as a smartphone is described below (**Figure 4**).

(1) Establish BLE link

The Portable SIM and the communication device exchange the information needed to establish a BLE link and then proceed to establish the link. This prototype uses NFC technology to exchange the information needed for a BLE link thereby enabling a connection to be established by a simple and intuitive "wave" operation.

(2) Connection by SAP on BLE

After the BLE link has been established, the SIM in the Portable SIM and the communication device connect using SAP on BLE. At this time, Portable SIM transmits the information for connecting a mobile network to the communication device (modem). The communication device then performs the same processing as if SIM was a built-in component.

(3) Use of SE area

The information stored in the SIM's Secure Element (SE)*8 can be exchanged through an NFC-based touch operation. Once the BLE link is established, the information is exchanged using the SAP on BLE profile.

The above basic operations of Portable SIM can be combined to enhance the user experience when using multiple devices, sharing devices, and performing ID authentication. We describe these three usage scenarios below (**Figure 5**).

- Multi-device

Connecting Portable SIM to a tablet enables mobile-phone functions to be activated with the mobile phone number of that Portable SIM. Then, after the same Portable SIM connects to the user's smartphone, the functions of the smartphone can be activated with the same number that the user used with the tablet. At this time, the tablet becomes deactivated.

In other words, the user can easily select a tablet with a large screen while at home and a smartphone that is easy to carry around while com-

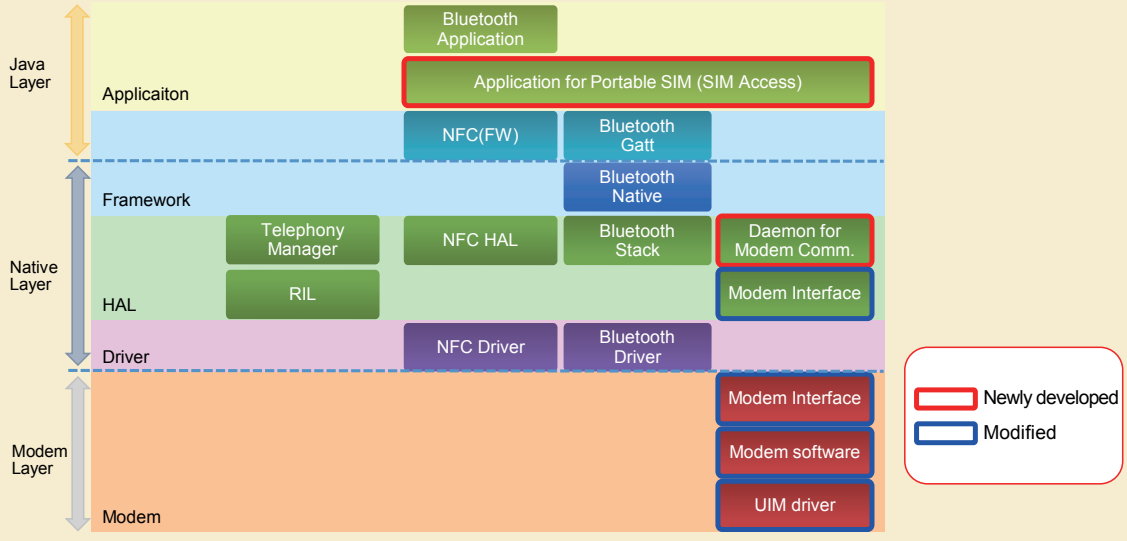

Figure 3 Software configuration of smartphone supporting Portable SIM

*6 **Peripheral:** The role of a device in Bluetooth Low Energy communication, which divides roles into "central" (see *7) and "peripheral." The central device detects and controls the peripheral device.

*7 **Central:** The role of a device in Bluetooth Low Energy communication, which divides roles into "central" and "peripheral" (see *6). The central device detects and controls the peripheral device.

*8 **SE:** An area for securely storing encrypted keys and other types of confidential information.

muting.

- Device sharing

A user can possess multiple Portable SIM devices for use with a single communication device and can easily use one or the other depending on the use case by simply switching connections.

For example, a user could possess two Portable SIM units—one for private use and one for business use—and then use the same smartphone

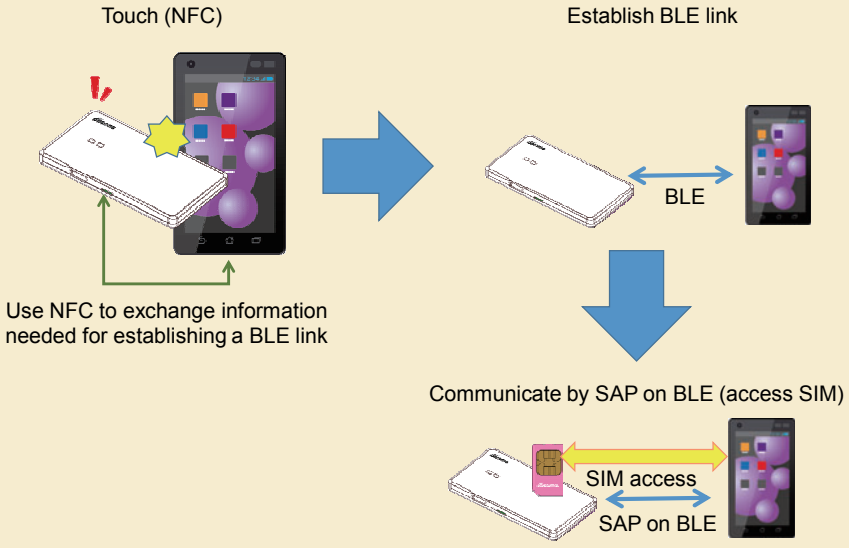

Figure 4 Portable SIM usage scheme

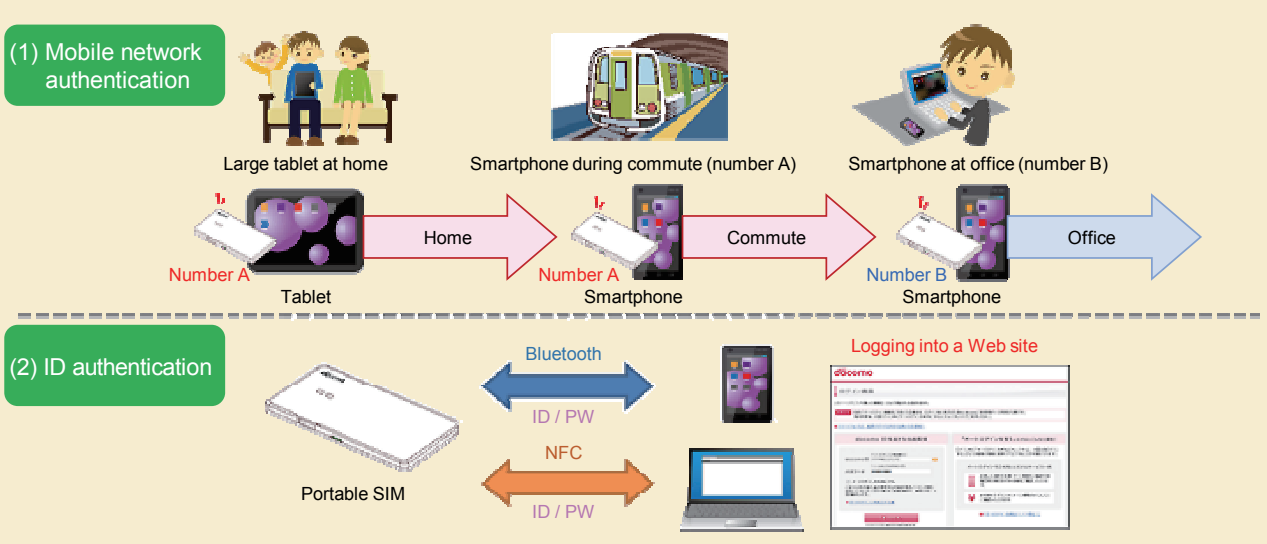

Figure 5 Portable SIM usage scenarios

for either private or business matters. The same idea could be applied to the case in which a family shares a single tablet: different members of the family could use separate Portable SIM units enabling the tablet to be used under settings tailored to each user.

In other words, if Mobile Device Management (MDM) functions were to be linked to phone numbers, it would be possible, for example, to suppress the execution of the camera function or apps when using the Portable SIM for business purposes or to activate parental controls*9 in the case of a family tablet when using the Portable SIM set for children.

- ID authentication

Storing regularly used service authentication information (Web site address, ID/password, etc.) in the SE area of an SIM card simplifies the use of the same service authentication information when going back and forth among various communication devices in a multi-device environment or when using IoT devices.

4. New Ecosystem Enabled by Portable SIM

With Portable SIM, the user can easily switch phone numbers and settings while keeping service authentication information with them. Thus, Portable SIM enables the creation of an environment in which users can carry around their phone numbers and service authentication information. The following describes a new ecosystem enabled by Portable SIM (**Figure 6**).

1) Flexible Combinations of People and devices

A direct value provided by Portable SIM is the ability to "carry around one's (user-specific) phone number and ID." However, looking forward to the IoT world that is predicted to grow in the years to come, there will be many occasions when the user will want to connect

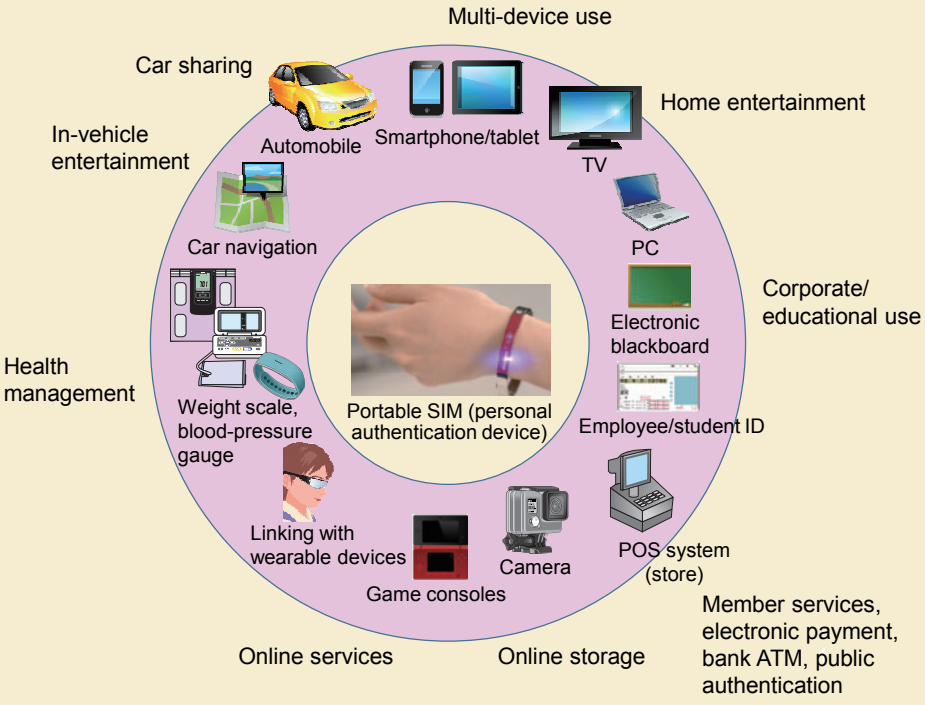

Figure 6 New ecosystem enabled by Portable SIM

*9 **Parental controls:** Functions that enable parents to control how their children use devices such as smartphones and PCs.

to a network (Internet, cellular net, etc.) through devices (such as smartphones and other devices having communication functions), and at these occasions, identifying the user to provide desired services will be extremely important. If we therefore consider what value Portable SIM can provide in an IoT world, we can say, first, from the viewpoint of devices, that it will be able to make all kinds of devices into a network entry point by separating devices and the mobile network (billing contracts) thereby eliminating the need to be concerned about the latter. At the same time, from the viewpoint of users, Portable SIM will make it easy to access desired services from network entry points that will exist at many and varied locations throughout this ecosystem. In short, as shown in **Figure 7**, Portable SIM will make it easy to identify the service user, and this, in turn, will facilitate the creation of a new ecosystem with flexible combinations of user and devices without the user having to own those devices. In contrast, a mobile network (billing contract) and user have conventionally been fixed to a device. This flexibility should lead to the creation of new value that we can call "from ownership to use."

Taking, for example, a user of health services, we can envision a service that enables the user to obtain data from nearby health-related devices through intuitive operations made possible by Portable SIM, even if using those devices for the first time. This service could also guide the user toward appropriate health services based on the data obtained. Additionally, in the case of automobiles, Portable SIM will make it possible to quickly identify the user entering the vehicle so that services tailored to the user can be provided in a seamless manner. For example, travel plans (routes, desired destinations, etc.) that have been previously prepared by the user on the

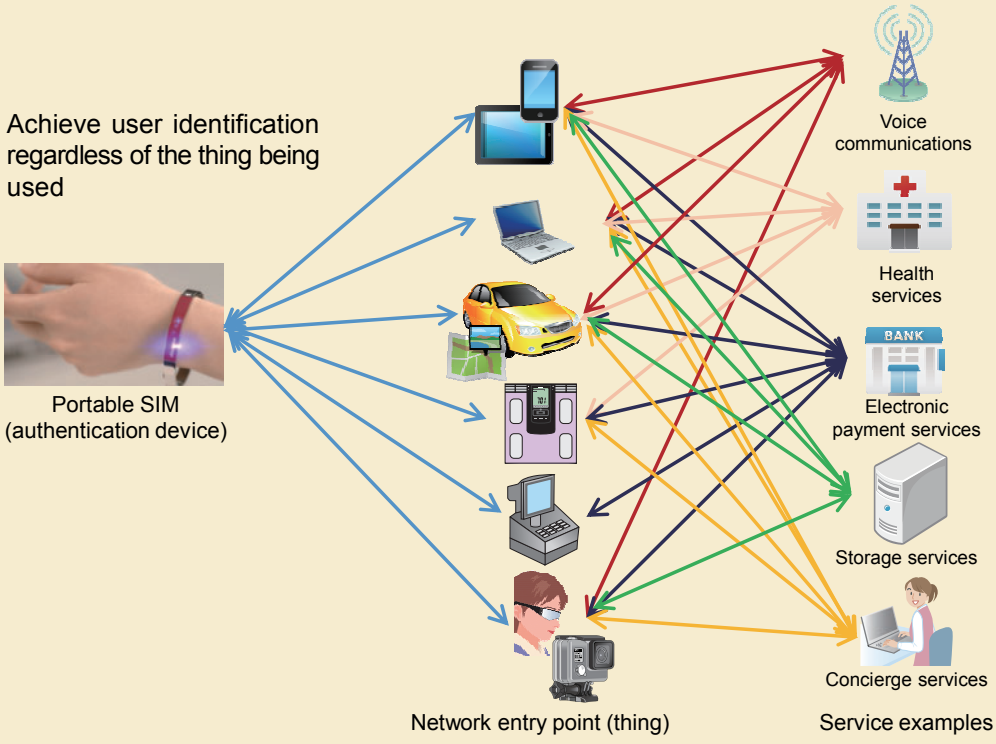

Figure 7 Flexible combinations of people and things

cloud could be set in the car navigation system and in-vehicle entertainment devices could be linked to the user's favorite music, content, etc.

2) Provision of Secure and Open Authentication functions

Up to now, SIM has been used as a component built into a smartphone. However, with the development of this new functional device called Portable SIM, the functions that SIM has conventionally been equipped with can now be used through Portable SIM alone. This is the second direct value that Portable SIM can provide, as shown in **Figure 8**.

SIM has PIN authentication and a remote lock [4] function for use when a handset is lost. Authentication functions can similarly be disabled when a Portable SIM (device) is lost likewise through remote locking.

In addition, Portable SIM has a built-in mechanism for adding an applet*10 [4] to SE from a service issuing/management system [3] called Trusted Service Manager (TSM). An applet stored in SE can be programmed based on JavaCard™*11 specifications [4], making it easy to add ID/password management functions and authentication functions for member ID cards, electronic locks, basic resident registration cards, etc. In this way, applets stored in Portable SIM can be used to perform personal authentication for connecting to a variety of services. This mechanism is advantageous for service providers since it enables them to construct a proprietary authentication platform for specific services without having to use devices such as cards that have been traditionally distributed for personal authentication. It is also advantageous for users since it consolidates authentication functions for diverse services while ensuring safety and eliminates the complexity of ID/password management. In addition, these advantages can be integrated to fortify

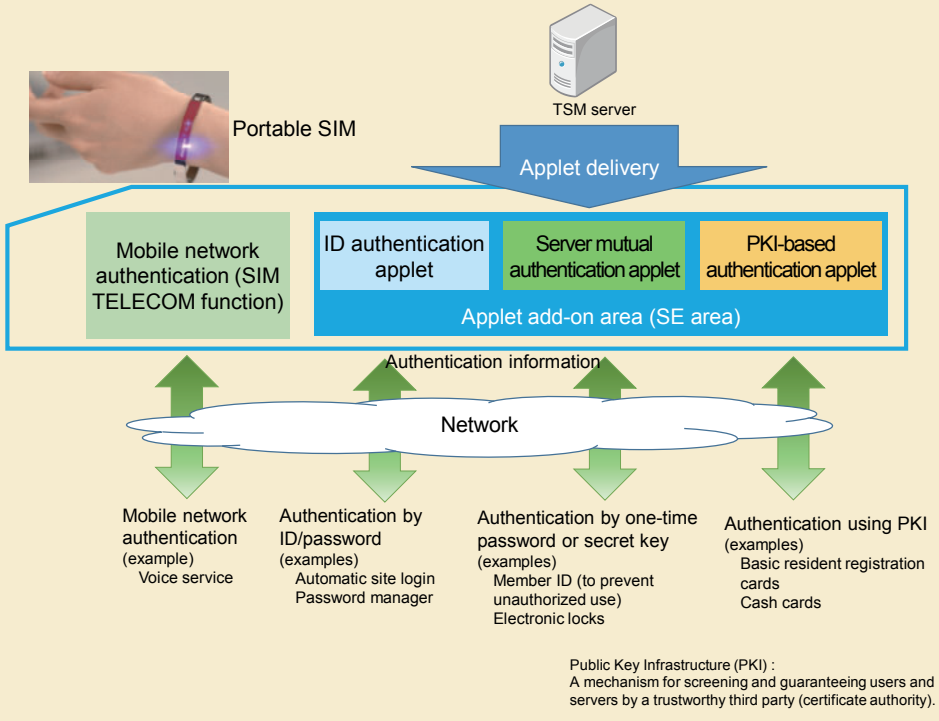

Figure 8 Authentication using Portable SIM

*10 **Applet:** A JavaCard™ (see *11) application running on SIM.

*11 **JavaCard™:** A Java execution environment operating on a device having limited memory and processing ability such as smart cards including SIM. Java is a registered trademark of Oracle Corporation and/or its subsidiaries and affiliates in the United States and other countries.

coordination between services, which assumes a secure authentication platform. We expect such secure inter-service linking to enable the creation of new services.

For example, such authentication functions could be combined with mobile network authentication to automate applet management (add, delete, etc.) so that passwords and signature information held by individual authentication functions can be automatically updated without bothering the user. Additionally, the consolidation of authentication functions should simplify the linking of content payment functions between different service providers and facilitate the mutual use of points and priviledge. Furthermore, in the health and medical care fields, Portable SIM authentication functions could be linked with personal information such as medical records that needs to be securely managed between hospitals. We expect such linking to enhance the user experience in using services.

In the above ways, Portable SIM can increase the number of network entry points, provide flexible combinations of users, devices, and services, and achieve diverse authentication functions tailored to different types of services. Integrating these capabilities in the form of Portable SIM can enhance the value of cloud services and provide new value to users.

5. Conclusion

In this article, we presented a prototype of the Portable SIM authentication mini device with the aim of creating new services. We explained the background leading up to its development, the technology needed to realize it, and its basic operation. We also described a new ecosystem enabled by Portable SIM through the creation of novel and attractive services.

Looking to the future, our plan is to miniaturize the Portable SIM device with an enhanced user experience toward commercialization and to accelerate system development toward the provision of diverse services enabled by Portable SIM.

References

[1] Kevin Ashton: "That 'Internet of Things' Thing," RFID Journal, Jun. 2009. http://www.rfidjournal.com/articles/view?4986

[2] Bluetooth SIG, Inc.: "SIM ACCESS PROFILE Interoperability Specification v1.1," Dec. 2008.

[3] T. Sugano et al.: "Advances with Osaifu-Keitai – Starting Services Supporting NFC (Type A/B) on NTT DOCOMO UIM Cards–," NTT DOCOMO Technical Journal, Vol. 15, No. 1, pp. 22-28, Jul. 2013.

[4] T. Akiyama et al.: "Technologies for Further Evolution of Osaifu-Keitai Service–NFC-enabled Mobile Terminals and NTT DOCOMO UIM Card–," NTT DOCOMO Technical Journal, Vol. 15, No. 1, pp. 13-21, Jul. 2013.