Special Articles on FirstPass Digital Authentication Service

FirstPass Service Overview

Norio Nakamura, Hiroaki Yamamoto and Masashi Onogawa

The FirstPass digital authentication service has been designed to enable client authentication to be performed with the aim of improving security and stimulating the expansion of mobile Internet services.

1. Introduction

The equipping of mobile terminals with mobile-Internet access functions has led to more diversified content and more sophisticated input/output interfaces. In this sense, the evolution of the mobile terminal has been driven not only by greater convenience of use but also by the services expansion provided by content providers and business-systems developers (hereinafter referred to as Contents Provider (CP)). As a part of this evolution, DoCoMo's third-generation mobile communication service named "Freedom Of Mobile multimedia Access" (FOMA) was launched in October 2001. At the end of March 2003, FOMA coverage had reached about 91% of the Japanese population and its service area covers almost all major municipalities in Japan.

In the year 2003, new services for FOMA terminals had been launched as well as enhancing the basic performance of FOMA terminals and adding new terminal functions like video display. These services include international roaming through an enhanced FOMA card also known as the User Identity Module (UIM); dual terminals supporting the International Mobile Telecommunications 2000 (IMT-2000) and Personal Digital Cellular (PDC) systems; and a digital authentication service. This expansion of functions by capitalizing on FOMA features is expected to broaden the scope of mobile-Internet services and to promote their use.

This article first describes the market trends in digital

authentication and the digital-authentication functions needed by mobile terminals. It then presents the FirstPass digital authentication service launched in June 2003, its operation method, and an application example.

2. Market Trends in Digital Authentication Services

Expansion of the "mobile Internet" as in Internet shopping, stock trading, and remote access of corporate intranets all by mobile terminal leads to a growing demand for high-level security through individual authentication.

The need for strict individual authentication has been recognized in fields where information is provided to employees over the Internet or shared by sales offices, and large-scale digital authentication systems are being introduced in response to these needs [1]. In 2002, major Internet service providers began to provide client certificate issuance services for their members, and their use in consumer-oriented services is spreading. In addition, the enactment of the e-Signature Law and IT Comprehensive Law in Japan in April 2001 established legal recognition of signatures and certificates created by electronic means, and their use in government-related services is expected to spread rapidly [2].

Client certificates are already being used on a scale of several million IDs, and while the need for such certificates is expected to become all the greater in the future, their use has not expanded to the extent expected several years ago. The main factors hindering the spread of client certificates have been reported to be the cost of introducing and operating digital authentication systems and problems in controlling and using digital certificates [1]. If a breakthrough can be found to resolve this situation, fields that require digital authentication should grow and spread rapidly.

Digital authentication is generally implemented by using Secure Sockets Layer (SSL) technology. The number of sites using SSL server authentication[*1] is increasing yearly and a certain percentage of those sites are providing services for mobile terminals. Most of these services for mobile terminals are thought to be provided by sites that configure intra-company or inter-company information systems, but the number of commercial i-mode sites providing these services is increasing steadily. In short, many sites which provide SSL server authentication are coming to perform some types of client authentication, and a firm foundation for the introduction of SSL client authentication is coming to be prepared.

3. Functional Requirements of Digital Authentication for Mobile Terminals

Digital authentication by mobile terminals means that the result of authentication is used as an individual's authenticates "key" when accessing various services on the Internet. The following describes the requirements of digital authentication using mobile terminals as seen from a service point of view.

Firstly, because of limited memory capacity in a mobile terminal, it is not a smart idea to store many applications. So instead, there is a demand to use only one client certificate for many applications. Most client certificates are in use today, however, they are limited in their application, for example, email certificates for encrypting email and ID certificates for special services. Furthermore, if a client certificate were to include personal attributes (personal information) or information concerning special services, a CP would find this advantageous while the user would not. Including such information would not be suitable for a system that uses one client certificate for various purposes. That is to say, the information included in a client certificate should be minimal and should consist only of what would be needed to identify the user.

Secondly, the ease of use and security for all mobile terminal users are demanded. It is extremely important that client certificates be easy to understand and easy to use without having to be an expert in digital authentication technology or information technology. Usability will be high if all operations related to client certificates can be completed simply by menu operations as same as it's used for the searching and downloading of ring tones or i-applis.

Since the client authentication during data communications replaces the authentication with ID/password which is well-known by users, it is highly demanded and above all, acceptant to users. While there are various ways of achieving digital authentication such as encrypted email, digital signatures, and the Virtual Private Network (VPN), SSL client authentication appears to be the most promising in terms of an authentication method accepted easily by users.

Furthermore, to make the basic functions of digital authentication easy to use for all users, it is crucial that user costs on certification be low, privacy be protected, and the means of certification be reliable.

4. FirstPass Digital Authentication Service

This chapter describes DoCoMo's FirstPass digital authentication service, which was launched on June 28, 2003.

4.1 Overview

The FirstPass service uses Public Key Infrastructure (PKI) [3][*2], a platform used extensively on the Internet. DoCoMo issues a client certificate to each FOMA subscriber and stores the certificate in each user's highly protected FOMA card.

Simpler and safer Internet access (SSL client authentication) is provided to a FOMA user that transmits this client certificate to a FirstPass-compatible CP compared with the past ID/password authentication in which multiple sets of IDs and passwords had to be managed for various services. The CP in this case need only to check the validity of the received certificate to proceed with the transaction. Compared with conventional password-oriented authentication, this system reduces the risk of impersonation by a third party (**Figure 1**).

Application and downloading a client certificate are both performed by a menu panel on a FirstPass-compatible FOMA terminal. In other words, FirstPass does away with troublesome procedures such as the sending of documents to confirm personal identity as usually required when applying for a PC-based certificate to a general PKI vender or service provider. This is because DoCoMo confirms personal identity when a user becomes a FOMA subscriber and issues a client certificate by linking with the customer database. All operations from application to downloading a client certificate can be performed from a FOMA terminal.

Because all client certificate function related to application, downloading to storage (in the FOMA card) and certificate usage is concentrated in FOMA terminals, reduced total cost, higher security and convnience can be achieved. The specific techniques used to accomplish these functions are described in another article of this special issue [4].

4.2 Obtaining a Client Certificate

Selecting "Client certificate operations" on the i-mode Menu of a FirstPass-compatible FOMA terminal connects the user with the FirstPass Center and enables the user to apply for issuance of a client certificate and to download the certificate (**Figure 2**).

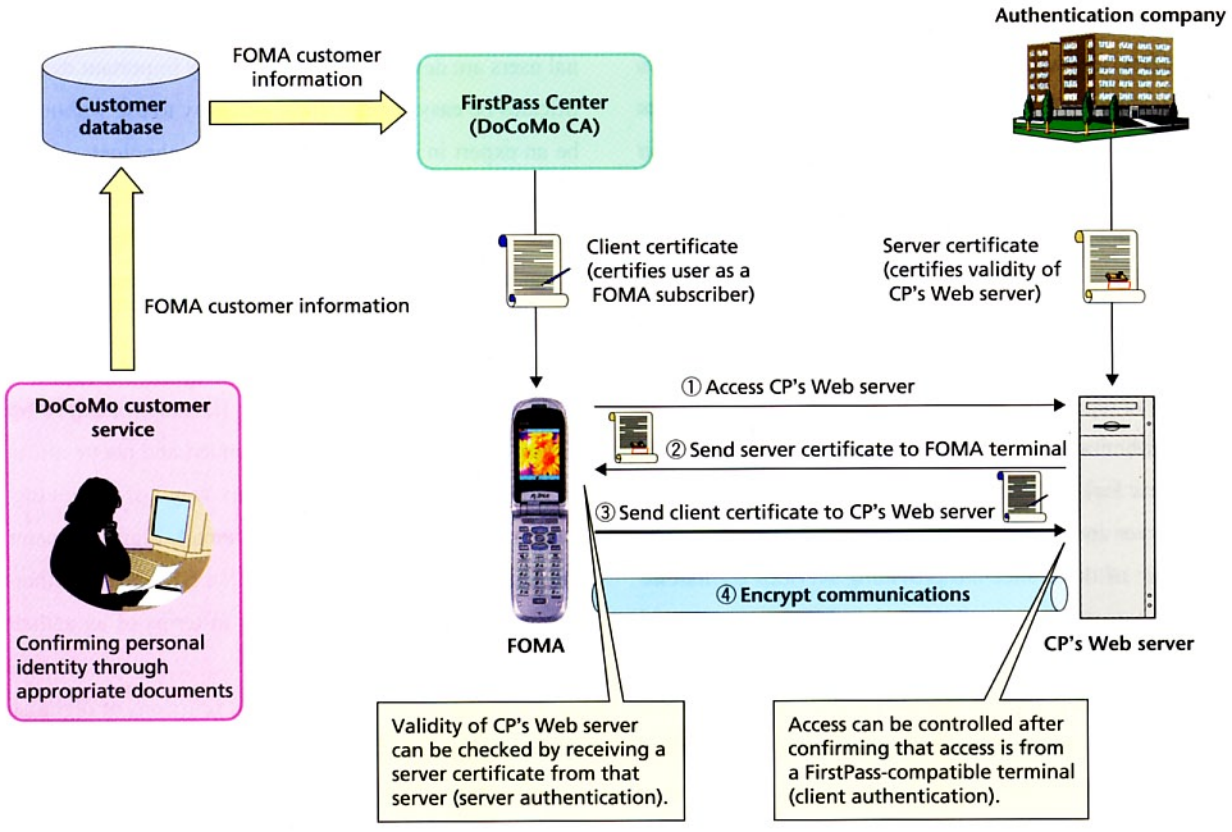

Figure 1 Service concept

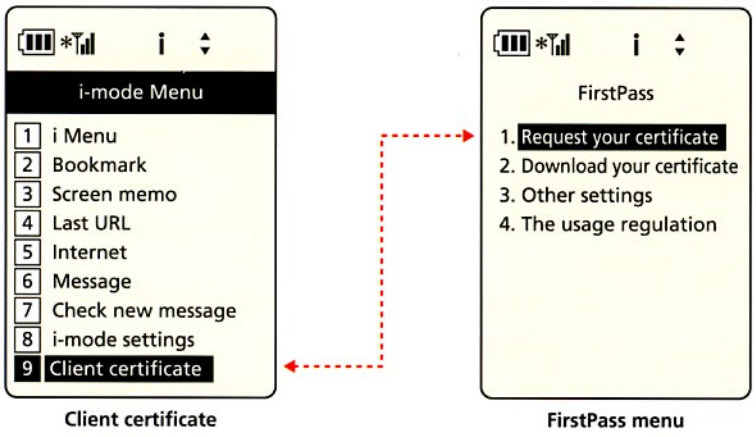

Figure 2 Operation for obtaining a client certificate

4.3 Client Certificate Revocation

To prevent the unauthorized use of a client certificate by a third party, FirstPass enables a client certificate to be revoked. Revocation can be performed through FOMA terminal operations as same as for obtaining a client certificate. The system is also being constructed to enable a user to request certificate revocation even when the FOMA card has been lost.

4.4 Issuance of Certificate Revocation List

A Certificate Revocation List (CRL) can be provided to a FirstPass-compatible CP. Information on client certificates for which revocation has been requested is centrally managed at the FirstPass Center, which issues one CRL daily. A CP can use this CRL to investigate whether the client certificate provided by a user at the time of access can be used. The CRL is defined as part of a PKI mechanism and can therefore be used immediately by existing Web servers.

4.5 SSL Client Authentication

After accessing a CP by a FOMA terminal on to which a client certificate has previously been downloaded, the user enters a Personal Identity Number (PIN) 2 code to enable use of SSL client authentication (**Figure 3**). The CP can then control access to the site based on the client certificate received at the time of SSL client authentication. Because this form of authentication uses standard Internet security technology, it can be applied to a variety of Web servers, applications, and authentication products.

A client certificate provided by FirstPass includes identification information unique to each FOMA subscriber. This information is conveyed to CPs in a fixed and safe manner for as long as the user is a FOMA subscriber, which is an effective method for service contents that require high reliability and continuity.

These techniques for mobile terminals are described in more detail in another article of this special issue [5].

5. Operation Method

5.1 FirstPass Operation Terms

Prime importance in providing FirstPass is that "client certificates not be issued and used improperly." The Certification Authority (CA) in this service is established on the basis of PKI security technology, an Internet standard, and operates in conformance with Request For Comments (RFC)-2527, which specifies facilities and operation standards/guidelines in relation to this technology [6]. In accordance with these standards and guidelines, FirstPass operation terms are publicly announced in the form of a Certification Practice Statement (CPS) and Certificate Policy. Extensive publicizing of these terms enables users and CPs to judge the reliability and safety of FirstPass. Almost all operating CAs, both government or private, issue a CPS for publicity.

To be more specific, establishing and publicizing the fol-

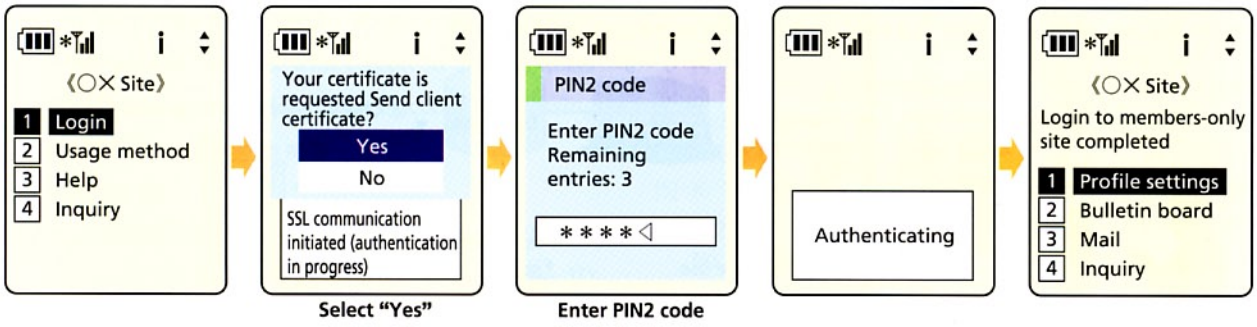

Figure 3 SSL client authentication procedure

lowing items enables users to judge the reliability and safety of an digital authentication service.

1) Service model: Types and targets of issued certificates.
2) Service levels: Reliability levels of issued certificates.
3) Operation procedures/system: Structure and rules for ensuring reliability.

5.2 Security Management Mechanisms

Physical access to the FirstPass Center is governed by several sophisticated security levels based on security policies used for critical DoCoMo communication facilities. Each of these security levels provides specific forms of protection in conjunction with agreements or equipment stipulated by that level. Specifically, entering and leaving a room are managed according to the importance of the security level, and identification and authentication at that time are performed using smart cards or biological authentication equipment and/or by detailed rules such as entering and leaving in groups of two or more people.

On the other hand, terminal (FOMA card) security is established in the following way. After the specialized equipment of manufacturer generates a set of keys (public keys and private keys) which are required for digital authentication, the keys are stored in the tamper-resistant[*3] FOMA card while the private key outside the card is simultaneously deleted thereby restricting the private key to the FOMA card. The user, meanwhile, need only to enter his or her PIN2 code to activate the private key on the FOMA card when applying for or using a client certificate. After using the private key in this manner, it will automatically enter a deactivation state preventing it from being improperly used.

6. Application Example of FirstPass Authentication

6.1 Application to Access Control and Related Issues

The FirstPass service makes it easier for a user to obtain a client certificate, and this in turn enables CPs to offer services that presume the use of FirstPass. A FirstPass client certificate, moreover, features robust security compared to the widely used ID/password method and therefore provides high usage value for CPs.

At the same time, it must be kept in mind that only a unique ID is stored in the client certificate issued by the FirstPass service as identification information. Thus, when applying FirstPass to login authentication as a usage model, the CP itself would need more than just the FirstPass ID for access control since ID is not the information that CP has assigned. In other words, user information (rights) must be added to the client certificate in order for the latter to be used by a CP. Two typical

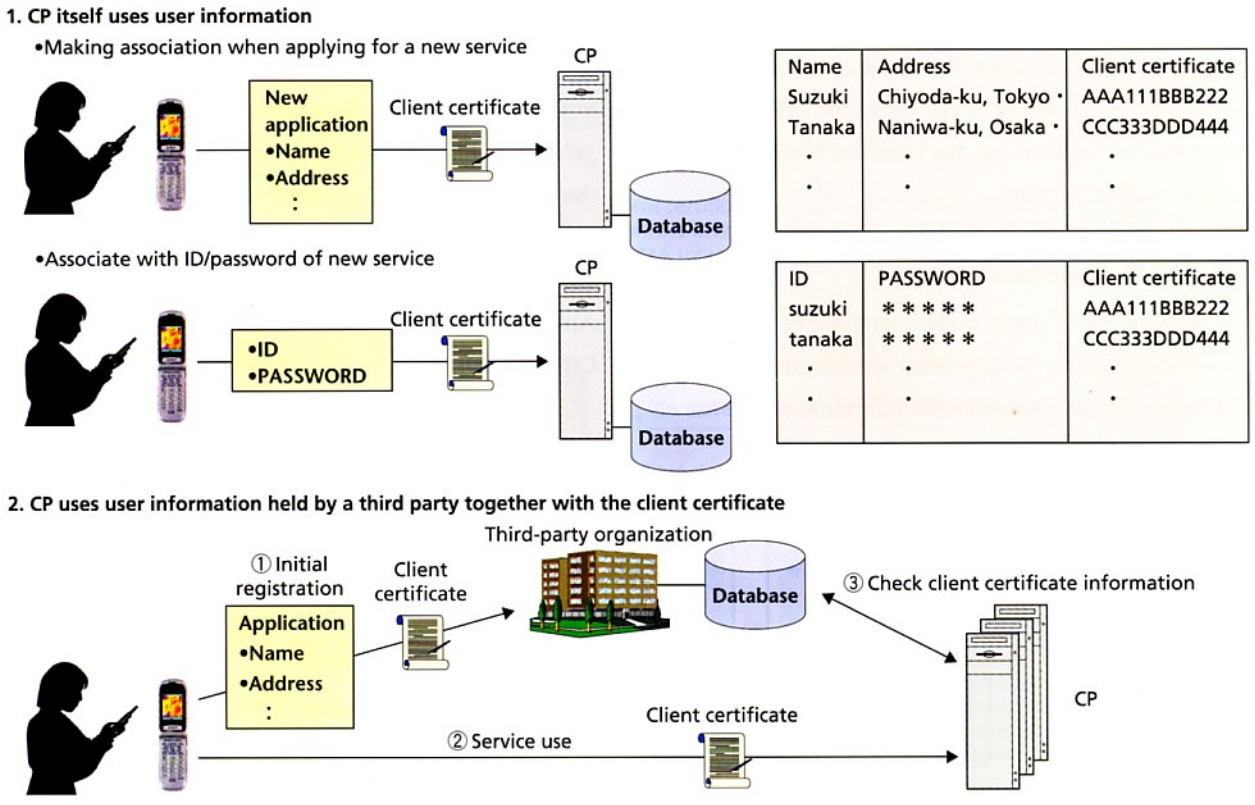

Figure 4 Associating user information with the client certificate

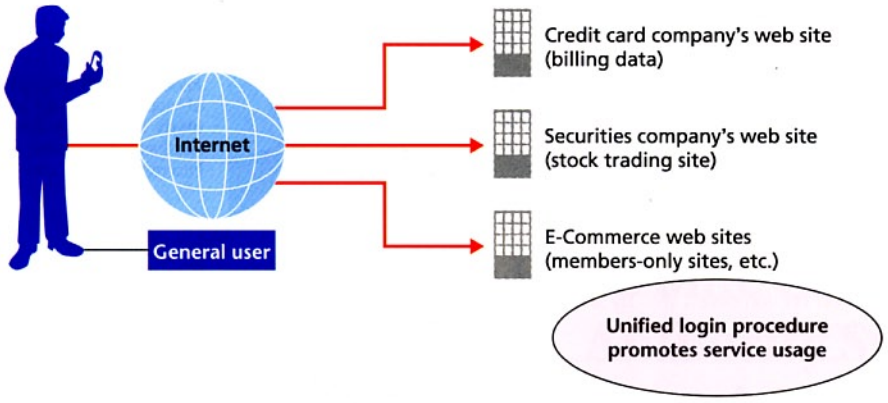

Figure 5 Login to a members-only site

methods for adding user information are shown in **Figure 4**. In the first method, the CP itself adds user information (rights) to the client certificate, while in the second method, the CP uses user information held by a third party together with the client certificate.

Adding user attribute information to the client certificate by such methods enable FirstPass to be used for access control making it a useful means of digital authentication for CPs. Furthermore, from the viewpoint of total CP operation cost, we can expect there to be more cases of using client certificates provided by FirstPass than certificates issued by CPs themselves. Here, it is important that client certificates satisfy the following conditions.

1) User operation of FOMA terminals must be made easier and more convenient (including access performance).
2) CP operation costs incurred by using FirstPass must be reduced.

6.2 Specific Usage Examples

1) Corporate Intranet

The i-appli function enables a user to send and receive data as needed to and from a server, and its use can reduce packet transmission fees. Therefore, i-appli is being used increasingly for accessing corporate intranets. In addition to the i-mode browser, FirstPass can be used with i-appli to communicate with servers. This makes a safer intranet access when using business applications in a mobile mode.

2) Members-only Site

FirstPass enables a user to access multiple sites including mobile-commerce and members-only sites with just one ID (**Figure 5**). In other words, a user no longer needs to remember an ID and password for each site. This should eliminate the situation in which a user gives up on accessing to use a service after forgetting an ID and password combination.

7. Conclusion

This article has described the background and contents of the FirstPass digital authentication service on the FOMA network, and has shown how it can be used to make mobile Internet services more convenient and safer to use.

To facilitate the construction of systems using FirstPass, DoCoMo is setting up an environment that will enable services featuring SSL-related products and single-sign-on products to be used in combination with Web servers. In the future, DoCoMo plans to make FirstPass even more convenient for FOMA users and to expand its range of application as a means of authentication for a wide variety of Internet services.

REFERENCES

[1] "Survey on Current State of Digital Signatures and Digital Authentication and Future Trends," Japan Information Processing Development Corporation, March 2002. [In Japanese]
[2] "Results of Survey on Market Scale of Digital Authentication Business," http://www.soumu.go.jp/s-news/2002/020412_2html, Ministry of Public Management, Home Affairs, Posts and Telecommunications, April 2002. [In Japanese]
[3] A. Arsenault and S. Turner: "Internet X.509 Public Key Infrastructure Roadmap", IETF draft-ietf-pkix-roadmap-09, IETF PKIX Working Group, July 2002.
[4] K. Sekino et al.: "Electronic Certification Authority System Construction Technology," NTT DoCoMo Technical Journal, Vol. 5, No. 3, PP.11–17, Dec. 2003.
[5] K. Takahashi et al.: "Technology for the Implementation of PKI Functions in Mobile Terminals," NTT DoCoMo Technical Journal, Vol. 5, No. 3, PP.18–23, Dec. 2003.
[6] S. Chokhani and W. Ford: "Internet X509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC2527, IETF Network Working Group, March 1999.

GLOSSARY

* 1 **SSL server authentication**: A form of authentication by which a third-party institution determines whether a server (domain) on the Internet is a real organization. Data transfers between the user and an authenticated server are encrypted.
* 2 **Public Key Infrastructure (PKI)**: A platform technology using public-key encryption techniques defined in IETF PKIX. It is often used as a basis for digital signatures and authentication systems that use digital certificates.
* 3 **Tamper-resistant**: Confidential information stored inside a device cannot be disclosed nor tampered with by anyone other than legitimate right holders.

ABBREVIATIONS

CA: Certification Authority
CP: Contents Provider
CPS: Certification Practice Statement
CRL: Certificate Revocation List
FOMA: Freedom Of Mobile multimedia Access
IMT-2000: International Mobile Telecommunications-2000
PDC: Personal Digital Cellular
PIN: Personal Identity Number
PKI: Public Key Infrastructure
RFC: Request For Comments
SSL: Secure Sockets Layer
UIM: User Identity Module
VPN: Virtual Private Network