Terminals UIM Remote Activation

Technology Reports

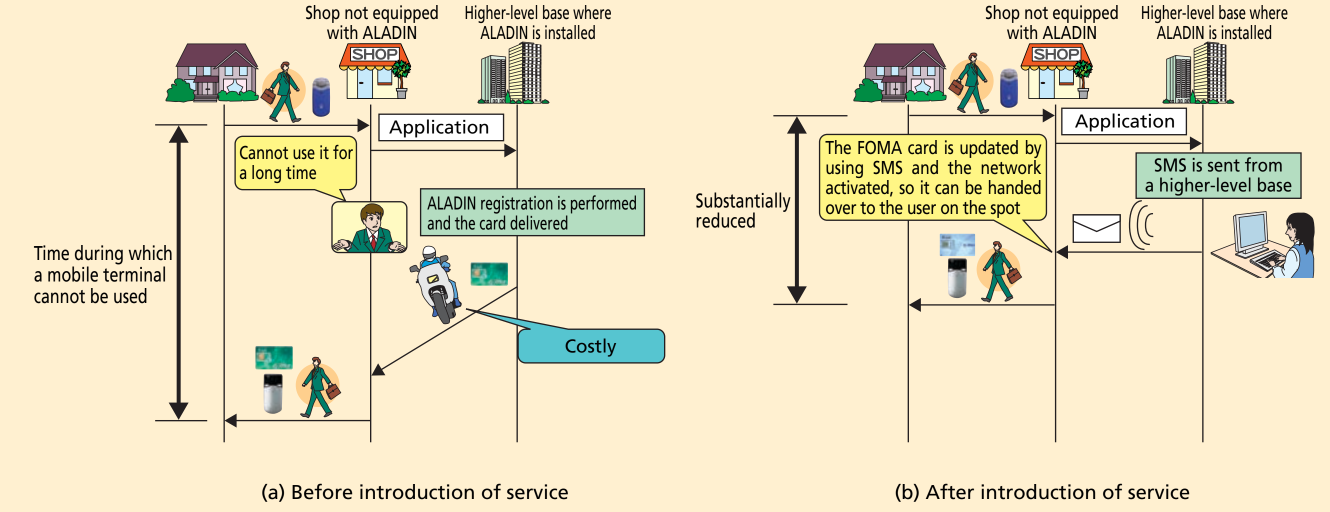
UIM Version 3

Motoi Minami and Sanae Hotani

There are situations where users cannot use their mobile terminals upon replacing models at shops that are not equipped with a customer management system. UIM version 3 comes equipped with a function that makes it possible to remotely update files on the UIM card, and was specifically developed to reduce the time needed for this process.

1. Introduction

Mobile Number Portability (MNP) launched in October 2006 requires that upon meeting a user's request to switch subscription from another telecommunication carrier to NTT DoCoMo, that user's "own phone number" and other user data be written to NTT DoCoMo's User Identity Module (UIM)[*1]. Moreover, given the rapid transition in recent years from mova of Second-Generation (2G) to FOMA of Third-Generation (3G) as evidenced by the number of FOMA subscribers exceeding the number of mova subscribers in June 2006, the shift to FOMA is expected to accelerate even more in the future. Conventionally when mova users went to a shop not equipped with the ALl Around DoCoMo INformation systems (ALADIN) customer management system for replacing their mova mobile terminals with FOMA models, their "own phone numbers" and other user data could not be written to the UIM card. Therefore, such data had to be written to the UIM card at a shop with ALADIN, and then delivered and handed over to the user (**Figure 1** (a)). This delay prevented the user from using the mobile terminal for a while, as well as increased delivery costs. UIM version 3 equipped with the User Subscriber identity module Application Toolkit (USAT) function was developed to address these issues. Among FOMA mobile terminals, the 903i series


Shop not equipped with ALADIN
Higher-level base where ALADIN is installed
SHOP
Application
Cannot use it for a long time
ALADIN registration is performed and the card delivered
Time during which a mobile terminal cannot be used
Costly
Shop not equipped with ALADIN
Higher-level base where ALADIN is installed
SHOP
Application
The FOMA card is updated by using SMS and the network activated, so it can be handed over to the user on the spot
SMS is sent from a higher-level base
Substantially reduced

(a) Before introduction of service

(b) After introduction of service

Figure 1 Flow of model replacement process

[*1] **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.

and later models support this USAT function. As a result, when a user wants to replace his/her mobile terminal with a different model and visits a shop without ALADIN, the waiting time can be dramatically reduced by using these mobile terminals in combination with UIM version 3, since the model replacement process is completed by a higher-level base simply transmitting Short Message Service (SMS)[*2] and activating a Network (Fig. 1 (b)).

The newly developed UIM version 3, which incorporates a new USAT function, makes it possible to remotely update data on the UIM card via Over The Air (OTA)—a function that can write, update, and delete data, as well as perform other tasks wirelessly. Another advantage is that when introducing overseas terminals equipped with the USAT function compliant with 3rd Generation Partnership Project (3GPP) standards, the need for new terminal development is reduced. The use of the USAT function also makes it possible to not only update files on the UIM card, but also to show text on the mobile terminal's display and activate ring tones by remotely transmitting commands from the UIM card. In particular, UIM version 3 can issue proactive commands sequentially without requiring additional development when equipped with NTT DoCoMo's unique applet[*3], and is characterized by its ability to realize a flexible mobile terminal User Interface (UI). When equipped with this function, distinctive services unique to the operator can be provided and shops without ALADIN can improve their operational efficiency. Various files on the UIM card can also be updated securely even after handing the card over to the user, upon NTT DoCoMo performing authentication between the OTA server and UIM card, and sending SMS via OTA as necessary.

This article provides an overview of UIM version 3 and the USAT function, and describes examples of services using the OTA/USAT function.

2. UIM Version 3

This chapter describes the architecture of UIM version 3 and compares it with earlier versions.

Figure 2 shows the architecture of UIM version 3. UIM version 2 is equipped with such functions as the Subscriber Identity Module (SIM)[*4] application, PDC application, and Public Key Infrastructure (PKI)[*5], in addition to the functions inherited from UIM version 1 [1]. On top of these functions, UIM version 3 is equipped with the new USAT function, which consists of USAT commands/proactive commands and the USAT application. Regarding other commands, physical or electrical characteristics, protocol specifications or other aspects, no changes have been made from the previous versions, so that compatibility is ensured with existing FOMA terminals that do not support the USAT function. The card design varies in color between the versions as follows: blue for version 1, green for version 2, and white for version 3 (**Photo 1**). The color scheme makes it easy to distinguish UIM version 3.

3. USAT Function Overview

The USAT function is a standard function specified in 3GPP TS31.111 [2].

Photo 1 UIM version 3

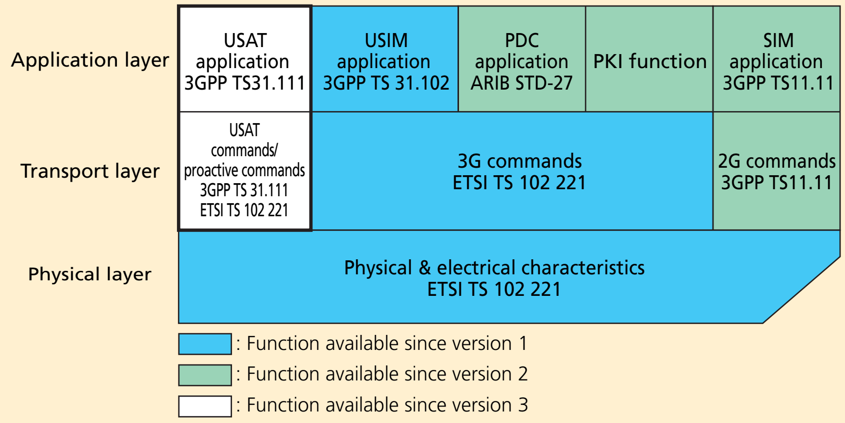

Application layer
Transport layer
Physical layer
USAT application 3GPP TS31.111
USIM application 3GPP TS 31.102
PDC application ARIB STD-27
PKI function
SIM application 3GPP TS11.11
USAT commands/ proactive commands 3GPP TS 31.111 ETSI TS 102 221
3G commands ETSI TS 102 221
2G commands 3GPP TS11.11
Physical & electrical characteristics ETSI TS 102 221
🟦 : Function available since version 1
🟩 : Function available since version 2
□ : Function available since version 3

Figure 2 Architecture of UIM version 3

[*2] **SMS**: Service for sending/receiving short text-based messages mainly between mobile terminals. It can also be used for sending/receiving control signals for mobile terminals.

[*3] **Applet**: A relatively small application that runs on the card's operation system.

[*4] **SIM**: An IC card on which the phone number and other information about a user are stored in subscribing to a mobile communication company. The subscriber identification module in GSM is referred to as SIM.

[*5] **PKI**: A generic term for systems, etc. built for ensuring secure communications using public key encryption technology.

Given its use of proactive commands as specified in 3GPP TS31.111 and USAT commands specified in European Telecommunications Standards Institute (ETSI)[*6] TS 102 221 [3], it is possible to provide various functions and services among UIM cards, mobile terminals and networks that support the USAT function. This chapter provides an overview of the proactive commands and USAT commands, and explains the USAT application and security of OTA.

3.1 Proactive Commands

In the case of 3G commands[*7] and 2G commands[*8], the mobile terminal acts as the master while the UIM card serves as a slave. In contrast, the UIM card issues proactive commands to the mobile terminal, enabling the UIM card to act as the master and control the mobile terminal. Among the many proactive commands that have been defined, this article explains four principal commands:

1) DISPLAY TEXT

This command shows text messages and icons on the mobile terminal's display.

2) PLAY TONE

This command activates ring tones on the mobile terminal. The tone, ringing time, and other settings can also be specified.

3) REFRESH

This command updates cache data on the mobile terminal after file data or file status on the UIM card is changed.

4) SEND SMS

This command sends data from the UIM card to networks via the mobile terminal, and is used to report command processing results, etc.

3.2 USAT Commands

The following four commands are defined as USAT commands:

1) TERMINAL PROFILE

This command notifies the UIM card about which USAT-function-related commands are supported by the mobile terminal. This command is normally issued after resetting (such as switching ON the mobile terminal's power).

2) ENVELOPE

This command conveys a data string received from the network in the form of SMS to the UIM card. Optional 3G commands, 2G commands, proactive commands, and other data can be stored in this data string.

3) FETCH

This command is used to issue a proactive command from the UIM card to the mobile terminal.

4) TERMINAL RESPONSE

This command is issued upon conveying the execution results of proactive commands from the mobile terminal to the UIM card.

3.3 USAT Application

The USAT application allows the addition of unique applets in addition to the Remote File Management (RFM) segment that defines the basic action required for accessing files on the UIM card, and its configuration enables the operator to expand various services uniquely. The USAT application as configured in UIM version 3 consists of RFM and DoCoMo's unique applet based on the USAT framework (**Figure 3**). In SMS via OTA sent from the network, the target is set in the header section and the command processed accordingly by RFM or NTT DoCoMo's unique applet in the USAT application.

RFM is compliant with 3GPP TS31.111 and 3GPP TS23.048 [4], and

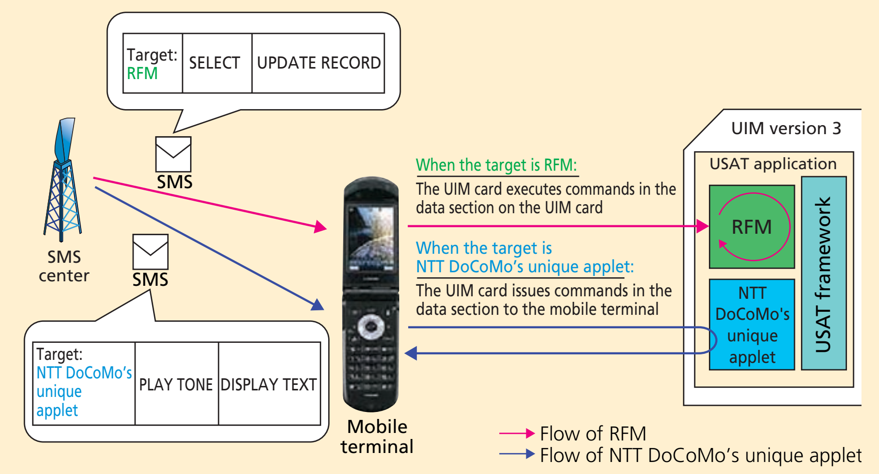

Target: RFM
SELECT
UPDATE RECORD
SMS
SMS center
SMS
Target: NTT DoCoMo's unique applet
PLAY TONE
DISPLAY TEXT
Mobile terminal
When the target is RFM:
The UIM card executes commands in the data section on the UIM card
When the target is NTT DoCoMo's unique applet:
The UIM card issues commands in the data section to the mobile terminal
UIM version 3
USAT application
RFM
NTT DoCoMo's unique applet
USAT framework
Flow of RFM
Flow of NTT DoCoMo's unique applet

Figure 3 RFM and NTT DoCoMo's unique applet

[*6] **ETSI**: A European standardization body engaged in the standardization of telecommunications technologies. Headquartered in Sophia Antipolis, France.

[*7] **3G commands**: Commands set forth in the ETSI TS102 221 specifications that can select and read files, and perform other tasks.

[*8] **2G commands**: Commands set forth in the 3GPP TS11.11 specifications that basically have the same functions as 3G commands but with certain different names. Network authentication (RUN GSM ALGORITHM) and SIM control (SLEEP) are distinctive 2G commands.

enables remote access to files on the UIM card. For example, RFM is used when updating "own phone numbers."

On the other hand, NTT DoCoMo unique applet is installed for the purpose of issuing any proactive commands. In response to receiving SMS consisting of proactive commands sent to the applet from the network, the UIM card issues proactive commands sequentially to the mobile terminal.

As noted in Section 3.2 3), the UIM card requires a trigger to issue proactive commands to the mobile terminal. Without NTT DoCoMo's unique applet installed, it would be necessary to create a trigger to issue commands on the mobile terminal or UIM card with respect to each proactive command to be issued. On the mobile terminal, for example, it is necessary to create a function to issue a proactive command after the user selects a menu or add a new applet on the UIM card to define the trigger used to issue a proactive command. With NTT DoCoMo's unique applet installed, however, UIM version 3 can issue any proactive commands directly from the UIM card. For instance, when notifying the commencement of usage by using the proactive commands "PLAY TONE" and "DISPLAY TEXT," proactive commands are issued by sending SMS via OTA consisting of both proactive commands to NTT DoCoMo's unique applet. It can also change the information displayed on the mobile terminal, its order, and other aspects by simply altering the content of proactive commands sent from the network.

3.4 Security

For the transmission and reception of SMS via OTA, NTT DoCoMo's unique authentication algorithm is adopted to protect against the illegal tampering of SMS transmissions and data by malicious third parties, in addition to the security mechanism specified in 3GPP TS23.048. Security is further enhanced since OTA-based update access conditions are defined with respect to each file, and updatable files are limited by setting files that can be updated via OTA and those that are not.

4. Services Examples Using the OTA/USAT Function

This chapter explains how an "own phone number" is updated and the commencement of usage notified by using the OTA/USAT function.

Advance preparations made at a shop without ALADIN involve the procurement of UIM version 3 cards in the "gray" state where International Mobile Subscriber Identity (IMSI)[*9], operator-controlled Public Land Mobile Network (PLMN)[*10] and other communication setup information except "own phone number" are written, along with mobile terminals supporting the USAT function. When a user visits a shop without ALADIN and wants to replace a mova mobile terminal with a FOMA model or switch subscription from another telecommunication carrier, a UIM version 3 card and mobile terminal supporting the USAT function provided in advance are used to update the "own phone number" and activate the network, after which the mobile terminal is handed over to the user.

4.1 Updating "Own Phone Number"

Figure 4 shows the sequence of updating an "own phone number." At the shop without ALADIN and visited by the user, a UIM version 3 card in the "gray" state with a temporary phone number is inserted into the mobile terminal, which is switched ON (Fig. 4 (1)) and left in standby mode. The mobile terminal issues TERMINAL PROFILE to the UIM card (Fig. 4 (2)), to which UIM responds normally (Fig. 4 (3)). Then it enters USAT Idle mode (Fig. 4 (4)), after which actions using the USAT function are enabled. While in this mode, a higher-level base sends SMS consisting of commands to update the "own phone number" stored in a file on the UIM card with respect to the temporary phone number in the "gray" state (Fig. 4 (5)). The mobile terminal supporting the USAT function that receives the SMS interprets it as being targeted at the UIM card and passes the SMS content to the UIM card (Fig. 4 (6)). Then the UIM card processes the commands in the SMS received and updates the "own phone number." RFM executes this process. After updating the "own phone number," the UIM card responds with SW (Status Word)[*11]=91XXh (where XX stores the data length of the proactive command to be transmitted next) in order to receive FETCH—which triggers a response to the server—from the mobile

[*9] **IMSI**: A number used in mobile communications that is unique to each user and stored on a UIM card.

[*10] **Operator-controlled PLMN**: Order of priority that can be stored by the operator on the UIM card regarding connection to the networks of other operators.

[*11] **SW**: 2-byte response data sent back from the UIM card.

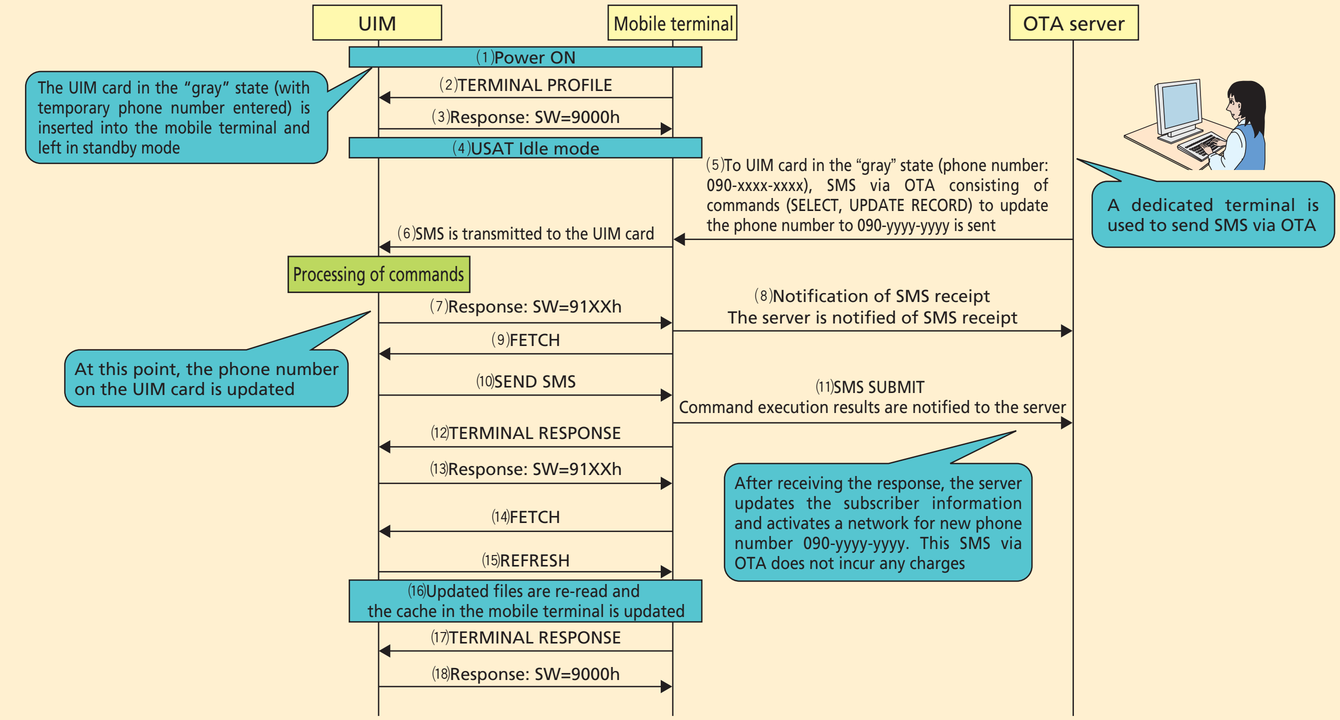

UIM
Mobile terminal
OTA server
(1)Power ON
The UIM card in the "gray" state (with temporary phone number entered) is inserted into the mobile terminal and left in standby mode
(2)TERMINAL PROFILE
(3)Response: SW=9000h
(4)USAT Idle mode
(5)To UIM card in the "gray" state (phone number: 090-xxxx-xxxx), SMS via OTA consisting of commands (SELECT, UPDATE RECORD) to update the phone number to 090-yyyy-yyyy is sent
A dedicated terminal is used to send SMS via OTA
(6)SMS is transmitted to the UIM card
Processing of commands
(7)Response: SW=91XXh
(8)Notification of SMS receipt
The server is notified of SMS receipt
At this point, the phone number on the UIM card is updated
(9)FETCH
(10)SEND SMS
(11)SMS SUBMIT
Command execution results are notified to the server
(12)TERMINAL RESPONSE
(13)Response: SW=91XXh
After receiving the response, the server updates the subscriber information and activates a network for new phone number 090-yyyy-yyyy. This SMS via OTA does not incur any charges
(14)FETCH
(15)REFRESH
(16)Updated files are re-read and the cache in the mobile terminal is updated
(17)TERMINAL RESPONSE
(18)Response: SW=9000h

Figure 4 Sequence of updating "own phone number"

terminal (Fig. 4 (7)). At this point, the mobile terminal that received the response sends a notification of SMS receipt to the OTA server (Fig. 4 (8)). Upon receiving FETCH from the mobile terminal (Fig. 4 (9)), the UIM card issues SEND SMS to the mobile terminal (Fig. 4 (10)) and conveys the results of updating the "own phone number," which are then passed from the mobile terminal to the OTA server (Fig. 4 (11)). The mobile terminal subsequently issues TERMINAL RESPONSE to inform the UIM card that SMS transmission to the server has been successfully completed (Fig. 4 (12)). Then the UIM card issues a new proactive command to resynchronize the difference between the information stored on the UIM card and in the cache of the mobile terminal resulting from information updated on the UIM card. For this purpose, the UIM card responds to TERMINAL RESPONSE with SW=91XXh (Fig. 4 (13)) and receives FETCH from the mobile terminal (Fig. 4 (14)). It subsequently issues REFRESH to the mobile terminal (Fig. 4 (15)), which re-reads the updated files and updates the cache in the mobile terminal (Fig. 4 (16)). After updating the cache, the mobile terminal issues TERMINAL RESPONSE to notify the UIM card that the process is completed (Fig. 4 (17)). The UIM card responds to TERMINAL RESPONSE with a normal response SW=9000h (Fig. 4 (18)). This completes the entire process.

4.2 Usage Commencement Notification

Figure 5 shows the sequence of notifying the commencement of usage. The server receives a normal response to SMS with regard to updating the "own phone number" mentioned in Section 4.1 (Fig. 4 (11)), and then automatically transmits SMS to notify the completion of network activation (Fig. 5 (1)). The mobile terminal supporting the USAT function that receives the SMS interprets it as being targeted at the UIM card and conveys the SMS content to the UIM card (Fig. 5 (2)). Then the UIM card interprets that the SMS received is targeted at NTT DoCoMo's unique applet and responds with SW=91XXh to receive FETCH—which serves as a trigger to issue a proactive command—from the mobile terminal (Fig. 5

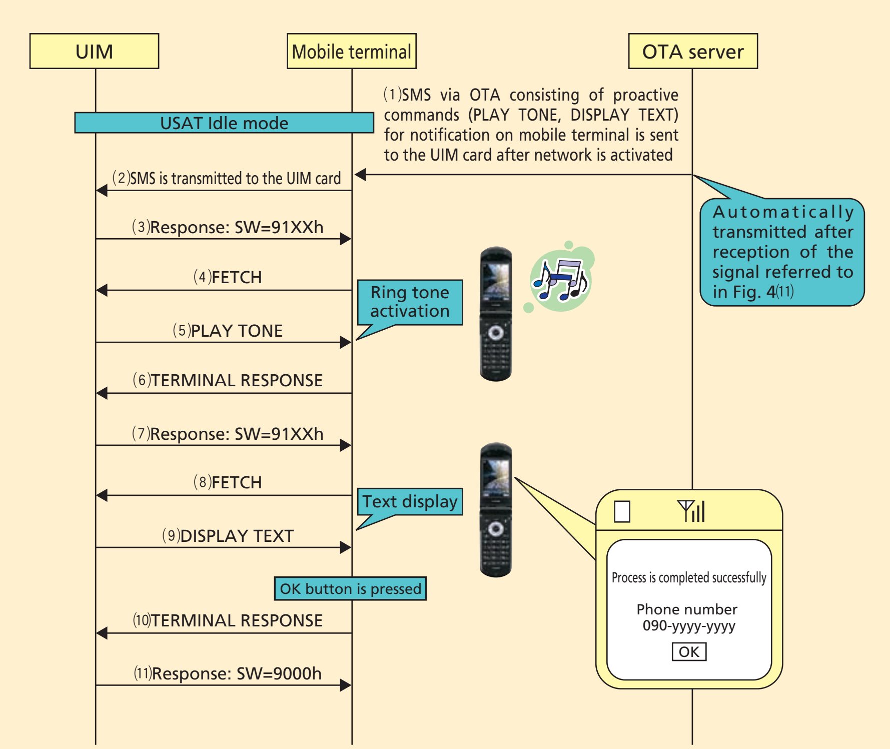

UIM
Mobile terminal
OTA server
USAT Idle mode
(1)SMS via OTA consisting of proactive commands (PLAY TONE, DISPLAY TEXT) for notification on mobile terminal is sent to the UIM card after network is activated
(2)SMS is transmitted to the UIM card
Automatically transmitted after reception of the signal referred to in Fig. 4(11)
(3)Response: SW=91XXh
(4)FETCH
Ring tone activation
(5)PLAY TONE
(6)TERMINAL RESPONSE
(7)Response: SW=91XXh
(8)FETCH
Text display
(9)DISPLAY TEXT
OK button is pressed
(10)TERMINAL RESPONSE
(11)Response: SW=9000h
Process is completed successfully
Phone number
090-yyyy-yyyy
OK

Figure 5 Sequence of usage commencement notification

(3)). After receiving FETCH from the mobile terminal (Fig. 5 (4)), the UIM card issues PLAY TONE, the first of the proactive commands in the SMS received, to the mobile terminal (Fig. 5 (5)) and thereby activates the ring tone on the mobile terminal. The mobile terminal subsequently issues TERMINAL RESPONSE to inform the UIM card that ring tone activation has been successfully completed (Fig. 5 (6)). Then the UIM card responds with SW=91XXh to receive FETCH—which serves as a trigger to issue second proactive command DISPLAY TEXT in SMS—from the mobile terminal (Fig. 5 (7)). After receiving FETCH from the mobile terminal (Fig. 5 (8)), the UIM card issues DISPLAY TEXT to the mobile terminal (Fig. 5 (9)) and shows the text on the mobile terminal's display. Since these processes are actually executed in an extremely short time, ring tone activation and text display seem to occur almost simultaneously. When the "OK" button shown on the display is pressed, the mobile terminal issues TERMINAL RESPONSE (Fig. 5 (10)) and notifies the UIM card of the command execution results. The UIM card then sends a response (Fig. 5 (11)), with which the process is completed. At this point, all necessary tasks have been completed and the UIM card can be handed over to the user.

5. Other Services Using OTA

In addition to updating an "own phone number" as explained above, it is possible to update other files on the UIM card using the combination of UIM version 3 and a mobile terminal supporting the USAT function by simply expanding functions on the network side. For example, operator-controlled PLMN stored on the UIM card can be updated. This makes it possible to remotely change the priority order of networks in cases where more than one network is available during international roaming. It also enables us to easily update the operator-controlled PLMN list upon concluding a new roaming contract or canceling an existing one. This feature eliminates the need for a user to search unnecessary networks when using the UIM card overseas, and thus allows the user to begin using it much more quickly.

6. Conclusion

This article provided an overview of UIM version 3 and the OTA/USAT function incorporated into the 903i series, and explained some examples of usage in specific services. As standardization efforts are being made on Universal SIM (USIM)*12 and SIM at the 3GPP TSG-CT WG6 and ETSI Smart Card Platform (SCP), NTT DoCoMo attends these standardization meetings and actively contributes to the preparation and clarification of specifications. Studies are now being conducted to standardize the expansion of USIM memory capacity and accelerate communication between mobile terminals and USIM. Portability when switching between models is expected to improve dramatically as USIM becomes usable even in

*12 **USIM**: An IC card on which the phone number and other information about a user are stored in subscribing to a mobile communication company. In 3GPP, the mobile communication subscriber identification module for W-CDMA is referred to as USIM.

the form of external media in the future, such as a phonebook function equivalent to that of mobile terminals being incorporated into UIM cards (for up to 1,000 entries with images, etc.) and more available video and image storage. There are also ongoing studies being conducted to determine what kind of services would gain wide acceptance among users, since expanded memory will make it possible to incorporate new applications and applets into UIM cards.

References

[1] H.Ishikawa et al.: "UIM Version 2," NTT DoCoMo Technical Journal, Vol.5, No.3, pp. 37–43, Dec. 2003.

[2] 3GPP TS31.111 V3.13.0 (2004–09): "USIM Application Toolkit (USAT)."

[3] ETSI TS102 221V3.17.0 (2005–10): "Physical and logical characteristics."

[4] 3GPP TS23.048V5.9.0 (2005–06): "Security mechanisms for the(U)SIM application toolkit; stage2."