New Technology Reports

Special Articles on FirstPass Digital Authentication Service

Electronic Certification Authority System Construction Technology

Kimihiko Sekino, Hiroshi Furuya, Fuminori Kihara,
Nobuyuki Oguri and Kenichiro Kawamoto

This article describes the development of an electronic certification authority system required for content provider to authenticate mobile terminal users on the basis of the public key cryptosystem.

1. Introduction

Certain authentication of the identity of communicating parties is essential to the implementation of electronic commerce (EC) and electronic applications in the information society. The main means of authentication are based on the public key cryptosystem. Actually, personal computers and Web servers come equipped with public key algorithms and functions for certificate storage as standard features. Furthermore, the establishment of a social infrastructure, including the enactment of electronic signature law and the distribution of national ID numbers as well as the beginning of specific authentication tasks, is proceeding steadily as a national policy, and is also gradually penetrating into the private sector. The infrastructure for use of the public key cryptosystem is referred to generically as the Public Key Infrastructure (PKI).

DoCoMo has equipped a Secure Socket Layer (SSL) communication function for encryption and server authentication based on the public key cryptosystem to i-mode mobile terminal models after 503i of the Personal Digital Cellular (PDC) system. Moreover, a client authentication function that allows Content Providers (CP) to perform authentication on the user side has been added, beginning with the F2102V and N2102V mobile terminals for Freedom Of Mobile multimedia Access

(FOMA). To accompany that, DoCoMo has developed the DoCoMo Certification Authority (CA), an electronic certification authority for issuing the certificates (user certificates) used for SSL client authentication.

This article covers the technology for constructing the electronic certification authority. Chapter 2, the background to construction of the DoCoMo CA and presents an overview of the DoCoMo CA. Chapter 3, the construction technology for the DoCoMo CA. Chapter 4, the items contained in the user certificates issued by the DoCoMo CA.

2. Background and DoCoMo CA Overview

2.1 Authentication by Certificate and the Role of the CA

1) Authentication Using Certificates

Authentication using electronic signatures, an application of the public key cryptosystem, is conducted in the following way. The sender of the document generates a message digest from the document that is to be sent. An electronic signature is generated by using a private key, which is possessed only by the sender, to compute the message digest. The electronic signature is attached to the document and the document is sent with the signature attached. The receiver of the document uses the sender's public key to verify the electronic signature attached to the document.

To determine that the sender is actually the person indicated by the electronic signature, it is necessary to prove that the sender manage the secret key. For that purpose, a certificate that proves the relationship between person and public key is issued by an organization known as Certification Authority (CA). The sender presents the certificate in addition to the document and electronic signature, thus allowing the receiver to confirm the sender's identity.

2) Role of the CA

For the CA to certify the relationship between the person and the public key, it becomes necessary to prove the relationship of the identity guarantee, the identity and public key. In most cases, the CA comprises a Registration Authority (RA) and an Issuing Authority (IA). The RA confirms the actual person's identity and guarantees the identity. Based on the identity guaranteed by the RA, the IA then certifies the relationship between the identity and the public key. For that purpose, a certificate that has an electronic signature generated using the private key of the IA is issued.

To generate a trustable electronic signature, the user must safely manage the private key. Furthermore, to issue a trustable certificate, the CA must guarantee a high level of security. By enabling this trustworthiness, a PKI is constructed to provide a safe means of authentication.

2.2 The DoCoMo Approach to PKI Design

The PKI is a concept that includes a variety of functions, such as certification of the user's identity, certification of attributes such as name and address, electronic signatures, and guarantee of time by a time stamp authority [1], [2]. In the development of this PKI, however, considering the priority on widespread use, we chose to offer as the basic function only SSL client authentication, anticipating use for intranet access and EC portals, etc.

Furthermore, because the DoCoMo CA is positioned as a network services for providing safe communications, the certificates issued by the DoCoMo CA are guaranteed by an ID based on the communication line contract. By doing so, our objective was to provide the same degree of safety in communications as for notification of ID within the network, even for Service Providers (SP) on the Internet, where there is no guarantee of communication path safety.

In the development of the system, we took heed of the advantages of DoCoMo and made use of the special features of the International Mobile Telecommunications-2000 (IMT-2000) network (tamper-resistant[*1] of the User Identity Module (UIM) and safety of network downloads, communication facilities, etc.) to solve various problems that have hindered widespread use of PKI in the past, such as IC card management, user management, the cost of certificate distribution, guaranteeing the safety of CA facilities, etc. (**Figure 1**).

2.3 Overview of the DoCoMo CA and Issues Concerned

Technical problems concerning construction of the DoCoMo PKI on the basis of the design approach described in section 2.2 are described here and an overview of the system is given.

1) User Registration and User Authentication

Generally, a CA will confirm the identity of the user in an office or other such place, register the data in the user database, and then issue a certificate. For user registration, proof of user

[*1] Tamper-resistant: Confidential information stored inside a device cannot be disclosed nor tampered with by anyone other than legitimate right holders.

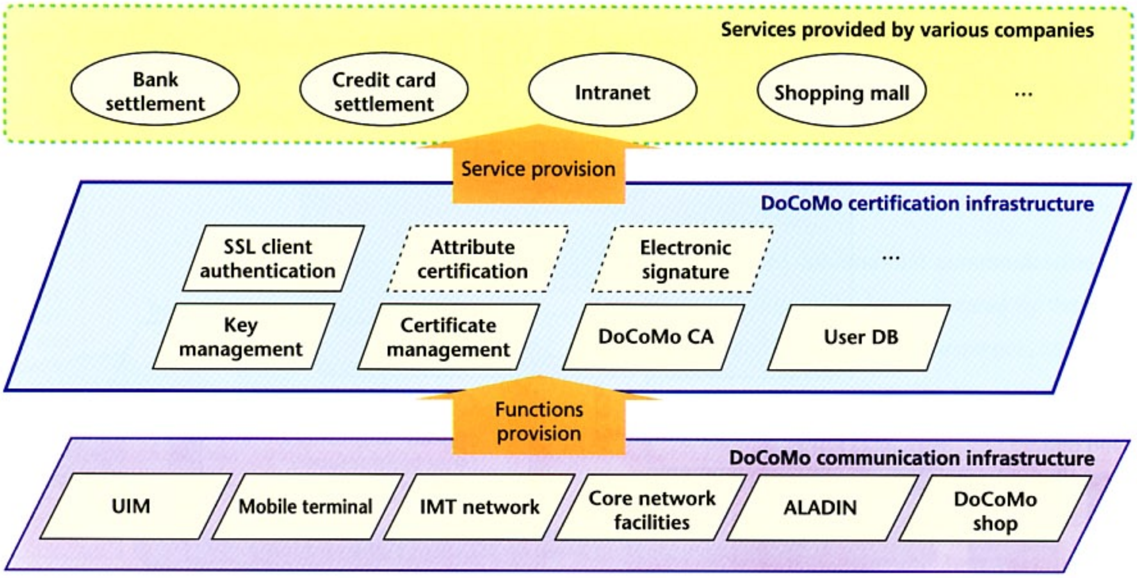

Figure 1 Conceptual diagram of the positioning of the DoCoMo certification platform

identity requires some bother, such as preparation of public documents. There is also a large cost incurred by the CA for maintaining the registration office and the construction and operation of the user database. The DoCoMo CA solves these problems, because the user identity confirmation procedure is completed at the time of the communication line contract and the data from the DoCoMo customer management system, ALl Around DoCoMo Information systems (ALADIN) is used when issuing the certificate. This process is described in detail in section 3.2.

2) Key and Certificate Status Management

The certificates issued by a CA in a conventional PKI are managed as user files. Furthermore, the certificate issuing processing (application forms, downloads, etc.) is mostly done via the fixed network. Accordingly, interruption of the issuing processing can be solved by retrying on the part of the user or other such means. The certificates issued by the DoCoMo CA, on the other hand, are provided as a means of offering safe mobile communications, and are managed within the UIM under the responsibility of DoCoMo. Furthermore, applications and downloads are done using the IMT network, so the possibility of a communication cut-off during processing is also high. Accordingly, recovery processing as a network function to cope with interruptions of processing is an important issue. The DoCoMo CA implements a method for continuing processing that has been interrupted by a break in communication after the connection has been reestablished by defining the keys status and certificates within the UIM. This is described in detail in section 3.3.

3) IA System Surveillance

As has already been mentioned, a high level of security is required of the IA that manages the private keys used to sign the certificates. As a means of ensuring that security, the IA generally accepts communication only from the RA, so remote surveillance of the two-way communication, which is the usual system surveillance method, cannot be applied. Considering convenience in maintenance however, it is necessary that the IA can be monitored remotely in the same way as other systems. For that purpose, we employed the asynchronicity of Simple Network Management Protocol (SNMP) traps to achieve remote surveillance through one-way communication. The details are described in section 3.4.

4) User Certificate Format and Contained Items

The user certificates issued by the DoCoMo CA are premised on use for EC portals on the Internet and other such purposes, so it is necessary to take connectivity to the Internet into consideration. Furthermore, a CA operated by the mobile operator must consider protection of user privacy and other such factors. We therefore specified the items contained in the user certificate issued by the DoCoMo CA so as to satisfy these requirements. This is described in detail in chapter 4.

3. DoCoMo CA Configuration Technology

3.1 Overall System Configuration

The overall configuration of the DoCoMo CA system is shown in **Figure 2**. The DoCoMo CA is located inside the

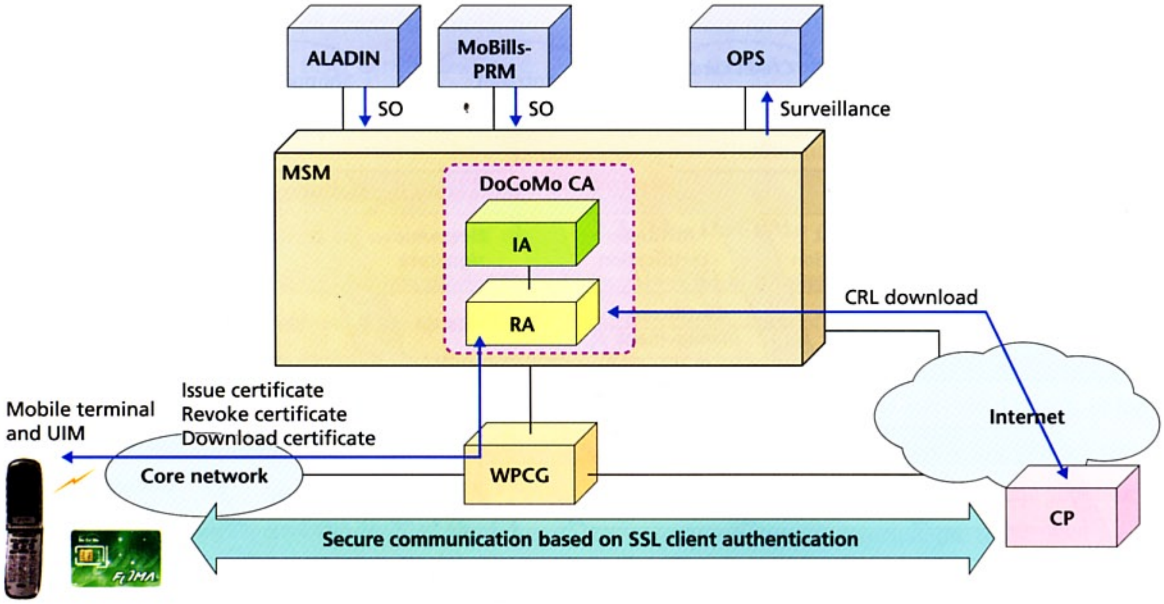

Figure 2 Overall system configuration

Multimedia Service Management (MSM), which is the service management layer of the Mobile MultiMedia Services Deployment Infrastructure (M^3In). It connects to the core network via a Wireless Protocol Conversion Gateway (WPCG). The user can operate the mobile terminal to access the DoCoMo CA, request the issuing of a certificate, download the certificate, and revoke the certificate. The CP is provided with the Certificate Revocation List (CRL) via the Internet. User information and CP information is obtained via connections with ALADIN and Mobile communication Billing systems card rating system-Partner Relationship Management system (MoBills-PRM). There is also a connection to OPeration Systems (OPS) to implement remote surveillance of the system.

The DoCoMo CA consists of an RA and an IA. When the user requests a certificate issuance, the RA receives the request and performs the inspection and registration. The registered request for issuance is sent to the IA, which performs the certificate issuance processing. The issued user certificates are managed by the RA and stored in the UIM when the user performs the download operation.

Furthermore, the CRL is provided only to registered CPs, so access control is performed on the basis of the company information obtained from MoBills-PRM.

3.2 User Registration and Authentication

The RA makes use of the ALADIN information to judge the validity of the user's UIM and then performs the registration [3]. This process is described in detail below.

When the user contracts for a new FOMA line, the Mobile Station Integrated Services Digital Network number (MSISDN) and UIM manufacturer's serial number that are registered in ALADIN are at the same time sent to the DoCoMo CA, where they are stored as user information. Next, if a user requesting issuance of a certificate accesses the DoCoMo CA, the manufacturer's serial number is automatically sent by the UIM on command from the RA. At this time, the MSISDN attached to the HyperText Transfer Protocol (HTTP) header by the WPCG is also obtained. With this MSISDN as a key, the RA compares the serial number obtained from the UIM and the serial number previously stored by the DoCoMo CA. In this way, the UIM of the user that has accessed the DoCoMo CA can be confirmed to be a legitimate DoCoMo UIM that is contracted for FOMA. That is to say, if a FOMA line contract is in effect, the user can request the issuance of a certificate without having to have registered formally at an office or other place and without having to enter user information from the mobile terminal (**Figure 3**).

3.3 Key and Certificate Status Management

Here we explain in detail the method that enables the restarting of process upon reconnection by management of the key status and certificate within the UIM [3]. There are four states defined for a key; 'in operation', 'key generated', 'certificate requested', and 'certificate stored'. Six states are defined for a certificate: 'not issued', 'issuance request in progress',

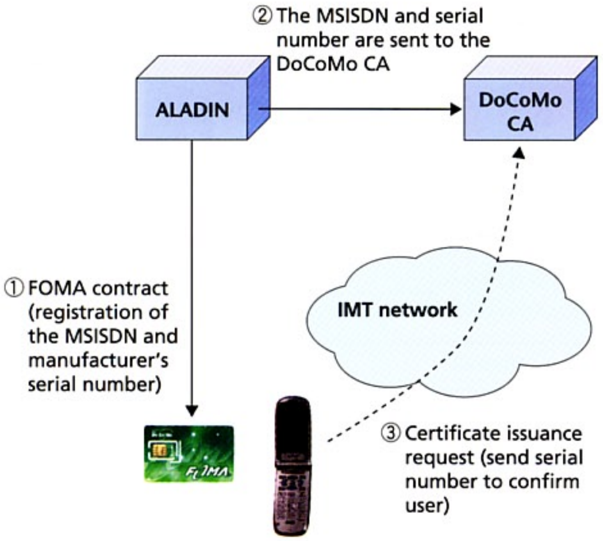
② The MSISDN and serial number are sent to the DoCoMo CA
ALADIN
DoCoMo CA
① FOMA contract (registration of the MSISDN and manufacturer's serial number)
IMT network
③ Certificate issuance request (send serial number to confirm user)
FOMA

Figure 3 User registration and user authentication

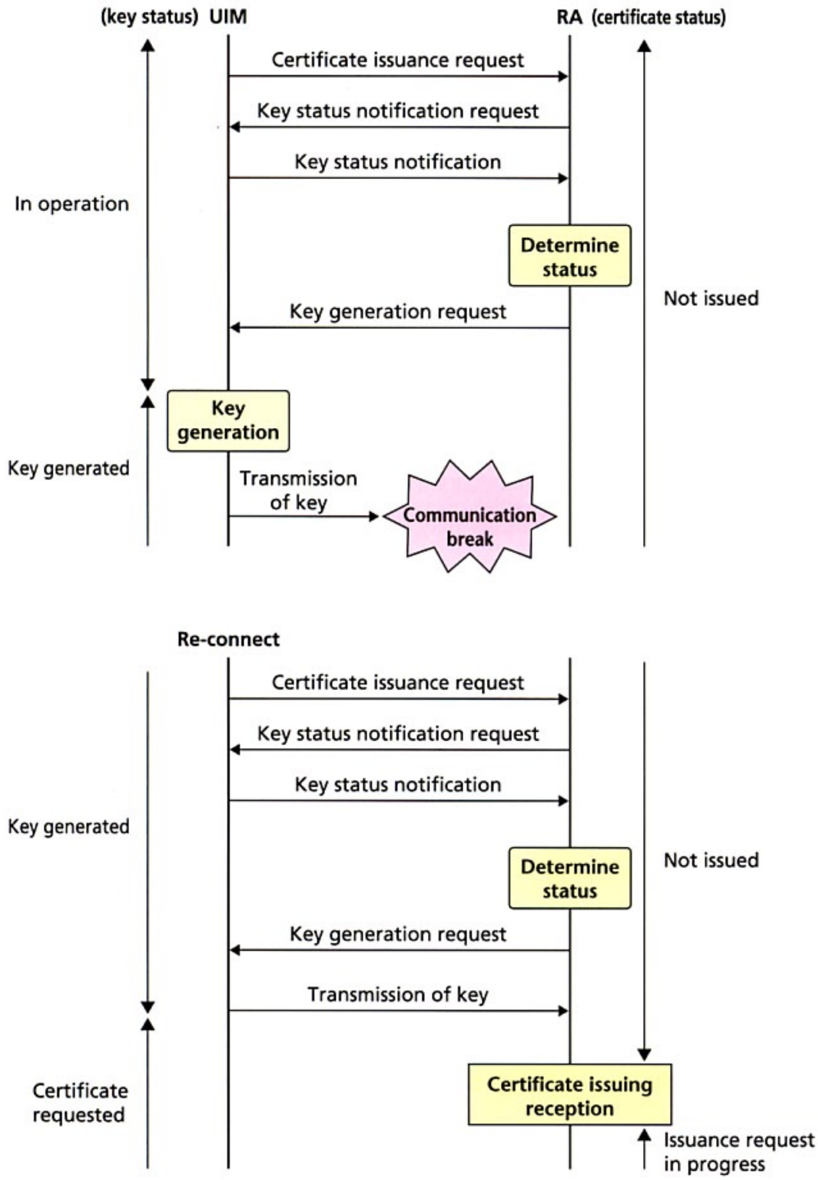

Figure 4 Status management in the certificate issuance request sequence

'issued but download not completed', 'downloaded', 'revocation request in progress', and 'revoked'. Transitions are made between states according to each certificate request, download and revocation processing sequence, so the point at which the processing sequence was interrupted can be determined by referring to this status.

As an example, assume that communication is interrupted during transmission of the key generated by the UIM to the RA in the certificate issuance request sequence, as shown in **Figure 4**. At the time of reconnection, the key status is 'key generated' and the certificate status is 'not issued', so the processing can be continued by sending the generated key to the RA.

Management of the keys status and certificates in the way described above makes it possible to shorten the user's communication wait time and make effective use of the key stored in the UIM.

3.4 IA System Surveillance

A method for remote surveillance of the IA by means of one-way communication using SNMP traps[*2] is explained in detail below. As shown in **Figure 5**, polling conducted by the department management server installed at the IA allows collection of failure information on the server hardware, OS, applications, etc. The management server converts the collected failure information to SNMP trap format and sends it to the OPS.

The SNMP trap is an interface that has a function for one-way notification of failures that is supported by existing OPS.

Using this approach, remote surveillance that maintains the level of security can be realized without modification of the existing OPS interface, allowing large-screen monitoring at the operation center in

[*2] SNMP trap: An asynchronous message that can be sent from an agent to a manager and is used mainly to inform of facility abnormalities and recovery.

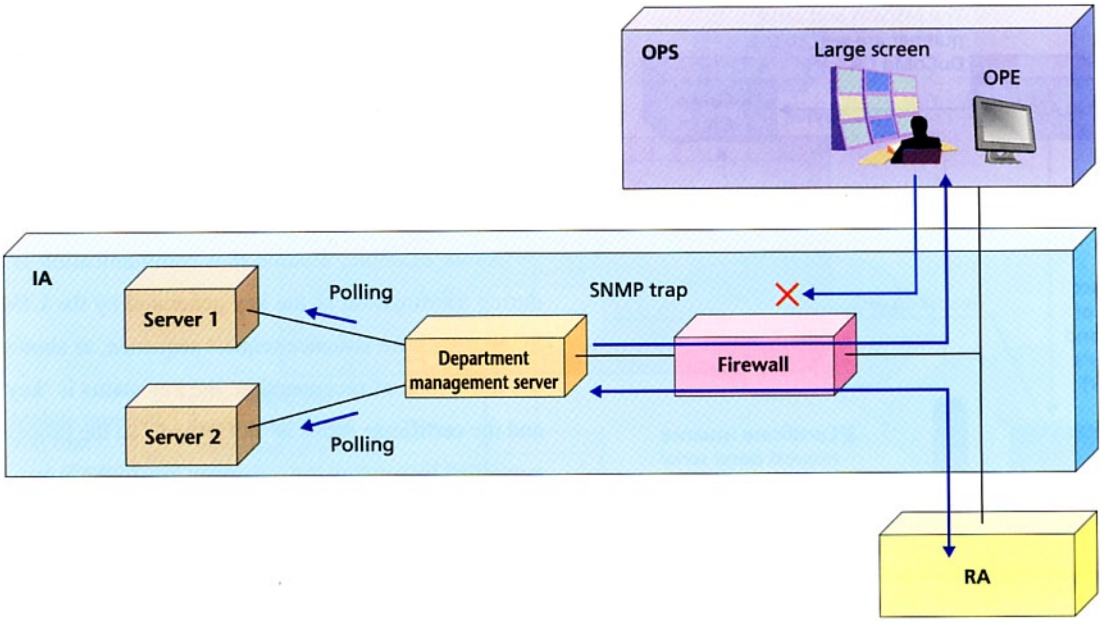

Figure 5 IA system surveillance

the same way as for conventional systems.

4. Items in the User Certificate

The International Telecommunication Union-Telecommunication standardizations sector (ITU-T) standard for certificates used on the Internet is specified as X.509 [4]. The certificates issued by the DoCoMo CA were designed to conform to X.509, considering connectivity to the Internet. The X.509 certificate profile contains the subject, validity, serial number, signature, etc. In this chapter, we describe the policy for specifying the subject and the validity in the user certificates issued by the DoCoMo CA.

4.1 Subject

In the certificate, the ID is written in the subject field for verification of the ID. Generally, the name, telephone number, serial number and other such information is considered for use as the ID, but it was necessary to take user privacy and ID continuity when the mobile operator certifies the ID.

To protect user privacy, the DoCoMo CA does not publish the information registered when the line contract is concluded, and continuity of ID is ensured by using an ID that does not change, even if the telephone number or mobile terminal is changed. Therefore, the ID certified by the DoCoMo CA is different from the telephone number that is assigned in the FOMA contract.

4.2 Validity

Many CAs set the validity period for the user certificate to one year. Updating every year was considered to be necessary because of changes in the user information contained in the user certificate.

One UIM limits the number of certificate issuance to five, so it is necessary for DoCoMo CA to extend the validity period of the user certificate. Furthermore, it is possible to extend the validity period because the ID written in the user certificate does not contain user information. On the other hand, extending the validity may increase the size of the CRL tremendously. As the result of taking an overall view of these points, we set the validity of the user certificate to two years.

5. Conclusion

FirstPass is Japan's first commercial service for performing authentication for mobile communications by adopting a PKI. Currently, we are tackling with introduction of services that make use of the DoCoMo CA and doing technological studies on "expanding the usage case", in which the same ID is used for authentication in various scenes.

In future work, we intend to make use of the safe facilities and operating expertise achieved in this work to extend the fundamental functions and develop the 2nd Generation PKI, which will be integrated with Web services on the Internet.

REFERENCES

[1] A. Arsenault and S. Turner. "Internet X.509 Public Key Infrastructure: Roadmap", IETF draft-ietf-pkix-road,ap-09, IETF PKIX Working Group, Jul.2002.

[2] R. Shirey: "Internet Security Glossary", RFC2828, IETF Network Working Group, May. 2000.

[3] K. Kawamoto and N. Nakamura: "Study of Management on the Mobile Public Key Infrastructure", NOMS2002, Apr. 2002.

[4] ITU-T Recommendation X.509: "Information Technology-Open System Interconnection-The Directory Authentication Framework", Jun. 1997.

ABBREVIATIONS

ALADIN: ALl Around DoCoMo INformation systems
CA: Certification Authority
CP: Contents Provider
CRL: Certificate Revocation List
EC: Electronic Commerce
FOMA: Freedom Of Mobile multimedia Access
HTTP: HyperText Transfer Protocol
IA: Issuing Authority
IMT-2000: International Mobile Telecommunications-2000
ITU-T: International Telecommunication Union-Telecommunication standardization sector
M^3In: Mobile MultiMedia services deployment Infrastructure
MoBills-PRM: Moble communication Billing systems card rating system-Partner Relationship Management system
MSISDN: Mobile Station Integrated Services Digital Network number
MSM: Multimedia Service Management
OPS: OPeration Systems
PDC: Personal Digital Cellular
PKI: Public Key Infrastructure
RA: Registration Authority
SNMP: Simple Network Management Protocol
SO: Service Order
SP: Service Provider
SSL: Secure Sockets Layer
WPCG: Wireless Protocol Conversion Gateway