UIM Version 2

Hidetoshi Ishikawa, Chiaki Nogawa, Kazuhiko Takahashi and Masahiro Furuse

UIM is a smart cards standard for mobile communications that allow storage of subscriber identification information of several networks. Conventionally, the usage of UIM was limited to USIM applications. In order to make it more sophisticated, we have developed UIM version 2, which implements the PKI function as well as GSM and PDC applications.

1. Introduction

A User Identity Module (UIM) smart card for mobile communications (the product name is FOMA card) is an integral part of the implementation of the Freedom Of Mobile Multimedia Access (FOMA) service (Photo 1).

The UIM smart card has the same shape as common credit cards, but for some types of terminals, it is used by removing the part of the card where the IC chip is embedded (plug-in size part) and inserting this into the terminal.

FOMA terminals are equipped with a UIM socket (Universal Integrated Circuit Card (UICC) socket). Users are allowed to make and receive outgoing/incoming calls using their contracted phone numbers by inserting the UIM smart card into the UIM socket of their terminals.

The main feature of UIM version 2 (UIMv2) is that it is compatible with the third-generation mobile communication (International Mobile Telecommunications-2000 (IMT-2000)) terminals and Global System for Mobile communications (GSM) terminals of other service operators; it can be used by inserting it into such terminals as well.

In the Japanese second-generation mobile communication
system, in the same way as for the Advanced Mobile Phone System (AMPS) of the US, user identification information was integrated into and inseparable from terminals. The implementation of UIM allows separating subscriber information from the mobile terminals themselves, which means that users do not need to register model changes; they can use new mobile terminals as their registered terminals just by inserting the UIM smart card from their old mobile terminals into new ones.

Moreover, operators can implement their own security features in the UIM smart card.

2. Overview

It is specified to use a Universal Subscriber Identity Module (USIM) in all IMT-2000 terminals. Correspondingly, in GSM, which is mainly used in Europe and other countries, a Subscriber Identity Module (SIM) is utilized.

Since the equivalent identity module standard of DoCoMo implements its own functions in addition to the USIM and SIM applications specified in the standard specifications, we call it UIM (Figure 1).

Basically, UIM provides the following functionality (Figure 2).

1) Function for Call Control and Authentication for Networks

This function is required when users use networks for activities such as making telephone calls, receiving/sending packet communication and roaming user communication. UIM allows supporting various types of networks to which the terminals can be connected, such as FOMA, GSM, or Personal Digital Cellular (PDC) systems (Figure 3).

2) Function for Providing Additional Services

In addition to the basic services such as telephone calls, UIM also allows to provide DoCoMo's own services such as the FirstPass (Secure Sockets Layer (SSL) client authentication) digital certificate service.

3) Function to Store Personal Information (e.g., phonebook) in Terminals

This function allows accessing phonebooks and writing/viewing short messages, used locally within terminals.

In addition to the above, UIM provides functions to link to customer systems and so forth.

The FOMA UIM smart card is supplied in two versions: version 1 (UIMv1: blue FOMA card) and version 2 (UIMv2: green FOMA card) (Figure 4).

In UIM version 1 (UIMv1), which was launched at the same time as the start of the FOMA service, only USIM application subscriber information was stored. In UIMv2, we have added the following functions in addition to the functions of UIMv1.

1) SIM Application

The UIMv2 smart card can be inserted into GSM terminals; this allows affiliated GSM operators to provide international roaming services. This service is provided under the name "WORLD WING."
2) PDC Application

The UIMv2 smart card can be inserted into IMT/PDC dual terminals (terminals used for both IMT-2000 and PDC: as of July 2003, FOMA N2701 is compliant to both of these standards); it allows using both FOMA and PDC services from the same terminal.

3) PKI Function

UIMv2 allows FirstPass SSL client authentication.

Some of the functions specified by the USIM and SIM standard specifications are not implemented in UIM for FOMA. Typical examples include the USIM Application Tool kit (USAT) and the SIM Application Tool kit (SAT).

The USAT and SAT provide functions that allow USIM and SIM smart cards to control the terminals, enabling them to show characters in the display and access networks (Short Message Services (SMS) transmission). Therefore, by implementing the USAT and SAT functions in USIM and SIM, it would become possible for operators to provide their own unique services. Moreover, a user would be able to enjoy the same services even if they were to move a USIM/SIM smart card from one terminal with USAT/SAT support to another terminal supporting USAT/SAT. However, DoCoMo had no special needs to implement the USAT and SAT functions in UIMv1 and UIMv2 because the i-mode service has already become popular.

3. Specifications

3.1 Physical Specifications

The UIMv2 smart card has the same physical size as a credit card, i.e., ID-1 size (full size), and the base material is treated with plug-in cutting. A material called PET-G is employed for the card base material, taking temperature and weather resistance into consideration. PET-G satisfies the temperature characteristics of the standard specifications and causes little environmental load at disposal. In the SIM and smart card markets in general, materials such as PolyVinyl Chloride (PVC) and ABS resin are often used.

3.2 Electric Specifications

The UIMv2 smart card can operate with power supply voltages (Vcc) of 5 V and 3 V. Its maximum current consumption is compliant to the Technical Specification (TS) 102.221 R99 specification of European Telecommunications Standards Institute (ETSI); i.e., it is 7.5 mA or less, which is the minimum current that should be supplied from the UIM interface part of a terminal. Moreover, it supports a clock stop mode in which the clock signal is no longer supplied from the terminal when no command is executed for a period of time.

3.3 Protocol Specifications

We employed the Direct Convention for the data encoding. Direct Convention is a transfer method of individual bytes. Each byte is first sent with the Least Significant Bit (LSB) and using positive logic, i.e., logic values of 1 and 0 correspond to high and low electric potential, respectively. The standard specifications for the 3rd Generation Partnership Project (3GPP) specify both the T=0 protocol (mandatory: half-duplex asynchronous character transfer protocol) and the T=1 protocol (optional: half-duplex asynchronous block transfer protocol) as transfer protocols of USIM. UIMv2, however, adopts only the T=0 protocol.

3.4 Command Specifications

1) USIM Commands

UIMv2 supports the class byte 00h and 80h commands specified by the ETSI TS 102.221 specification, however it does not support commands related to USAT.

Types of commands include file selection (SELECT), acquisition of file selection status (STATUS), file read (READ BINARY, READ RECORD), file update (UPDATE BINARY, UPDATE RECORD), record search (SEARCH RECORD), addition to setup value (INCREASE), PIN related commands such as checking/changing PIN (VERIFY PIN, CHANGE PIN, DISABLE PIN, UNBLOCK PIN), network authentication (AUTHENTICATE), file activation/deactivation (DEACTIVATE FILE, ACTIVATE FILE) and information acquisition (GET RESPONSE).
3.6 Security

The IC chips used for the UIM smart cards have a tamper-resistant \(^1\) structure that is robust against physical/electrical reverse-engineering and other forms of malign manipulation. Moreover, the operating system is designed to make the best possible use of this tamper resistant structure and taking the security fully into consideration; the UIM smart card thus has excellent security performance.

4. Telecommunication Applications

4.1 Overview

In the 3GPP and ETSI standard specifications, the file trees expanded under the main ADFs and DFs are sometimes called applications. This term is different from application software used in general PCs and does not necessarily refer to cases where software functions (e.g., commands) and files are paired.

1) USIM Application

The USIM application stores subscriber information used in FOMA terminals. It can store up to 20 messages of SMS and 50 phonebooks (Global Phonebook), among others. It can store prioritized operator lists containing up to 20 entries on the user side and 40 entries on the DoCoMo side.

2) SIM Application

The SIM application stores subscriber information used in GSM terminals, in the same way as for the USIM application.

Some of the EFs have the same structure as the USIM application and allows linking files (file link).

3) PDC Application

It is used by IMT/PDC dual terminals to connect to a PDC network. The PDC application shares the phonebooks (Global Phonebook) of the USIM application.

4.2 Common Specifications Among the Applications

1) Phonebook

UIMv2 supports Global Phonebooks, and UIMv2 smart cards are thus not equipped with Local Phonebooks.

2) File Link

For historical reasons, the EFs supported by the USIM application and GSM application have many structural similarities, which means that EFs assigned to logically different locations can use common information by referring to the same memory area in the IC chip.

\(^1\) Tamper-resistant: Confidential information stored inside a device cannot be disclosed nor tampered with by anyone other than legitimate right holders.
For example, the Global Phonebooks of the USIM application share the same physical memory areas as the phonebooks of the SIM application via a file link. This can reduce the physical memory area to approximately half of the logically required memory capacity.

Moreover, this allows simplifying the processing procedure involved in issuing the UIM smart card in customer management systems ALI Around DoCoMo INformation systems (ALADIN).

5. PKI Function

5.1 Advantages of Implementing PKI Function in UIM

The Public Key Infrastructure (PKI) function is necessary for the digital certificate service.

One of the important issues of the PKI function is how private keys paired with public keys can be managed and operated safely. The solution chosen here, to manage the private keys within the UIM smart card, is beneficial in terms of tamper resistance viewpoint.

The signature generation function will require entry of a Personal Identity Number (PIN) 2 code for the USIM application every time it generates a signature, rather than a PIN1 code. This prevents unauthorized use by third parties and improves the security of the signature-based identification. Moreover, this system has the further advantage of both high security and portability. The same certificate of the same user can be utilized commonly among different FOMA terminals supporting the PKI function by mounting the UIMv2 smart card in the terminals.

5.2 Basic Design

In order to implement the PKI function in UIMv2, we adopted the RSA*" public key cryptosystem, which has become the standard on the Internet. This section provides an outline of the UIM design related to the PKI function.

(1) File Layout

We allocated a dedicated DF in the USIM application and put all data related to the PKI function there, such as user cer-
tificates and RSA public keys. This allows terminals to access the PKI function while the USIM application is running without using logical channels.

(2) Commands

As commands dedicated to the PKI function, we added original commands for generating RSA key pairs, downloading user certificates and generating signatures.

(3) Security

We classified the security related design into two categories: design related to information that can be referenced from the outside including user certificates, and design related to information and functions that must be protected against access from the outside by security measures such as private keys and methods for storing user certificates while downloading from the certificate authority. For the latter, we made the design so that secure procedures are established as a self-contained system and sufficient security is maintained for operation of the UIM smart card itself, in order to prevent access other than authorized operations.

(4) Restrictions on the Memory and Operation Speed

In order to carry out the complex calculations involved in the RSA algorithm at high speeds, we selected an IC chip with built-in co-processor function; processing times well under half a second were achieved.

RSA key pair generation process on the IC chip, on the other hand, generally takes a long time. For this reason, we judged that dynamic generation is impractical while the UIM smart card is mounted on terminals, considering the operation in mobile communication. We therefore decided to store five RSA key pairs in advance during production of the UIM smart card.

6. Tests of UIMv2

6.1 Command Test

UIMv2 smart cards are supplied from several UIM smart card manufacturers, and their products must operate according to identical specifications. It is, however, difficult to exactly obtain identical operations including those under the interface level of commands, simply by specifying standard specifications and so forth for reference purposes.

For this reason, we developed an original command test system that allows checking all the command functions of UIMv2. This has made it possible to achieve uniform and improved operation quality for UIM smart cards produced by different manufacturers.

6.2 File Test

Since file configuration and default values of files are important for each application, it is necessary to conduct a thorough file test. We specified a list of file parameters necessary to interface with terminals and networks and require all the tests to be conducted for delivered products.

7. Interoperability

Interoperability refers to connectivity between devices. That is, interoperable devices are products of various vendors that can be mutually connected and used because they are designed to be compliant to well-defined interface specifications.

As the number of vendors and products increases, the importance of interoperability becomes higher and the number of items to be checked and the amount of necessary tasks will increase. In other words, a multi-vendor market can only be achieved in systems with interoperability.

1) Interoperability of IMT-2000

Since IMT-2000 assumes international roaming, USIM smart cards, terminals and networks from any vendor can be freely combined and used mutually as far as the products are compliant to the 3GPP specifications and others.

2) Interoperability of FOMA Networks

In the development of DoCoMo’s FOMA network devices, interoperability is secured by being compliant to the 3GPP specifications and so forth. Moreover, we constantly conduct interoperability tests on actual products, so that the interoperability can be guaranteed in a reliable manner.

3) Interoperability with FOMA Terminals

In the development of UIMv2, connectivity tests with UIMv2 smart cards are conducted on both FOMA terminals under development and all the FOMA terminals that have been commercialized already in order to secure interoperability with existing FOMA terminals.

4) Interoperability with GSM Terminals

Since UIMv2 smart cards are equipped with the GSM application, it was necessary to verify that they would operate normally when they are inserted into GSM terminals. During the development of UIMv2, we conducted interoperability verification tests with more than 60 GSM terminal models from 12 manufacturers.

5) Interoperability with IMT-2000 Terminals

Since the IMT-2000 network service has been launched by several overseas operators, several IMT-2000 terminal models
other than FOMA terminals have already been introduced on
the market. We verified the interoperability of such terminals
with UIMv2 as well.

8. Standardization Activities

The standard specifications related to USIM and SIM are
examined at 3GPP-TSG-TWG3 and ETSI Smart Card Platform
(SCP). DoCoMo also continuously contributes to the creation
of specifications and clarification of the contents of the specifi-
cations through participation in various standardization confer-
ences.

In order to achieve better interoperability, the activities at
standardization conferences are essential. In such conferences, it
is first necessary to coordinate specifications—both design
specifications and test specifications—and upgrade the docu-
ments. Secondly, it is important to make the descriptions of the
standard specifications more accurate, so that each participant
(vendor and operator) agrees on the same understanding.

9. Conclusion

Presently, various types of smart cards for ID are used and
going to be used in the near future such as identification cards,
driver’s licenses, credit cards, telephone cards, transportation
system cards, electronic settlement of small amount and railway
commuting passes, and some are now being tested in practical
use. A social infrastructure based on these smart cards will pen-
etrate into our lives, the services will be developed, and the con-
venience of using them will become more and more higher.

It is expected that some of these service applications will be
able to function in cooperation with the UIM smart card, or
there will be further development when it’s integrated into the
UIM smart card itself. A society where we can handle most of
our daily activities just by carrying around a terminal with an
advanced UIM smart card may become reality in the immediate
future.

<table>
<thead>
<tr>
<th>ABBREVIATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP: 3rd Generation Partnership Project</td>
</tr>
<tr>
<td>ADF: Application Dedicated File</td>
</tr>
<tr>
<td>AID: Application IDentifier</td>
</tr>
<tr>
<td>ALADIN: All Around DoCoMo INformation systems</td>
</tr>
<tr>
<td>ARIB: Association of Radio Industries and Businesses</td>
</tr>
<tr>
<td>ATR: Answer To Reset</td>
</tr>
<tr>
<td>DF: Dedicated File</td>
</tr>
<tr>
<td>EF: Elementary File</td>
</tr>
<tr>
<td>ETSI: European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>FOMA: Freedom Of Mobile multimedia Access</td>
</tr>
<tr>
<td>G3M: Global System for Mobile communications</td>
</tr>
<tr>
<td>IMT: International Mobile Telecommunications-2000</td>
</tr>
<tr>
<td>MF: Master File</td>
</tr>
<tr>
<td>OS: Operating System</td>
</tr>
<tr>
<td>POC: Personal Digital Cellular</td>
</tr>
<tr>
<td>PIN: Personal Identity Number</td>
</tr>
<tr>
<td>PKI: Public Key Infrastructure</td>
</tr>
<tr>
<td>PPS: Protocol and Parameter Selection</td>
</tr>
<tr>
<td>PVC: PolyVinyl Chloride</td>
</tr>
<tr>
<td>SAT: SIM Application Tool kit</td>
</tr>
<tr>
<td>SCP: Smart Card Platform</td>
</tr>
<tr>
<td>SIM: Subscriber Identity Module</td>
</tr>
<tr>
<td>SMS: Short Message Service</td>
</tr>
<tr>
<td>SSL: Secure Sockets Layer</td>
</tr>
<tr>
<td>TS: Technical Specification</td>
</tr>
<tr>
<td>UICC: Universal Integrated Circuit Card</td>
</tr>
<tr>
<td>UIM: User Identity Module</td>
</tr>
<tr>
<td>UIMv1: UIM version 1</td>
</tr>
<tr>
<td>UIMv2: UIM version 2</td>
</tr>
<tr>
<td>USBAT: USIM Application Tool kit</td>
</tr>
<tr>
<td>USIM: Universal Subscriber Identity Module</td>
</tr>
</tbody>
</table>