NFC UIM FeliCa

Technology Reports

Technologies for Further Evolution of Osaifu-Keitai Service —NFC-enabled Mobile Terminals and NTT DOCOMO UIM Card—

*The use of NFC Type A/B services is expanding in Japan and throughout the world. To achieve a mutually beneficial relationship between these services and its pioneering FeliCa®[*1] service having similar functions, NTT DOCOMO recognized that NFC international specifications should be incorporated in the development of new mobile terminals while making good use of the features and convenience of existing Osaifu-Keitai functions. To this end, we have developed a new mobile terminal configuration supporting NFC Type A/B specifications including a UIM and commercialized this new configuration in fiscal year 2012. This article describes platform technologies for this new mobile terminal configuration supporting NFC services and a UIM.*

Communication Device Development Department

Tomohiro Akiyama
Tetsuhiro Tanno
Tetsuhiro Sasagawa
Kumiko Yamaguchi

1. Introduction

As the application of Near Field Communication (NFC) Type A/B functions expands throughout the world, contactless tags and cards using these functions are becoming a major turning point in the provision of mobile services. In Japan, the Osaifu-Keitai (mobile wallet) service that is already using NTT DOCOMO FeliCa technology has come to be used for a variety of applications including mobile credit cards, train/bus tickets and employee ID cards. The need has grown, however, to make contactless tags and cards compatible with NFC Type A/B functions while maintaining the beneficial features of FeliCa technology. It has also become necessary to study security measures to deal with unauthorized access or theft when equipping smartphones with these functions.

In the winter of fiscal year 2012, NTT DOCOMO began to commercialize NFC-enabled mobile terminals and a User Identity Module (UIM)[*2] incorporating a NFC Type A/B Secure Element (SE)[*3].

In this article, we describe NTT DOCOMO's technical efforts in achieving NFC services from the viewpoint of a new mobile terminal configuration and UIM card.

2. NFC Overview

As the name implies, NFC is a short-range radio communication technology specified as an international standard by the International Organization for Standardization (ISO)[*4] for use as a contactless smart card interface.

*1 **FeliCa®**: A contactless IC card technology developed by Sony Corp. A registered trademark of Sony Corp.

*2 **UIM**: An IC card on which such subscriber information as phone number is stored. It is inserted into a mobile terminal and used for the purpose of user identification. The FOMA card is an example of UIM. The media that stores subscriber information is referred to as UIM in ITU's recommendations of IMT-2000 systems.

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

Near field communication enables two devices to recognize and automatically communicate with each other by simply bringing them to within several centimeters of each other. It is a technology that simplifies the transmission and reception of diverse types of information.

NFC-enabled terminals operate mainly in the following three modes. This article is centered about the card emulation mode.

1) Card Emulation Mode

This mode emulates on a mobile terminal functions typically provided by a plastic card, such as credit-card functions, e-money or train/bus tickets. It therefore enables a mobile terminal user to use functions equivalent to those of a plastic card by simply holding the handset over a Reader/Writer (R/W).

The access method can be broadly divided into two types. One is contactless access from the R/W and the other is access from the mobile terminal to the SE of the UIM such as for checking an account balance. An example of the former method would be a R/W device at a retail store accessing the SE of the UIM via a ContactLess Frontend (CLF)[*5]. This would occur when the user holds the mobile terminal over the R/W to perform some function like settling a transaction. An example of the latter method in addition to the above balance-checking function would be a Trusted Service Manger (TSM)[*6] server accessing the SE of the UIM to perform functions like issuing and charging accounts.

The existing Osaifu-Keitai service can also operate in a card emulation mode so that e-money can be used by holding the mobile terminal over a R/W device and related functions like balance display and account charging from any location can be performed.

2) R/W Mode

This mode enables a mobile terminal to be used as a NFC-enabled R/W terminal. In this mode, holding the mobile terminal over a smartcard or IC tag enables data stored on such digital devices to be referenced or rewritten. To give some examples, R/W mode can be used to access a site via a Smart Poster[*7], check the balance of a prepaid e-money smartcard, or rewrite information on a smartcard.

3) Peer-to-Peer (P2P)[*8] Mode

This mode enables a pair of NFC-enabled mobile terminals or NFC-enabled devices (e.g., personal computers, tablet computers or home appliances equipped with contactless smartcard communication functions) to transfer or exchange data. It can be used to transfer contact data, pictures, etc. as performed by the Android Beam[*9] function.

Table 1 compares Type A/B and FeliCa methods. Though dependent on the bit rate of external R/W terminals, the lower limit of Type A/B and FeliCa bit rates differs by two times. The FeliCa method is said to be applicable to high-speed processing and its use of proprietary commands is also significant.

The relationship between the various short-range radio communication methods is shown in **Figure 1**. Only radio communication methods have been standardized by ISO, and processing systems and commands are significantly different between Type A/B and FeliCa. In Type A/B, commands are specified by ISO7816 and the processing system by GlobalPlatform[*10], for example.

Furthermore, when applying these processing systems and commands to the Osaifu-Keitai service, an SE sup-

Table 1 Comparison of Type A/B and FeliCa methods

	Type A	Type B	FeliCa
Modulation method	ASK 100%	ASK 10%	ASK 10%
Coding	Modified Miller	NRZ	Manchester
Bit rate	106kbps-	106kbps-	212kbps-
Commands	ISO7816	ISO7816	Proprietary
Main applications	Taspo, etc.	Japanese driver's licenses, etc.	JR train passes, etc.

ASK : Amplitude-Shift Keying
NRZ : Non Return to Zero

*4 **ISO**: An organization for standardization in the information technology. Sets international standards for all industrial fields except electrical and telecommunication fields.
*5 **CLF**: A module for performing NFC wireless communication functions.
*6 **TSM**: An operator entrusted by carriers and service providers to act as a primary issuer of card applications for UIM cards.
*7 **Smart Poster**: A type of tag storing browser-related information specified by the NFC Forum (see *21).
*8 **P2P**: A communication model in which computers exchange information on equal footing in contrast to the server-client model. In this article, mobile terminals and surrounding digital devices all exchange information on equal footing.
*9 **Android Beam**: A function for sending and receiving data between smartphones using near field communication.

porting the target specifications is needed. The SE is a secure area with high tamper resistance[*11] for storing data and applications. In FeliCa, the SE is implemented on a chip built into the mobile terminal, while in Type A/B, it is implemented on the UIM. In this development, all communication methods and functions are supported on the mobile terminal and UIM combined.

3. NFC-enabled Mobile Terminal and UIM

3.1 Configuration of NFC-enabled Mobile Terminal

1) Hardware Configuration

The hardware configuration of a NFC-enabled mobile terminal is shown in **Figure 2**. This configuration differs from existing FeliCa-only mobile terminals in two ways: the CLF contactless Radio Frequency (RF) chip that previously supported only FeliCa now supports both FeliCa and Type A/B specifications and a Single Wire Protocol/Host Controller Interface (SWP/HCI) has been added for communicating with UIM.

Equipping the mobile terminal with a built-in, dual-support CLF chip makes it possible to automatically differentiate between FeliCa and Type A/B radio communication methods and to receive signals accordingly. The SWP/HCI, meanwhile, is a communication method standardized by the European Telecommunications Standards Institute (ETSI)[*12]. It enables bidirectional communications to be performed between the UIM and CLF chip over a single physical transmission path (single wire).

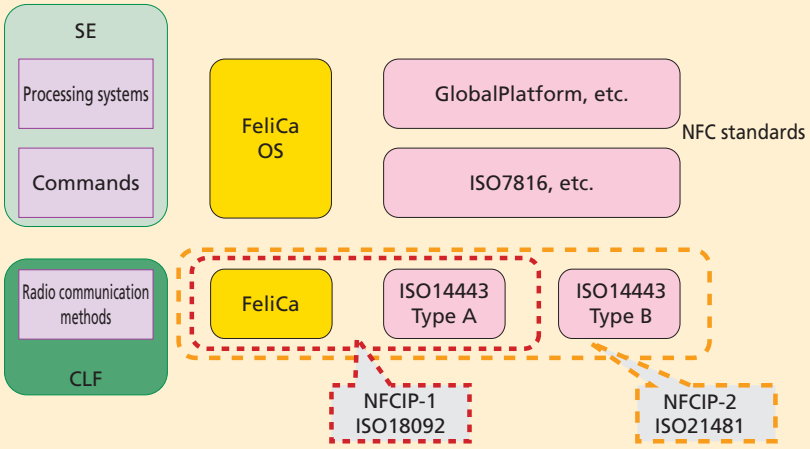

Figure 1 Relationship between short-range radio communication methods

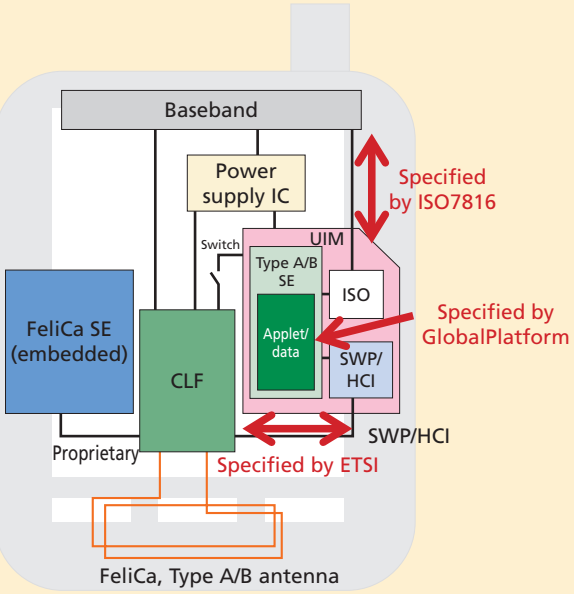

Figure 2 Hardware configuration of NFC-enabled mobile terminal and UIM

2) Software Configuration

The software configuration of a NFC-enabled mobile terminal is shown in **Figure 3**. The Android™[*13] OS layer includes NFC middleware[*14], Open Mobile API and Access Control as

*10 **GlobalPlatform**: Standard specifications of a card platform based on VISA Open Platform specifications and centered about the financial industry.

*11 **Tamper resistance**: A property to prevent integrated programs, data and other digital information from unauthorized referencing or rewriting.

*12 **ETSI**: European Telecommunications Standards Institute. A European standardization body engaged in the standardization of telecommunications technologies. Headquartered in Sophia Antipolis, France.

*13 **Android™**: A trademark or registered trademark of Google, Inc., in the United States.

*14 **Middleware**: Software positioned between the OS and actual applications providing common functions for diverse applications thereby making application development more efficient.

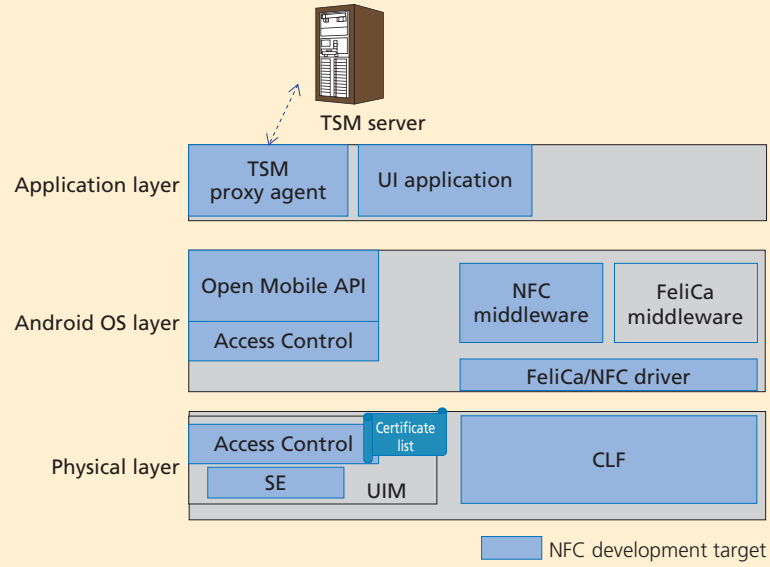

Figure 3 Software configuration of NFC-enabled mobile terminal and UIM

described below. Incidentally, the TSM proxy agent implemented on the application layer is an application that has the task of controlling communications between the UIM and TSM server (see [9] for details).

(1) NFC middleware

Of the three operating modes described above, NFC middleware achieves R/W and P2P. The Android OS is also equipped with a discovery-mode function likewise achieved by NFC middleware. This function transmits a carrier wave under preset conditions such as screen ON to automatically detect tags or another mobile terminal.

(2) Open Mobile API

The Open Mobile API provides access to the UIM. Since Android OS provides no general-purpose API for accessing the UIM, this layer is equipped with an API standardized by SIMalliance [1]. Using open source software to achieve this API reduced our development load. This API specifies as few common specifications as possible to facilitate the provision of content (NFC applet[*15]) by a service provider.

(3) Access Control

Access Control is an application that controls access to the UIM. It is assumed that this UIM will be storing a credit card application as well as many other applications and various types of information and that such data must be stored in a secure manner. It is important that the user be reassured that personal data are secure by appropriately controlling access to the UIM from the mobile terminal. Nevertheless, there is always concern that an attack could be mounted from a malicious application through the preparation of an API capable of accessing the UIM, and to defend against such an attack, the Access Control function standardized by the Global System for Mobile communications Association (GSMA)[*16] [2] controls UIM access. Here, each UI application[*17] is associated with a signature[*18] in the form of a certificate (HASH value[*19]), and a list of these certificates is stored in the UIM. The function controls UIM access on the mobile terminal by comparing this list with the HASH value owned by a UI application attempting to access the UIM.

To give an example, we consider a user using a service provided by UI application A on the mobile terminal. In response to a user operation on the mobile terminal, the TSM proxy agent receives an install request from UI application A and sends a service-issue request to the TSM server. On receiving this request, the TSM server downloads NFC applet A from the server onto the mobile terminal and installs it. The TSM server also issues a UI-application-A certificate (HASH value) at this time. On receiving these items, the TSM proxy agent saves the certificate (HASH value)

*15 **NFC applet**: An applet loaded on the UIM to provide a NFC service.
*16 **GSMA**: World's largest industry association in the mobile communications domain.
*17 **UI application**: An application operating on the mobile terminal to provide a user interface; specifically, a Java application on an Android terminal.
*18 **Signature**: A digital signature required when distributing Android applications, certifying the developer of the application.
*19 **HASH value**: The value computed by a HASH function.

linked with NFC applet A on the certificate list within the UIM via Access Control and installs NFC applet A in SE on the UIM (**Figure 4**).

Then, whenever UI application A issues an access request to NFC applet A on the UIM, Access Control on the mobile terminal will request the certificate (HASH value) linked with NFC applet A, which is stored on the UIM certificate list. This certificate (HASH value) linked with NFC applet A can now be compared with the HASH value of the certificate owned by UI application A. If they match, UI application A will be allowed access to NFC applet A within the UIM (**Figure 5**). Conversely, failure to achieve a match will generate an error (**Figure 6**). This scheme prevents unauthorized UIM access from applications.

3.2 Configuration of NFC-enabled UIM (NTT DOCOMO UIM Card)

This UIM features two interfaces: an ISO7816 interface for connecting to the mobile terminal's baseband[*20] and a SWP/HCI interface for connecting to the mobile terminal's CLF (Fig. 2). The former is used for sending and receiving commands to and from the mobile terminal for performing 3G or LTE communications, location registration, etc., and also for sending and receiving GlobalPlatform-compatible commands, which is one objective of this development. The latter, meanwhile, is used for sending and receiving commands to and from a contactless R/W via CLF.

The UIM incorporates a SE for storing a variety of applications and data that realize the features specified by the GlobalPlatform standard.

4. NFC Features

4.1 Functions Conforming to NFC Standards

1) NFC Forum[*21]

Of the three operating modes described earlier, the NFC Forum [3] deals mostly with the standardization of the R/W and P2P modes, specifying, for example, types of tags, operations to perform on detecting tags and protocol for achieving P2P. The mobile terminal configuration introduced in this article

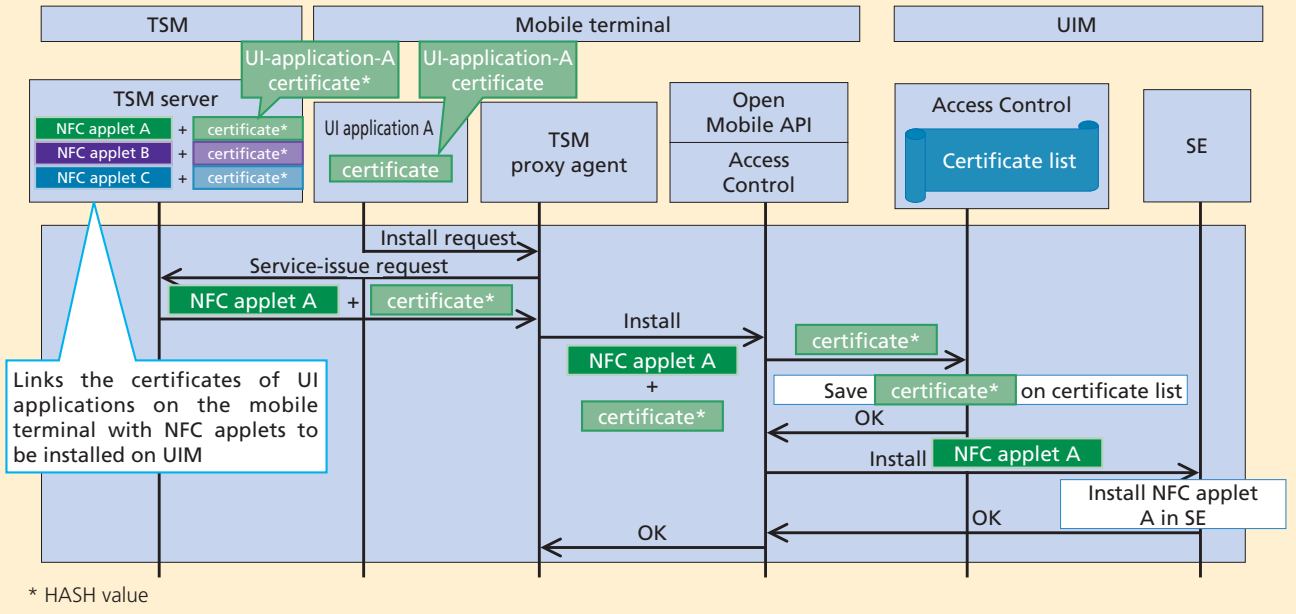

Figure 4 Sequence flow of Access Control function(install NFC applet in SE)

*20 **Baseband**: The circuits or functional blocks that perform digital signal processing.

*21 **NFC Forum**: An industry association whose activities include the promotion of short-range radio communications and the drafting of technical specifications.

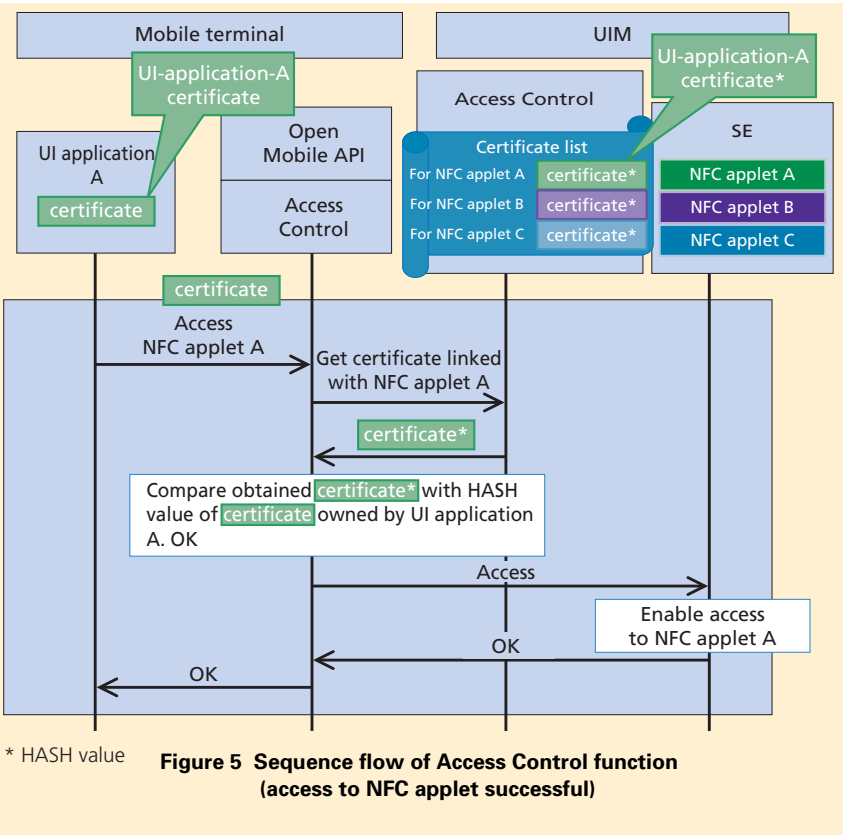

Figure 5 Sequence flow of Access Control function (access to NFC applet successful)

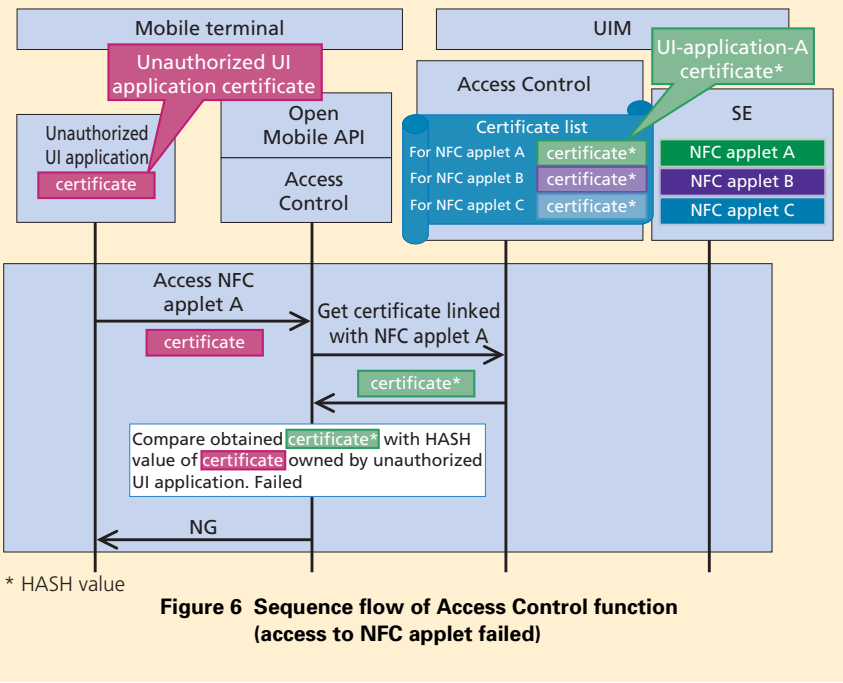

Figure 6 Sequence flow of Access Control function (access to NFC applet failed)

supports these specifications. Given that inexpensive NFC tags are expected to proliferate in the years to come, the application of NFC-enabled mobile terminals should become quite diversified starting with the dissemination of content in the vicinity of the user through the use of tag-equipped Smart Posters and expanding to information gathering and real-world interaction.

2) GlobalPlatform

GlobalPlatform specifications have been based from the start on VISA OPEN Platform specifications for credit cards established by VISA International. Of these, the GlobalPlatform Card Specification [4] is a publically released specification prescribing security mechanisms and commands for various tasks such as install/delete card content in conformance with Java Card™*22 and other standards. This specification is widely referenced for card applications in the financial industry. In addition to this specification, there is also GlobalPlatform Universal Integrated Circuit Card (UICC) Configuration [5], which specifies more detailed parameters envisioning the use of UIMs in a mobile environment, and GlobalPlatform Card Contactless Services Card Specification Amendment C [6], which envisions access of contactless service content on a card from a contactless R/W terminal as well as status updating and screen display of that content. The UIM introduced in this article supports

*22 **Java Card™**: A platform for smart cards developed by Sun Microsystems, Inc. (now a part of Oracle Corp.). A trademark of Oracle Corp.

all of the above specifications.

By adopting a design that conforms to these technical specifications, we have achieved a function for remotely installing applications from a TSM into the secure area on the UIM and a function for accessing a UIM application from a contactless R/W via CLF.

3) ETSI

The ETSI prescribes specifications for the SWP/HCI interface handling communications between the UIM and CLF. This UIM conforms to those specifications. The reference technical specifications in [7] and [8] pertain to SWP and HCI, respectively.

By adopting a design that conforms to these technical specifications, we have achieved a contactless communication interface for performing communications with the UIM via CLF.

4.2 NFC Extended Functions

1) Lock Functions

Lock functions have been achieved even in FeliCa handsets for the sake of safety and security. These functions are of two types: a local lock purposely applied by the user and a remote lock that becomes necessary in specific situations such as when a handset is lost. Our development of NFC Type A/B includes similar functions.

However, it may be possible for a UIM supporting NFC Type A/B specifications to be inserted into or removed from a NFC-enabled mobile terminal while storing applications such as a transaction-settlement service. This calls for functions that can lock NFC Type A/B functions on the UIM independent of the mobile terminal's lock functions.

Our UIM achieves lock-state management independent of the mobile terminal. Furthermore, to enhance compatibility with existing FeliCa functions, this UIM implementation makes the two types of lock functions—remote lock and local lock—independent of each other.

At the same time, incorporating lock functions in the UIM can make lock-state control complicated. It must also be considered that lock passwords for FeliCa and UIM may be different. To provide operations that do not confuse the user, we have established fixed patterns governing the locking and releasing of FeliCa and UIM. As shown in **Table 2**, only a release operation can be performed if either FeliCa or UIM are locked thereby preventing complicated lock/release scenarios.

2) Access Control Application

As described in section 3.1, the installation of a new application in the UIM is accompanied by its registration in an application called Access Control so that any subsequent access to that application can be performed accordingly.

When implementing an Access Control function, overseas carriers have been known to use a file-centered format instead of an application-centered format. In our UIM, we have decided to go with the latter. When using a file-centered format, the updating of a file within the UIM must be controlled remotely from a network server, which requires that the TSM server and network server interact in real time. When using an application-centered format, however, the functions that we have developed in conformance with GlobalPlatform specifications make it possible to remotely update the Access Control function from the TSM server the same as any other application on the UIM. This approach negates the need for any additional development work or control functions for a network server thereby simplifying the construction and operation of the entire system.

Table 2 Example of lock/lock-release patterns

State	FeliCa	UIM	Permissible operation
A	Lock	Lock	Release only
B	Release	Release	Lock only
C	Lock	Release	Release only
D	Release	Lock	Release only

* For example, if in state C or D and the objective is to lock both FeliCa and UIM, state B must first be entered before a transition to state A can be made.

3) Commonality with FeliCa

As shown in Fig. 2, the antenna and CLF are used in common with the existing FeliCa function. From a software point of view, however, FeliCa and NFC Type A/B are separated at the middleware level and operate independently. However, the fact that they use the same CLF means that both FeliCa and NFC Type A/B must control the CLF as needed, which means that some sort of driver is needed to prevent conflicts. For example, adding money to FeliCa during NFC Type A/B P2P operations would naturally incur a processing conflict, and to prevent this from happening, exclusive control is performed.

In addition, FeliCa must be usable not only in a power ON state but also in a power OFF state provided that the battery is still charged. To provide the user of NFC Type A/B functions with the same level of convenience as that of FeliCa functions, specifications for the same sort of operations have been established. These have become common specifications among three cooperating carriers in Japan. For example, power must be supplied to the UIM to activate card emulation mode when power is OFF, but feeding power continuously to the UIM is hardly desirable form the viewpoint of saving power, so a mechanism that supplies power only on detecting a carrier signal has been adopted. The timing for supplying power to the UIM depends on the existing ISO interface when power is ON and on the newly added SWP/HCI interface via CLF when power is OFF. Since control could become complicated here, a carrier-detection function and a switch-equipped control mechanism have been implemented in CLF.

5. Conclusion

This article provided a functional overview of NTT DOCOMO's newly developed NFC-enabled mobile terminal configuration and associated UIM.

This configuration places functions of the NFC Type A/B global standard in the UIM's SE. In other words, it places FeliCa's SE on the mobile terminal side while placing the Type A/B SE on the UIM side making for cumbersome SE management. Looking forward, we have been studying means of also incorporating FeliCa's SE in the UIM (**Figure 7**). Some issues, however, must be addressed to achieve such a configuration, such as how to satisfy

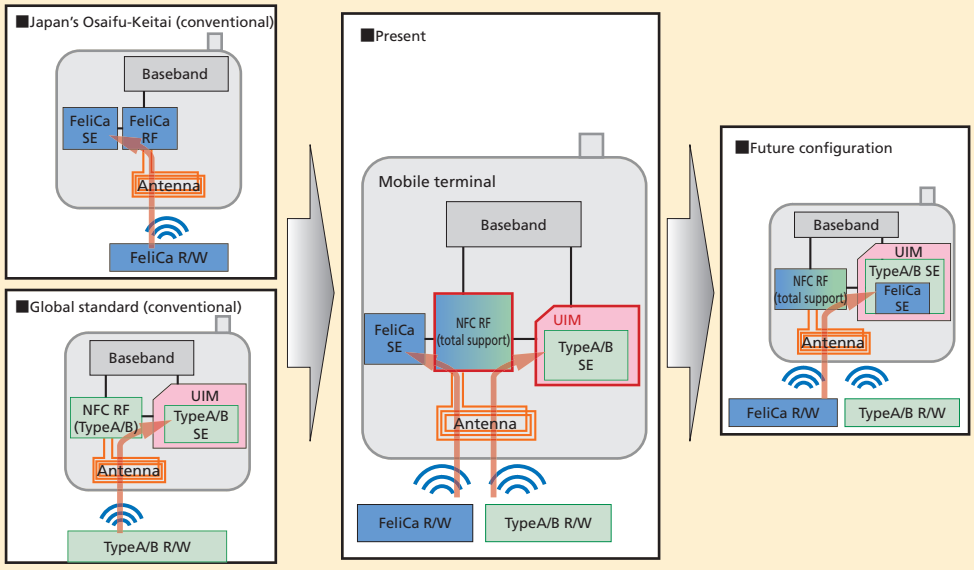

Figure 7 Transition of NFC-enabled mobile terminal and UIM

the processing speeds required by ticket gates in Japanese public transport facilities. At present, the possibility exists of satisfying such processing speeds even with different SEs incorporated in the UIM. However, given the trend toward smaller and thinner UIMs as specified by such standards as Mini-UICC (miniSIM)[*23] and 4FF (nanoSIM)[*24], this may be difficult to achieve looking forward and more study is needed.

We can envision the use of NFC functions for a wide variety of applications both inside and outside Japan. NTT DOCOMO will continue to study the application of NFC services and functions including the above study items with the aim of making the use NFC-enabled mobile terminals even more convenient for users.

REFERENCES

[1] SIMalliance: "Open Mobile API Specification v2.02," Nov. 2011.

[2] GSM Association: "NFC Handset APIs & Requirements v2.0," Nov. 2011.

[3] NFC Forum: "NFC Forum Device Requirements v1.0," Oct. 2010.

[4] GlobalPlatform: "GlobalPlatform Card Specification v2.2," Mar. 2006.

[5] GlobalPlatform: "GlobalPlatform Card UICC Configuration v1.0.1," Jan. 2011.

[6] GlobalPlatform: "GlobalPlatform Card Contactless Services Card Specification v2.2 - Amendment C v1.0," Feb. 2010.

[7] ETSI TS 102 613: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics v9.2.0," Mar. 2011.

[8] ETSI TS 102 622: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) v9.3.0," Mar. 2011.

[9] 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.

*23 **Mini-UICC (miniSIM)**: An ETSI standard specifying UIM physical shape. The formal name of this standard is Mini-UICC. Shrinks dimensions to 15 × 12 mm from 25 × 15 mm of past UIM (Plug-in UICC). Unchanged are thickness (0.76 mm) and pin arrangement.

*24 **4FF (nanoSIM)**: An ETSI standard specifying UIM physical shape (4th Form Factor). Shrinks dimensions from those of 3FF to 12.3 × 8.8 mm. Pin arrangement is the same but thickness is now 0.67 mm.