INTERNATIONAL TELECOMMUNICATION UNION

ITU-T X.1122

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(04/2004)

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

Telecommunication security

Guideline for implementing secure mobile systems based on PKI

ITU-T Recommendation X.1122

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation X.1122

Guideline for implementing secure mobile systems based on PKI

Summary

Although public-key infrastructure (PKI) technology is very useful security technology to realize many security functions (encipherment, digital signature, data integrity, and so on) in the mobile end-to-end data communications, the PKI technology should be adapted for mobile end-to-end data communication. However, the method to construct and manage secure mobile systems based on PKI technology has not been established yet. This Recommendation provides guidelines for constructing secure mobile systems based on PKI technology.

Source

ITU-T Recommendation X.1122 was approved on 29 April 2004 by ITU-T Study Group 17 (2001-2004) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation X.1122

Guideline for implementing secure mobile systems based on PKI

1 Scope

This Recommendation shows the guideline when constructing secure mobile systems based on PKI technology. The range of applications of this Recommendation shall be as follows:

- Its subject shall be the control of certificates in the mobile end-to-end data communication in general.
- However, defining a method of mobile settlement as a settlement model shall be excluded from the area of application of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

– ITU-T Recommendation F.116 (2000), *Service features and operational provisions in IMT-2000*.

– ITU-T Recommendation Q.814 (2000), *Specification of an electronic data interchange interactive agent*.

– ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks*.

– ITU-T Recommendation Q.1711 (1999), *Network functional model for IMT-2000*.

– ITU-T Recommendation Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems*.

– ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

– ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

– ITU-T Recommendation X.842 (2000) | ISO/IEC TR 14516:2002, *Information technology – Security techniques – Guidelines for the use and management of trusted third party services*.

– ITU-T Recommendation X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

3 Terms and definitions

3.1 Public-key and attribute certificate framework definitions

The following terms are defined in ITU-T Rec. X.509 | ISO/IEC 9594-8:

a) Attribute Authority;

b) Attribute Certificate;

c) Certification Authority (CA);

d) Certificate Revocation List (CRL);

e) Public-key;

f) Public-key certificate (Certificate);

g) Public Key Infrastructure (PKI).

3.2 OSI Reference Model security architecture definitions

The following terms are defined in ITU-T Rec. X.800 | ISO/IEC 7498-2:

a) authentication information;

b) confidentiality;

c) cryptography;

d) key;

e) password.

3.3 Guidelines for the use and management of trusted third party services definitions

The following term is defined in ITU-T Rec. X.842 | ISO/IEC TR 14516:

a) Registration Authority.

3.4 Service features and operational provisions in IMT-2000 definitions

The following term is defined in ITU-T Rec. F.116:

a) User Identity Module.

3.5 Additional definitions

This Recommendation defines the following terms:

3.5.1 secure mobile system: A system to realize secure mobile end-to-end data communication between mobile user and ASP or between mobile users.

3.5.2 certificate repository: A database in which the certificates, CRL and other PKI-related information are stored and which is accessible online.

3.5.3 validation authority: An authority that provides an online service of verification of a certificate's validity. It establishes a verification certificate path from a signer to a user who wishes to confirm the validity of the signature of the signer, and confirms whether all the certificates contained in the verification certificate path are reliable or not revoked. It also verifies if a certificate has been revoked.

4 Abbreviations

This Recommendation uses the following abbreviations:

AA Attribute Authority

ASP Application Service Provider

CA Certification Authority

CMC Certificate Management over CMS

CMP Certificate Management Protocol

CRL Certificate Revocation List

ID Identifier

PIN Personal Identification Number

PKI Public-Key Infrastructure

POP Proof Of Possession

RA Registration Authority

RSA RSA public key algorithm

TLS Transport Layer Security

UIM User Identity Module

VA Validation Authority

5 Categories to which PKI technologies belong

PKI technology is the security technology that is applied to the relation between a mobile terminal and an application server in the general model of mobile end-to-end data communication between a mobile user and an ASP, or to the relation between a mobile terminal and a mobile security gateway, and between a mobile security gateway and a server in the gateway model of mobile end-to-end data communication between a mobile user and an ASP.

PKI technology is a security technology that is used to realize the following security functions:

1) Encipherment;
2) Key Exchange;
3) Digital Signature;
4) Access Control;
5) Data Integrity;
6) Authentication Exchange;
7) Notarization.

Table 1/X.1122 – Functions and places to which PKI technology is applied

Places to which technologies apply / Functions realized by technologies	Mobile terminal	Application server/Mobile security gateway	Relation between mobile user and mobile terminal	Relation between mobile terminal and application server or other relations
Encipherment				X
Key Exchange				X
Digital Signature				X
Access Control				X
Data Integrity				X
Authentication Exchange				X
Notarization				X

Although PKI technology is often used in an open network to realize the above-mentioned security functions, due to characteristics of mobile end-to-end data communication, especially low processing power and small memory size, some adaptations of PKI technologies for mobile end-to-end data communication are needed.

6 Models of secure mobile systems based on PKI

As for other secure mobile systems, models of secure mobile systems based on PKI are classified as follows: a general model of secure mobile systems based on PKI for communication between a mobile user and an ASP, and a gateway model of secure mobile systems based on PKI for communication between a mobile user and an ASP.

However, for the purpose of PKI operations (for example, life cycle management of certificate), some entities (CA, RA, VA, Repository and so on) are added into the models.

6.1 General model of secure mobile systems based on PKI

A general model of secure mobile systems based on PKI for communication between a mobile user and an ASP is shown in Figure 1.

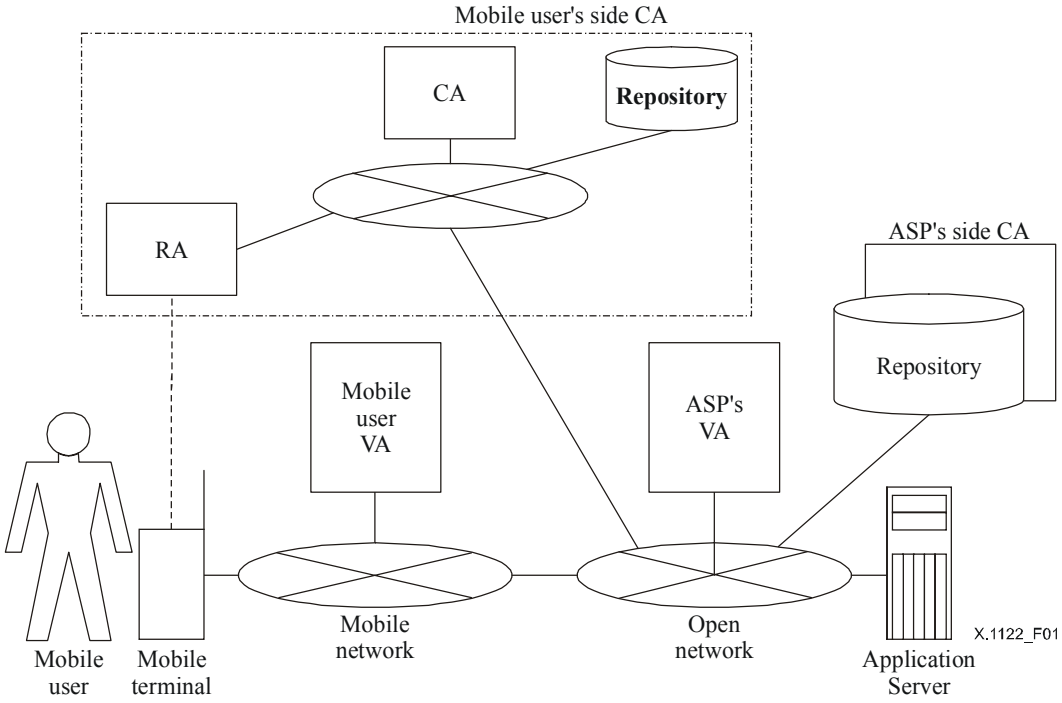

Figure 1/X.1122 – General model of secure mobile systems based on PKI

This model contains additional entities to that of the general model of mobile end-to-end data communication between a mobile user and an ASP; i.e., the mobile user's side CA (contains RA and repository), mobile user's VA, ASP's side CA and ASP's VA.

– *Mobile user's CA*

  The mobile user's side CA issues and manages the mobile user's certificate or the mobile terminal's certificate. This contains RA that is responsible for the identification and authentication of the mobile user and the repository that stores the mobile user's certificate and CRL.

– *Mobile user's VA*

  The mobile user's VA provides an online service of verification of validity of certificate received by mobile user to mobile user.

– *ASP's side CA*

  An ASP's side CA issues and manages the ASP's certificate or application server's certificate. This also contains RA that is responsible for the identification and authentication of the ASP and the repository that stores the ASP's certificate and CRL.

– *ASP's VA*

  The ASP's VA provides an online service of verification of validity of certificate received by the ASP.

6.2 Gateway model of secure mobile systems based on PKI

A gateway model of secure mobile systems, based on PKI for communication between mobile user and an ASP is shown in Figure 2.

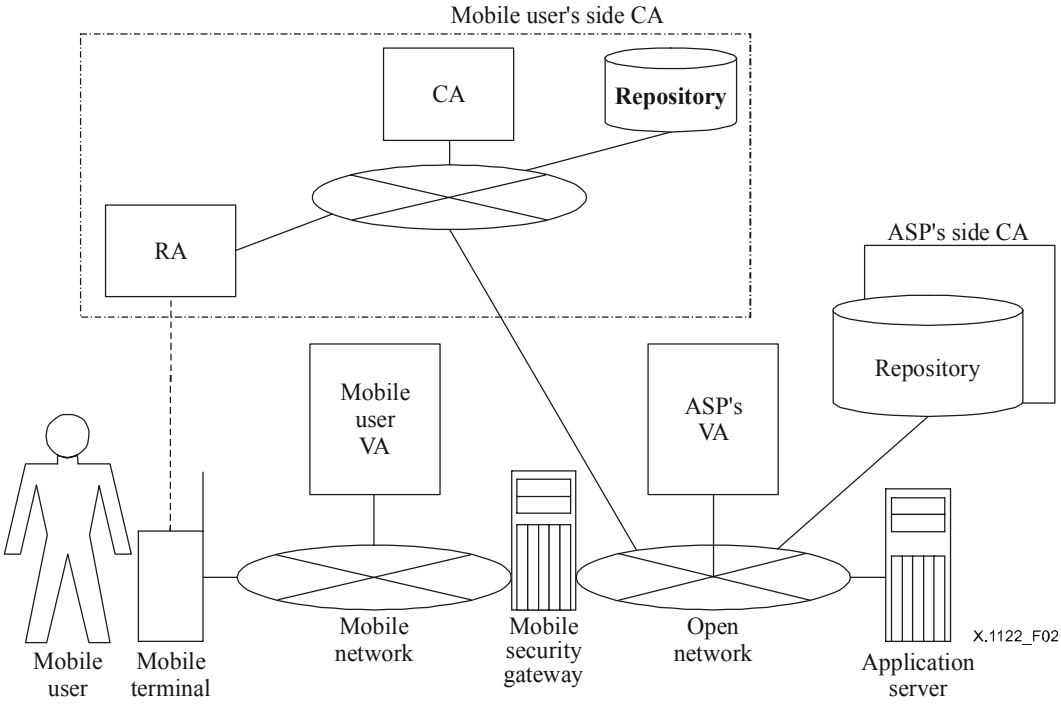

Figure 2/X.1122 – Gateway model of secure mobile systems based on PKI

Like the general model of secure mobile systems, based on the PKI for communication between a mobile user and an ASP, this model contains additional entities to that of the gateway model of mobile end-to-end data communication between a mobile user and an ASP; i.e., the mobile user's side CA (contains RA and repository), the mobile user's VA, the ASP's side CA and VA.

7 PKI operations for mobile end-to-end data communication

7.1 PKI operations related to the life cycle of the certificate

The general life cycle of the certificate is as follows:

1) Generation of a pair of private and public keys;
2) Application, issuance and activation of the certificate;
3) Utilization of the certificate;
4) Revocation of the certificate; and
5) Renewing the certificate.

7.1.1 Generation of the pair of private and public keys

For the generation of a pair of private and public keys, different models exist depending on who generates the key or where the key is generated.

7.1.1.1 Which entity generates the keys

Although the model in which the mobile user generates the keys is desired from the security point of view, there can be a model in which the CA generates the keys instead of the mobile user, and a model in which a third party generates the keys.

For models in which a third party processes the keys, there is a model where the user purchases the device in which the keys are installed. (The device might be a mobile terminal itself or it might be a component attached to the mobile terminal.) In this case, the manufacturer of the device is the producer of the key.

7.1.1.2 Where are the keys generated

There can be models in which the keys are generated in the device, and models in which the keys are generated outside the device and installed into the device.

7.1.2 Application for, issuance and activation of the certificate

For application, issuance and activation of the certificate, different models exist depending on whether the application, issuance and activation are done online or offline at each step.

There are cases where the certificate is deemed activated upon issuance of the certificate.

The model that should be selected depends on the person to whom the certificate is issued (mobile user), issuer (CA), what the certificate guarantees, and purpose of utilization of the certificate, and so on.

Furthermore, in the mobile environment, the models are different depending on the relationship between the timing of:

a) Generating the keys;

b) Issuing the certificate;

c) Activating the certificate; and

d) Obtaining the device.

7.1.2.1 Model in which the device is obtained after the certificate has been activated (model in which the order of the above items is (a)→(b)→(c)→(d))

This model corresponds to the case where the mobile user purchases a device in which the keys and the certificate have been previously installed. In this model, it is possible to sell a device that has previously installed the certificate having the subject that is not tied to the mobile user (e.g., when the device is a mobile terminal, the telephone number or some electronic serial number may be used as the subject), or to install the certificate at the shop-counter at the time of purchasing the device (e.g., the certificate is processed and installed based on the application information at the time of applying for a device). In this case, the timing of (b), (c) and (d) are desired to occur simultaneously.

7.1.2.2 Model in which a user obtains a device in which the certificate has been issued (model in which the order is (a)→(b)→(d)→(c))

This is basically the same as the above-mentioned model, but a procedure of activating the certificate is necessary after having obtained the device. It is desirable to keep the time interval between timing of (b) and (d) short.

7.1.2.3 Model in which a user obtains a device that stores only the keys (model in which the order is (a)→(d)→(b)→(c))

A model that corresponds to a case where the user applies for the certificate online after having purchased a device installed with the keys.

7.1.2.4 Model in which a user obtains a device that is not installed with any keys and certificates (model in which the order is (d)→(a)→(b)→(c))

In this model, the user generates the keys and applies for a certificate after having purchased the device. This is a model which provides privacy of the private key of a mobile terminal. But, it is required to have more computation capability, memory storage, and processing time to produce the keys in the device.

7.1.3 Utilization of the certificate

7.1.3.1 Signer

The signer associates his/her certificate with the signed message and sends it to the verifier. There are different models depending on the method of association (such as attaching the certificate to the message and attaching the place of the repository).

7.1.3.2 Verifier

In the verification of the authenticity of the message received from the signer, the following processes are required to be performed:

1) *Verification of the validity of the certificate*

   This is to verify the authenticity of the certificate of the signer. Concretely, the discovery of an authentication path of the certificate and the verification of the validity of each certificate in the authentication path.

   Depending on the method of verification, the following two models are available:

   a) *Model in which the verifier verifies by him/herself*

      At the time of verification, the verifier discovers an authentication path and verifies the validity of each certificate in the authentication path.

      For the verification of each certificate, the verifier verifies the validity of the certificate by acquiring the CRL from the repository of the CA, or by inquiring to the CA which provides the status information of the certificates online, or otherwise.

      Note that the frequency of the acquisitions of the CRL, or inquiries to the CA, depends on the use and importance of the certificate (in principle, necessary each time the certificate is verified).

   b) *Model in which a reliable verification authority (VA) is used*

      An inquiry as to whether the certificate associated with the message is valid is made to the VA, and the actual verification process (discovering an authentication path and verifying the validity of each certificate) is carried out by the VA.

      Short-lived certificate, or other, might omit this process.

2) *Verification of the signature affixed to a message*

   This is to verify whether or not the signature affixed to a message is authentic.

   It is often the case that the verifier him/herself verifies a signature using the public key in the certificate, but there are models in which the VA does it.

7.1.4 Revocation of the certificate

This is to apply for the revocation of the certificate to the CA and revokes the certificate. Depending on the method of application, there are two models for the revocation of the certificate: i.e., a model in which the revocation request is made online, and a model in which the revocation request is made offline.

7.1.5 Renewing the certificate

This is to revoke an existing certificate, to generate a new pair of the keys and to receive a new certificate issued by the CA. Basically, the revocation application and issuance of a certificate are made in succession, but the models are different depending on the order of the processes and whether or not (the information of) the existing certificate is used in the application for the new certificate.

8 The usage model in telecommunication services

This clause indicates the usage model that will become available by using the PKI.

There are two types of usage models: an over-the-session-layer usage model and an application layer usage model. The over-the-session-layer usage model is a model that provides the functions of encrypted communications, authentication and data integrity over the session layer in the OSI reference model (such as TLS). The application layer usage model is a model that provides the functions of integrity and confidentiality on the application layer.

Many existing implementations of the over-the-session-layer usage model (TLS is famous for its implementations) are designed to provide a secure end-to-end transportation and to provide a secure tunnel between a server and a client. Therefore, client and server can authorize each other, and these authentications can be realized by using PKI.

The over-the-session-layer usage model is based on the following security functions:

- Server authentication;
- Client authentication;
- Communication path encryption and integrity.

The application layer usage model is based on the following security functions:

- The digital signature function on the application level (for integrity and authentication);
- The data encryption function on the application level (for confidentiality).

Other than the above, a network layer usage model may also be possible.

8.1 Functions to be realized in the over-the-session-layer usage model

The over-the-session-layer usage model provides the following functions: the server authentication function, client authentication function and communication path encryption and integrity function (actually, it will be realized by a combination of the server authentication function and communication path encryption and integrity function, or a combination of the server authentication function, client authentication function and communication path encryption and integrity function). The implementations of this usage model (such as TLS) can be used in the mobile end-to-end data communication to provide the authentication of both a mobile terminal and an application server and to make a secure tunnel between two end-points. The certificate plays a very important role in this usage model. Therefore, it is important to specify procedure to issue, revoke, or suspend the certificate and authentication method for a user and a server.

8.1.1 Server authentication in the over-the-session-layer usage model

Because there are two models for secure mobile systems based on PKI, as mentioned in clause 6, there are two types of server authentication in this usage model; one is server authentication in the general model and another is server authentication in the gateway model.

In the server authentication in the general model, the mobile terminal verifies the application server by verifying the certificate presented by the application server and digital signature on received message during a handshake procedure.

The server authentication in the general model is executed in accordance with the following procedures:

- The application server sends its certificate and the relevant authentication information to the mobile terminal.
- The mobile terminal verifies whether the certificate is issued by the CA, which the mobile terminal trusts.

- The mobile terminal verifies the validity of received authentication information using the public key in the certificate of the application server.
- At the same time, the mobile terminal determines whether it is definitely the correct application server to which the mobile terminal wishes to gain access.

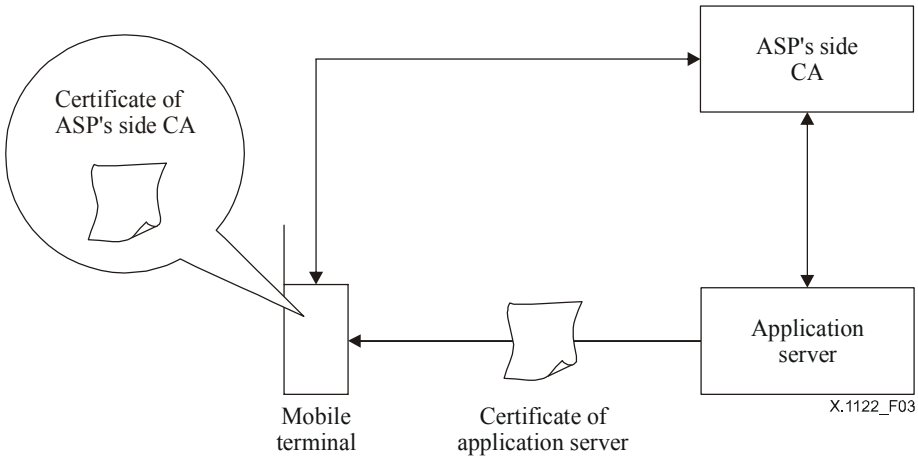

Figure 3/X.1122 – Server authentication in the general model

The server authentication in the gateway model performs double-phase authentication between the mobile terminal and the mobile security gateway and between the mobile security gateway and the application server.

The double-phase server authentication is executed in accordance with the following procedures:

- Firstly, a protected session is established between the mobile terminal and the mobile security gateway by using the certificate of the mobile security gateway.
- Then, a protected session is also established between the mobile security gateway and the application server.

Thus, in the double-phase server authentication, the mobile security gateway must be able to convert the protected session between the mobile terminal and the mobile security gateway appropriately into the protected session between the mobile security gateway and the application server.

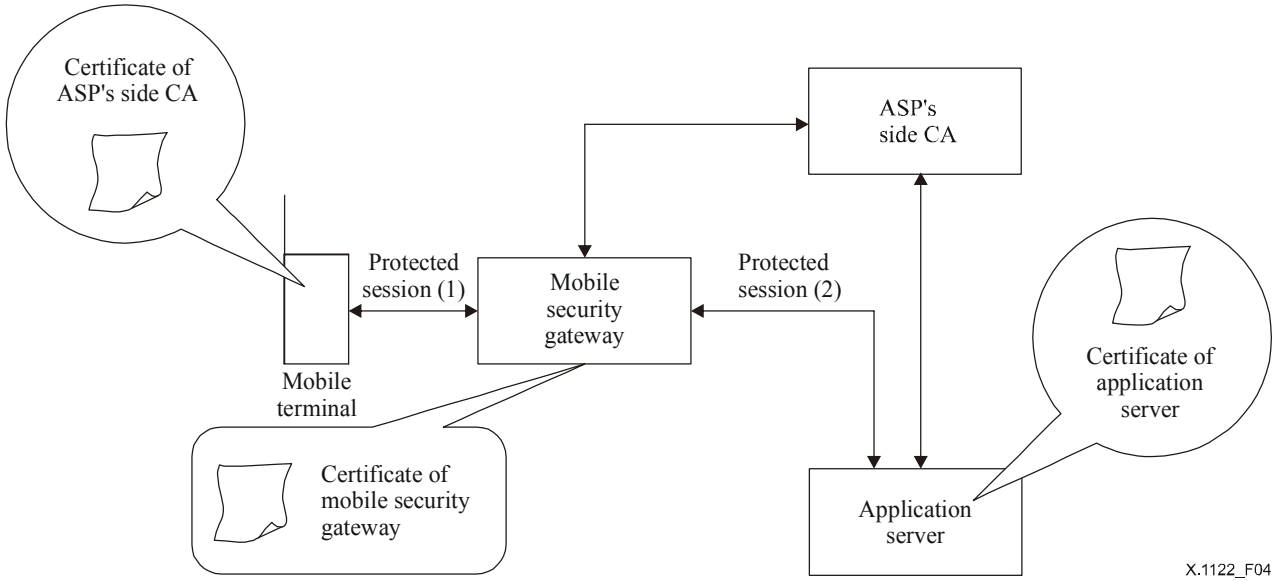

Figure 4/X.1122 – Server authentication in the gateway model

8.1.2 Client authentication in the over-the-session-layer usage model

In the client authentication in the over-the-session-layer usage model, the mobile terminal presents the certificate and the relevant authentication information to the application server responding to the request of the application server, and the application server executes the client authentication.

The client authentication in this usage model is executed in accordance with the following procedures:

- The mobile terminal sends the certificate to the application server.
- At the same time, the mobile terminal sends the signed verification message (created with the clients' private key) to the application server.
- The application server verifies the certificate of the mobile terminal.
- Furthermore, the application server decrypts and verifies the certificate verification message with the public key in the certificate.

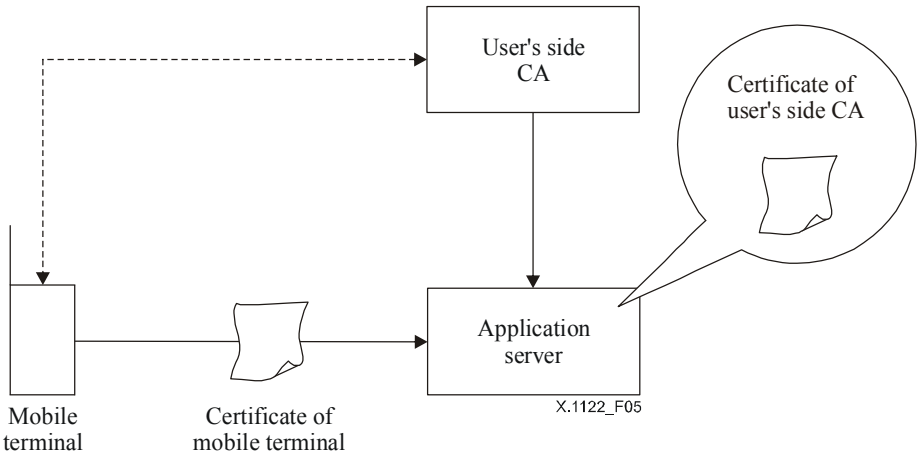

Figure 5/X.1122 – Client authentication in the over-the-session-layer usage model

Due to the characteristics of mobile end-to-end data communication, some implementations modify the procedure as follows:

- The mobile terminal sends a request for a certificate to the user's side CA (or its agent).
- The CA authenticates the mobile terminal.
- The CA generates the certificate of the mobile terminal and sends the location information of the certificate (such as URL) to the mobile terminal.
- The CA stores the certificate of the mobile terminal in the storage area.
- Subsequently, the mobile terminal signs the data to be signed and sends the signed data, signature and the location information of the certificate to the application server.
- The application server acquires the certificate of the mobile terminal from the repository using the location information of the certificate.
- The application server verifies the validity of the certificate of the mobile terminal (if needed), verifies the signature with its public key in the certificate of the mobile terminal and authenticates the mobile terminal by using the certificate of the mobile terminal.
- A protected session is established between the mobile terminal and the application server.

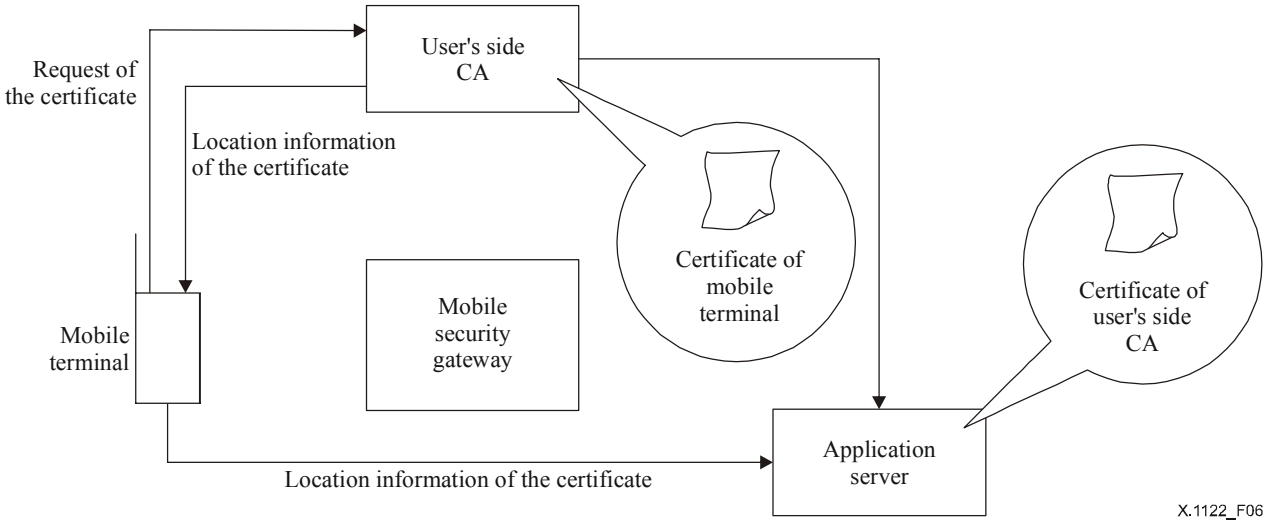

Figure 6/X.1122 – Client authentication in the over-the-session-layer usage model

8.1.3 Communication path encryption and integrity in the over-the-session-layer usage model

The communication path encryption and integrity in the over-the-session-layer usage model is executed in accordance with the following procedures:

- The mobile terminal transmits the suite of usable cryptographic algorithms and order of preference to the application server.
- The application server selects the specific cryptographic algorithm of the highest ranking from the common-key cryptographic algorithms that can be used by both parties.
- The server authentication is executed to prevent fraud of the application server.
- The mobile terminal generates the random number as a generator of session key and encrypts it with the public key of the application server in the certificate of the application server, in the case of the RSA key exchange method, and sends to the application server the encrypted generator of the session key. Both the application server and the mobile terminal

can make use of the common session key for subsequent communication from the generator.

- The encrypted communications are started.

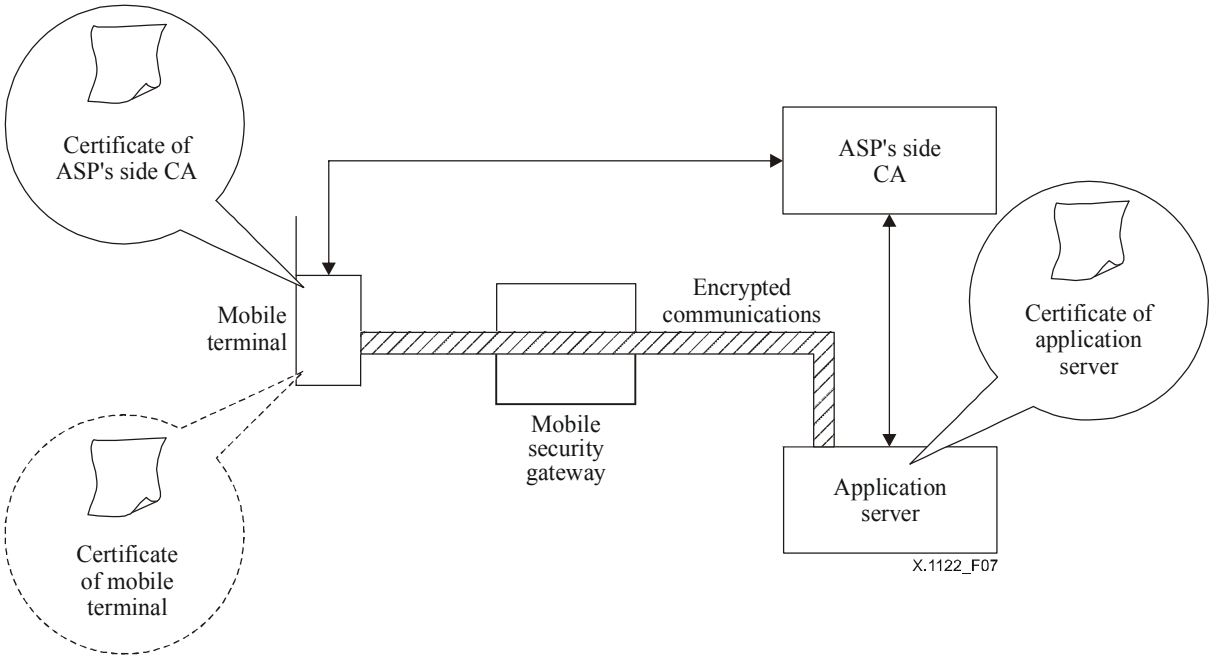

Figure 7/X.1122 – Communication path encryption in the over-the-session-layer usage model

8.2 Usage model on the application level

PKI can be utilized for an application-specific encryption function, a digital signature function, and a combination of both, which necessitates the identification and confidentiality in the data itself, and which cannot be covered only by the security on the communication path, such as authentication and encryption, over the session layer. Encrypted mails and an account-settlement application for e-commerce are examples of implementations of this model.

8.2.1 The signing function at the application level

This function guarantees the integrity of the data and creates a digital signature over the hashed value of data transmitted from the mobile terminal in order to guarantee that the data has been originated from a signing person. The signing function at the application level is realized by the following operations:

- Input or select the data to be signed.
- Process a digital signature over the hashed value of data using the private key stored in the mobile terminal or secure device, which is attached to the mobile terminal.
- Present the data to be signed, digital signature and the certificate including the public key corresponding to the private key.
- The recipient verifies the validity of the certificate and verifies the digital signature by the public key in the certificate.

This function can be used for a challenge-response type authentication by using a challenge (such as random numbers) from the server for the data to be signed.

8.2.2 The encryption function at the application level

The provision of an encryption function at the application level allows secure confidentiality of data in case an encryption on the communication path is not sufficient. The encryption function at the application level is realized by the following operations:

- Generate a random number as a common-key.
- Encrypt the data with the common-key using a symmetric cryptographic algorithm.
- Acquire the certificate of the person to whom the transmission is being made.
- Encrypt the common-key with the public key in the certificate.
- Send the encrypted data and encrypted common-key.
- The recipient decrypts the encrypted common-key with his/her own private key.
- Decrypt the encrypted data with the common-key.

9 System configuration examples

9.1 Configuration examples of a certificate management system

Figure 8 shows an example of a system in which the communication carrier issues a certificate for its user. Offline processing is used to issue/revoke a certificate, and the VA is used to verify the certificate.

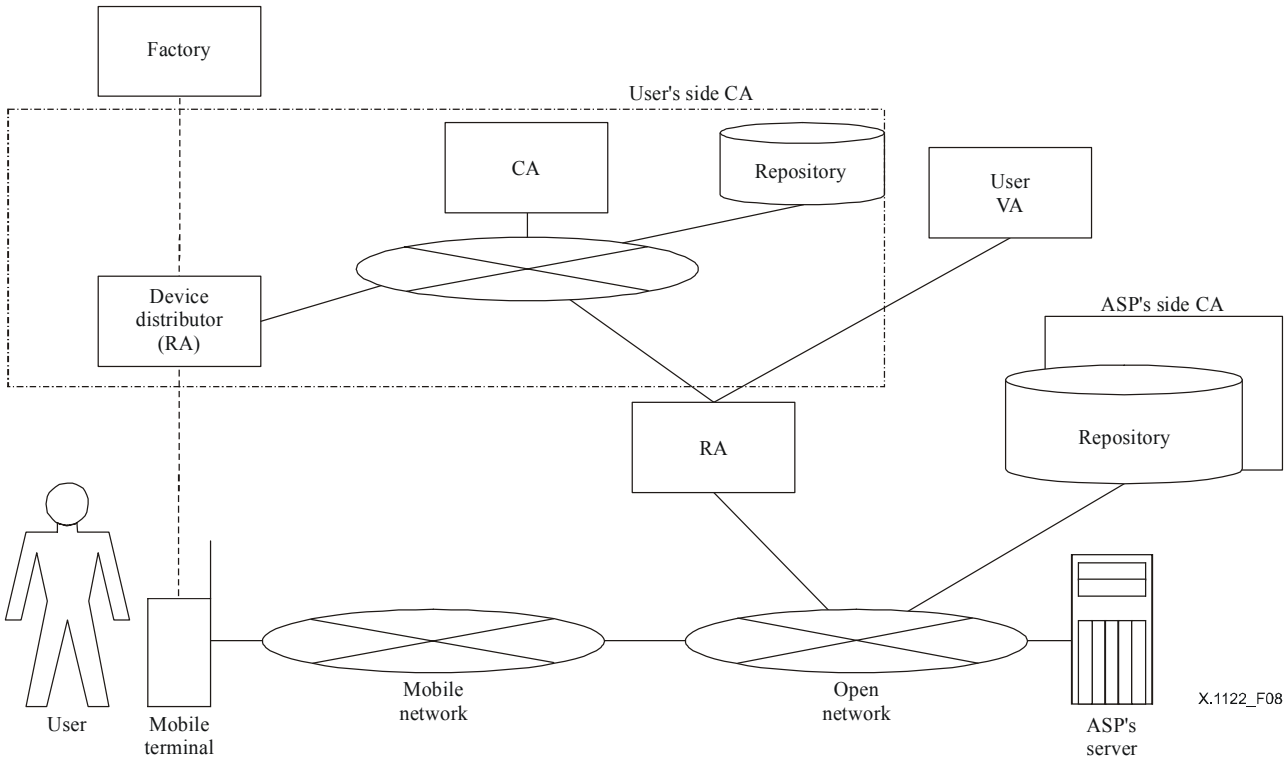

Figure 8/X.1122 – Example of a system in which the communication carrier issues a certificate for its user

9.1.1 Example of certificate issuance

There are two examples for issuing of the certificate depending on the location where the key is generated: one is a method in which the key is generated in a factory, the other is a method in which the key is generated in the mobile terminal or tamper-free token, like UIM, after he/she purchases the mobile terminal and the client wants to issue the certificate.

It is very important for the application of the certificate to prove it is in possession of the private key. The proof of possession (POP) protocol allows a CA/RA to check the validity of the binding between an end entity and a key pair. It is required that CAs/RAs must enforce the corresponding certificate. Specific POP may be accomplished in different ways depending upon the type of key for which a certificate is requested.

Figure 9 shows an example of a system in which the communication carrier issues a certificate for its user. The key is installed into the device when it is shipped from the factory. The certificate is applied for when the user purchases the device from the distributor and it is installed by the distributor. This is when POP is carried out.

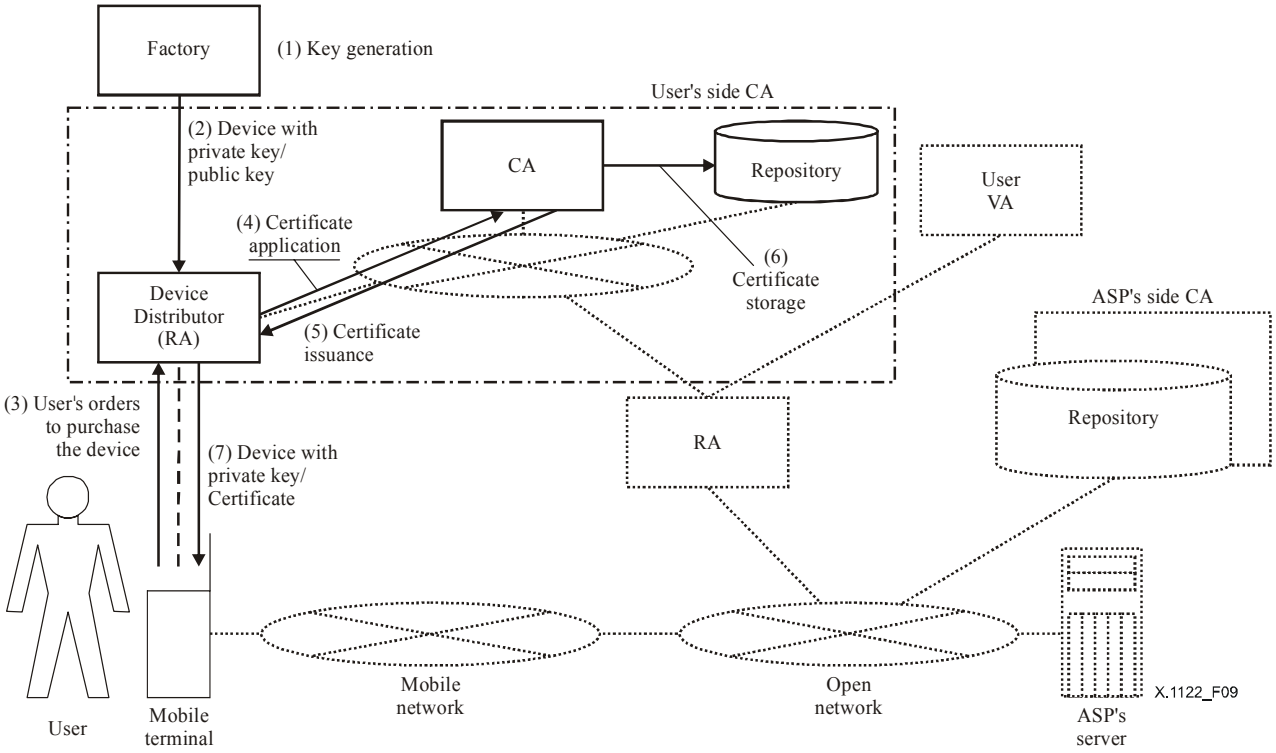

Figure 9/X.1122 – Example of certificate issue (1)

Figure 10 shows an example of a system in which the client generates a key and issues a request for the certificate itself. The certificate is applied for when the user wants to receive it from the CA and the private key can be kept secret in the mobile terminal. Before the above-described protocol is performed, it is assumed that both the mobile terminal and CA should share the common secret to provide the integrity and authenticity of the exchanged message. This method can protect the privacy of the private key of the mobile terminal.

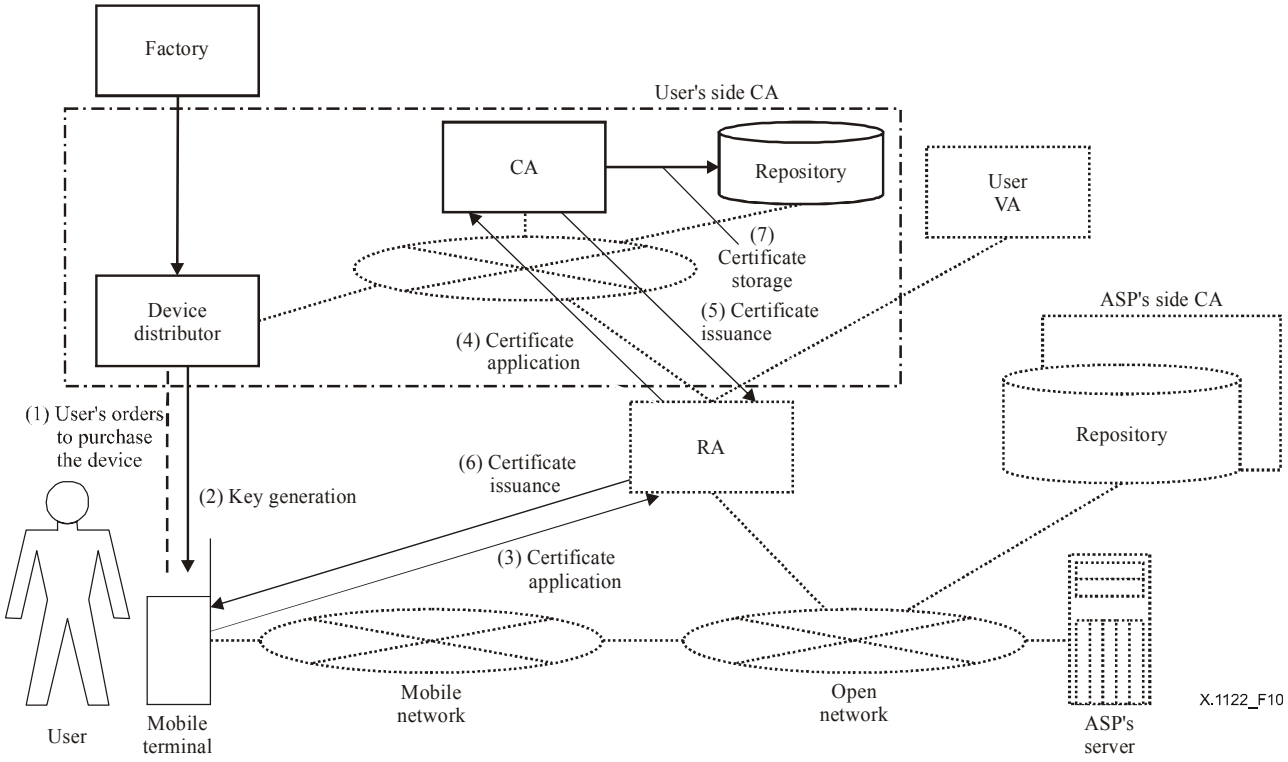

Figure 10/X.1122 – Example of certificate issue (2)

9.1.2 Example of certificate verification

In general, the mobile terminal has a limited computational power and a limited memory size. Therefore, the certificate verification scheme based on the CRL is difficult in the mobile terminal. The online certificate verification scheme utilizing the VA is preferred in the mobile terminal. Figure 11 shows an example of online certificate verification.

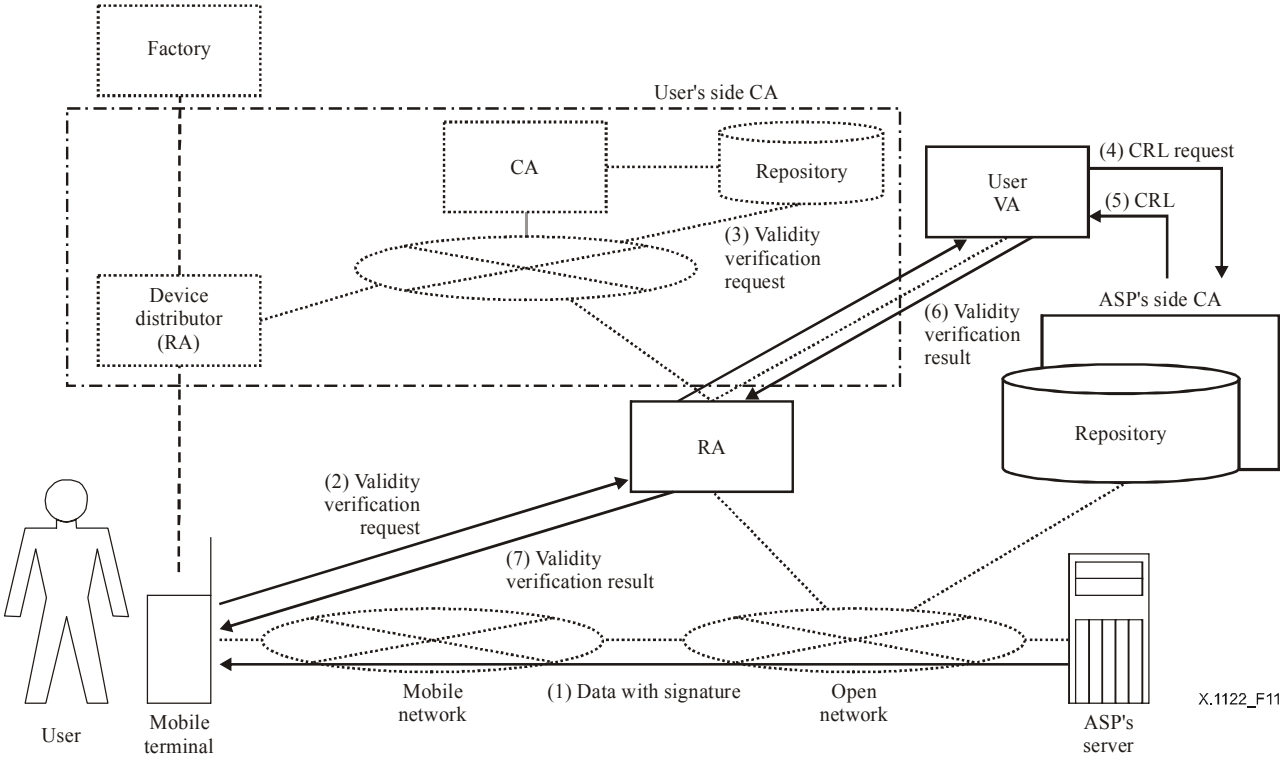

Figure 11/X.1122 – Example of certificate verification

To verify the data received from an ASP, the user inquires of a VA if the certificate of the ASP is valid through the RA. The VA verifies the validity of the certificate by acquiring the CRL from the ASP's side CA. The verification result is returned to the user through the RA. It is essential that the mobile user is able to verify the verification result (see 10.2.3.2).

9.1.3 Example of certificate revocation

To revoke a certificate, the user also visits the distributor to follow the revocation procedure. However, assuming an emergency condition, the service to suspend the validity of the certificate on the network is provided. To suspend the validity, an application is submitted to the CA through the RA. The revocation is completed by submitting the signed application to the CA through the RA. In the case of a lost or stolen mobile terminal, alternative methods of suspending validity would be needed. For example, the user can suspend validity by calling the device distribution directly to request suspension. Figure 12 shows an example of certificate revocation.

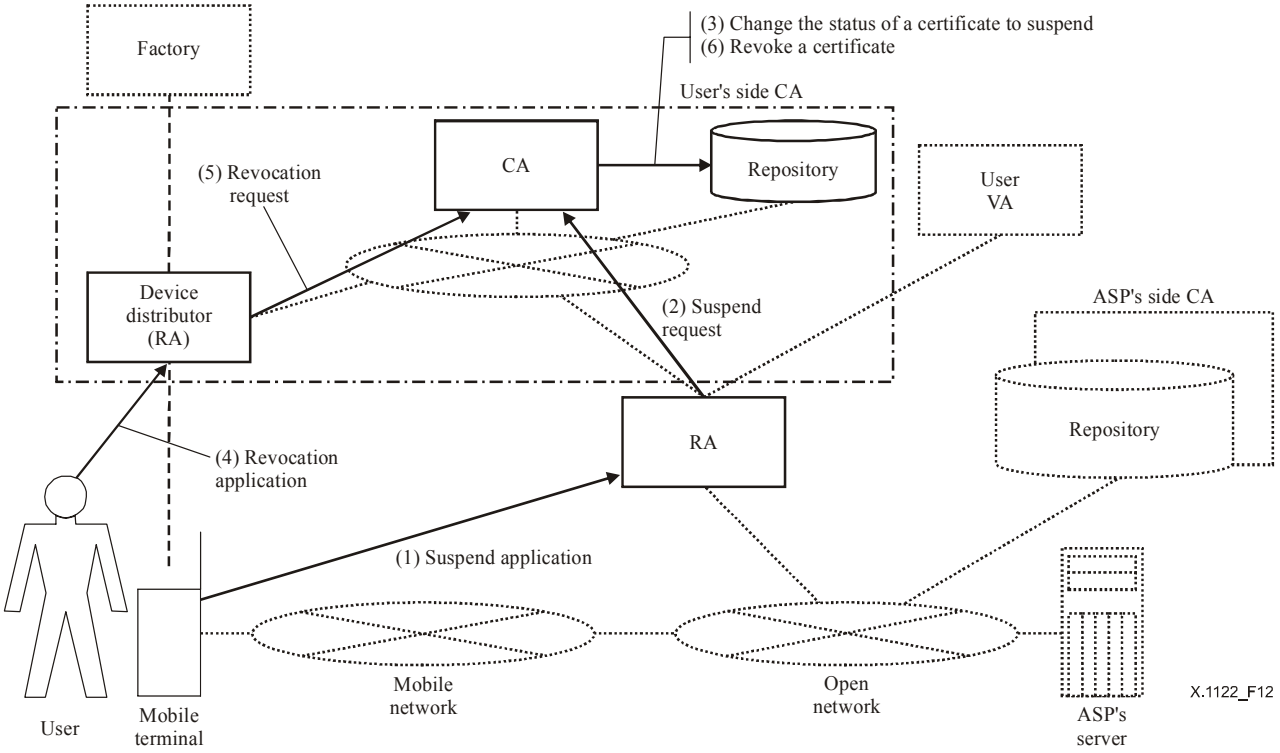

Figure 12/X.1122 – Example of certificate revocation

9.2 An example of an authentication model based on the certificate

The following is an example of an authentication model when a certificate is used.

9.2.1 Example of an authentication model for users, carriers and application service providers (ASP)

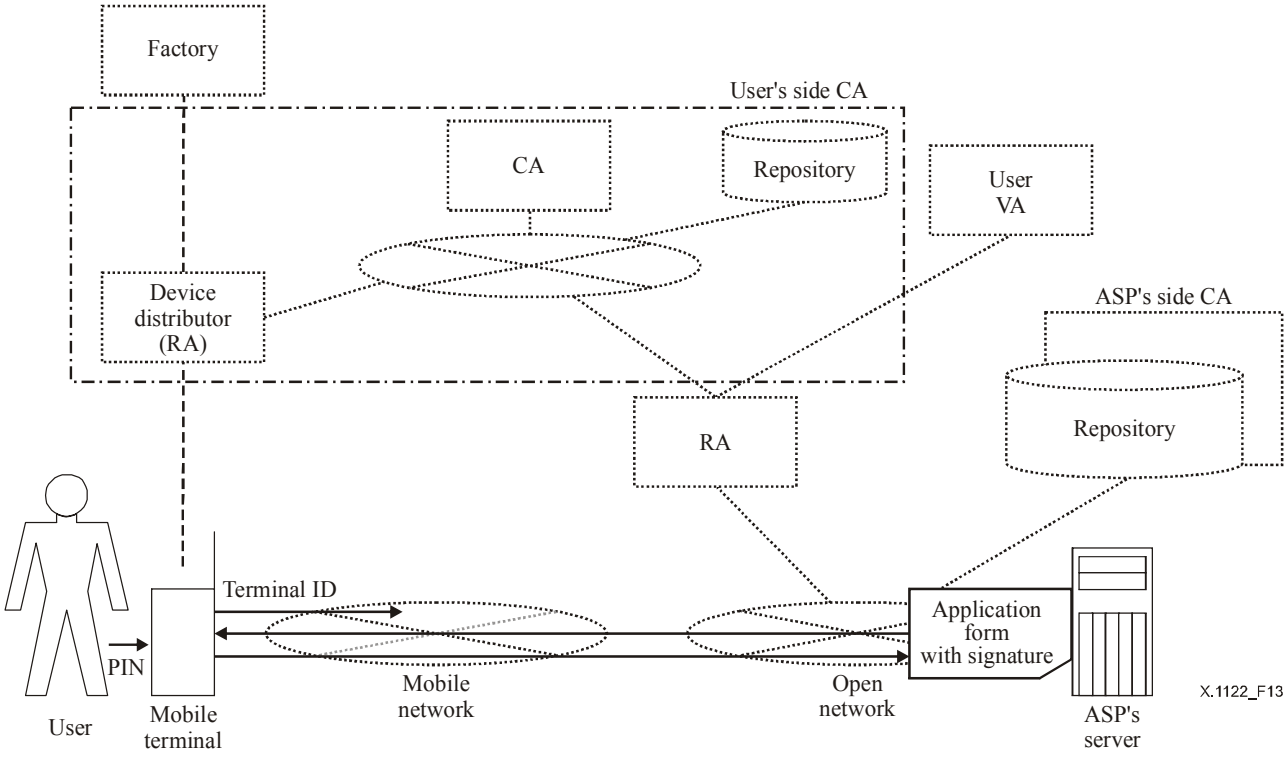

Figure 13/X.1122 – Example of an authentication model for users, carriers and ASPs

9.2.1.1 Authentication of a mobile terminal user by a carrier

The mobile terminal is identified as a legal subscriber by presenting the terminal ID of the mobile terminal within the carrier.

9.2.1.2 ASP authentication by a mobile terminal user

To check if it is a reliable ASP, the certificate of the ASP is verified. For this verification, the user may receive the certificate of the ASP itself and the relevant authentication data such as digital signature, message authentication code, and the encrypted data using the private key of the ASP in order to verify it within the user's mobile terminal. The user can also ask the VA to verify the received certificate through the RA. The user can also specify the certificate URL instead of the certificate itself. For ASP authentication, the user verifies the relevant authentication data using the pubic key corresponding to the public key in the certificate.

9.2.1.3 Mobile user authentication by mobile terminal (right of card user)

To avoid illegal use of a mobile terminal by a third party, when using the information on a chip such as a smart card (such as UIM) stored in a mobile terminal, user authentication with a PIN number should be performed. Another user authentication scheme, like finger printing authentication, could be used.

In addition, a locking mechanism should be provided to disable the use of the smart card if the device is lost or stolen.

9.2.1.4 Mobile terminal (or mobile user) authentication by the ASP

The user is certified on the ASP's side. Like the ASP authentication by mobile terminal, the ASP may receive the certificate of the mobile terminal (or the certificate of the mobile user) itself and the relevant authentication data such as digital signature, message authentication code, and the encrypted data using the private key of the user in order to verify it within the ASP. The ASP can also ask the VA to verify the received certificate. The ASP can also specify the location information of the certificate instead of the certificate itself. For the authentication, the ASP verifies the relevant authentication data using the pubic key corresponding to the public key in the certificate.

9.2.1.5 Legitimacy of application

To verify whether the application has really been originated from the mobile terminal that was authenticated in 9.2.1.4, the ASP verifies the digital signature attached to the application. The signature function on the application level can be utilized. The application form can also be encrypted for the purpose of divulgement protection.

9.2.2 Example of an authentication model utilizing a financial institution

An authentication model utilizing credit card information, or other existing infrastructures, is also possible, see Figure 14.

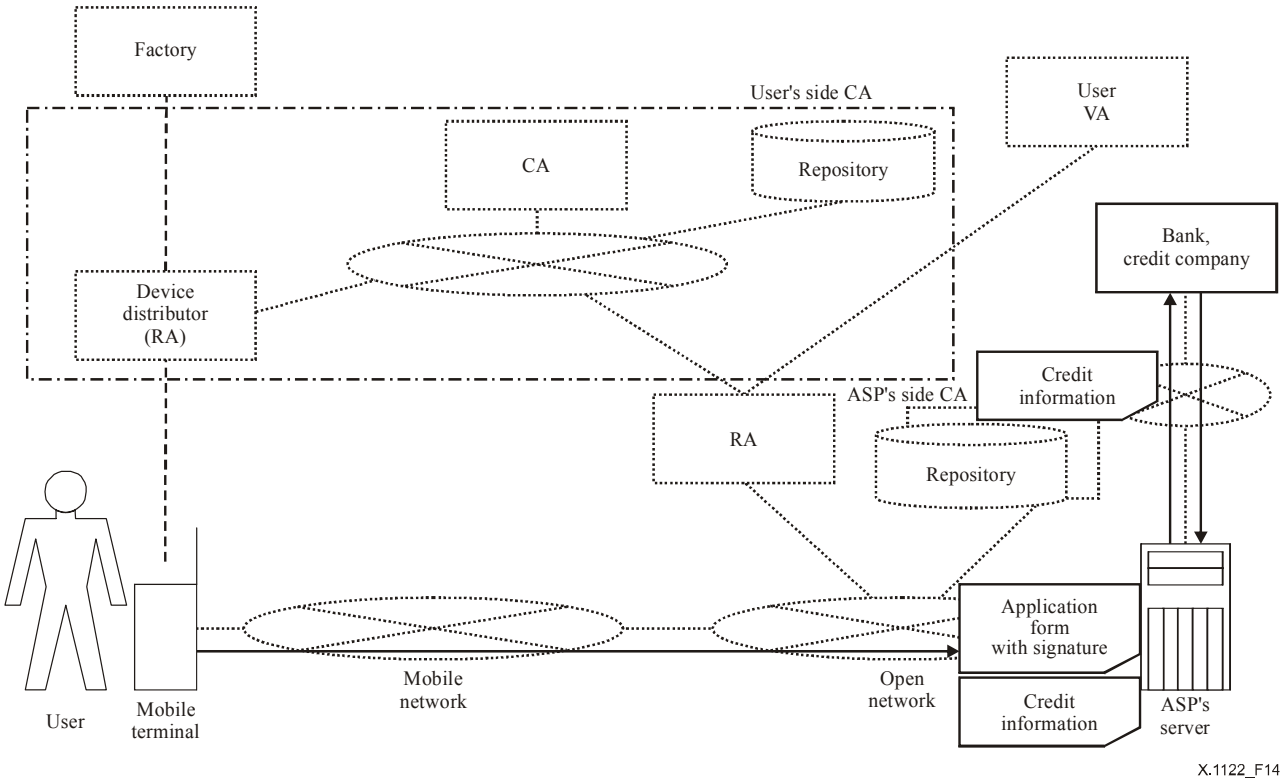

Figure 14/X.1122 – Example of authentication model utilizing financial institution

9.2.2.1 User authentication by a bank or credit card company

A bank or credit card company acquires the financial information (account number, credit card number, etc.) from the user to authenticate the user as a legitimate card owner.

On the user's side, the credit card number and expiration date stored in the smart card (UIM) chip are used, so that they do not need to be entered at every authentication. User authentication, like a PIN, is required when this information is used in the mobile terminal in order to identify the legal user that has an access right to it.

The financial information may also be implemented as an attribute certificate.

When the financial institute information is transmitted, it should be encrypted with a random session key that is encrypted by the public key of subject financial institute, but not by the public key of the ASP.

The authentication result is returned to the ASP from the financial institute.

9.2.2.2 ASP authentication by a bank or credit card company

When an open network is used instead of an existing payment network, the ASP must be authenticated as an authorized affiliated distributor by submitting a certificate and the relevant authentication information that indicates that it is an authorized affiliated distributor, issued by a bank or credit card company.

9.2.2.3 ASP authentication by user

The ASP must be authenticated as an authorized affiliated distributor by submitting a certificate and the relevant authentication information to the user that indicates that it is an authorized affiliated distributor, issued by a bank or credit card company. For example, an attribute certificate, issued by a bank, can be used to certify an authorized distributor.

10 Considerations of PKI for mobile end-to-end data communication

10.1 Considerations of interoperability with an existing system

When adapting the existing system based on PKI already developed with the open network into a mobile environment, the certificates for the ASP, or other users in the open network, will have been issued and used in (and behind) the ASP.

In such cases, the mobile terminal must be capable of verifying the validity of the existing certificates.

Furthermore, if the certificate format used in a mobile environment is different from that of the ASP's certificate format because of constraints of throughput capacity or memory capacity, the existing ASP system needs to be modified so that the ASP can verify the validity of certificates for mobile terminals.

In addition, if the mobile terminal does not have enough space to store his/her/its certificate, the mobile terminal may keep the certificate URL instead of the certificate itself, and it sends the certificate URL to the ASP. The ASP needs to retrieve the certificate using the certificate URL.

At present, SSL/TLS are widely used as message protection protocols (and authentication protocols) for an end-to-end data communication.

However, the cryptographic algorithm and/or certificate format that can be used for the TLS may not be suitable for the processing performance of the mobile terminal.

For example, in many existing systems using the PKI, the RSA cryptographic algorithm is widely used as a signature algorithm. However, the RSA cryptographic algorithm may need more processing powers than the mobile terminal has. It is preferred that a cryptographic algorithm with a low power or less-memory should be used for the mobile environments. One of the alternatives to the RSA is an elliptic curve algorithm. An elliptic curve cryptographic algorithm is faster than the RSA, and the mobile terminal can process it within a practical time period. The elliptic curve cryptographic algorithm, however, has not yet been adopted into the specifications of the TLS, etc. In addition, when elliptic curve cryptography is used, the hash bit length may exceed the key length, which may require multiple-time cryptography processing.

While the provision of the VA with a signature-verifying function is one approach to resolving the above problem, another consideration is how to protect the communication between the mobile terminal and the VA.

As a common-key cryptographic algorithm is much faster than a public-key cryptographic algorithm, technically it should not have problem even if it is adopted for the mobile terminal.

In addition, as SSL/TLS interchange their certificates at the initialization stage, this may require more storage area than the mobile terminal has.

Although an approach to convert a protocol using a mobile security gateway has been proposed, as previously mentioned, the authentication protocol between the ASP and user used at a higher layer may be needed.

10.2 Considerations for the use of PKI in the mobile environment

10.2.1 Considerations of key generation

10.2.1.1 Key generator

When adopting a model where the user generates a pair of keys, although a key generation function is required within a device (i.e., a model which generates the key within the device is adopted as the location where the key is generated), the storage capacity and processing performance will possibly cause problems in the mobile terminal.

When adopting a model in which the CA or third-party generates a pair of keys, operational considerations and a mechanism to prevent compromising the key are required.

10.2.1.2 Location for key generation

For security reasons, it is desirable to generate a private key within a device, and the processing performance will be another possible problem.

When adopting a model in which an externally generated key is installed in the device, a mechanism to prevent compromising the key is required.

10.2.1.3 Location for key/certificate storage

In general, nobody can remove a private key from the device. The private key must be stored in the protected area. There are two types of protected area:

– Physically protected area: The private key is written into the physically protected area such as the ROM within the mobile terminal or external devices like smart cards.

– Software protected area: The private key is stored in the software protected area within the mobile terminal.

Note that the software protected area must be a secure area so that only a valid user can rewrite or access the private key by access control and/or cryptographic protection. The typical cryptographic protection of such information is to use the password-based encryption scheme.

In addition, the storage of the user's public key (certificate) and the certificate of the root CA in the protected area within the device is preferred.

10.2.2 Considerations of certificate application and issuance

10.2.2.1 When the certificate is pre-installed in the device

For models in which the mobile user purchases the device with the certificate pre-installed, it is difficult to update the key and the certificate.

In addition, in the case where the certificate is not tied to the mobile user, it may be required, depending on usage, to issue an attribute certificate describing the association of the certificate with the mobile user.

10.2.2.2 When the key is pre-installed in the device

As key updating is difficult, the device is discarded when the certificate is revoked.

10.2.3 Considerations of certificate use

10.2.3.1 Considerations when the mobile terminal signs digitally

For the TLS, the method of attaching the certificates (all certificates from the root CA certificate to the signer's certificate) to the message is adopted as the method to associate the root CA certificate with the signer's certificate.

However, if all certificates from the root CA certificate to the signer's certificate are attached when the signature is attached, it may result in a heavy load due to restrictions such as the storage capacity of the mobile terminal.

Although the technique of attaching a URL describing the location where the certificate is stored to the message is also available, it is not yet supported by TLS.

10.2.3.2 Considerations when the mobile terminal verifies the signature

Models where certificate validity is verified by the verifier itself might be unsuitable for mobile terminals due to many restrictions in processing power and storage capacity.

For models that use a VA, the application using the certificate must know the VA on which it relies. In addition, when communicating with the VA, it must be capable of ensuring that the VA is valid.

In the example shown in 9.1.2, the mobile terminal accesses the VA through the RA. In this case, the mobile terminal requires a function to recognize the RA on which it relies in advance, as well as a function to certify (authenticate) that the RA is correct while communicating with the VA. The RA requires a function indentifying the VA that the mobile terminal relies on and a function certifying that the VA is valid while communicating with it.

10.2.4 Considerations concerning the CA

For existing systems using the PKI, reliable relationships between different certification domains are established by constructing a hierarchy with multiple CAs and establishing cross-certification.

However, when checking the validity of certificates of each CA for signature verification, the processing power of the mobile terminal may pose possible problems.

When a VA is not used, it is desirable to construct simple structure of CAs.

10.3 Considerations concerning the PKI in general

10.3.1 Considerations concerning key generation

10.3.1.1 Key generator

For models where the user generates the keys, it may be possible that someone may search another's keys by searching for certificates that match the public key generated, and pretending to be the owner of that certificate.

Therefore, for models in which the user generates the keys, it is required to adopt a key with enough length for the number of users assumed.

In addition, certain methods may be required for preventing the easy acquisition of another's certificate.

10.3.2 Considerations concerning certificate application/issuance/activation

10.3.2.1 When certificate activation procedure is required

When the user explicitly follows the certificate activation procedure, a mechanism to ensure that the procedure is followed by the user him/herself is required.

When a certificate activates online, the user signs the activation application data and transmits it to the RA, etc. For offline processes, the same mechanism as a credit card (including calling an operator to request activation) can be utilized.

10.3.2.2 When applying for a certificate online

A mechanism to ensure integrity and authenticity during application is required. In fact, CA verification, applicant verification, communication path protection, etc. are required.

10.3.3 Considerations concerning certificate revocation

To adopt a model with online revocation, a mechanism to verify that the applicant is the user is required. Especially, in the case where a certificate is revoked due to the loss of a private key, applicant identification with a digital signature cannot be used. Therefore, another method (such as a PIN) must be provided.

To adopt a model with offline revocation, the provision of the mechanism to "suspend" a certificate online may be required in the case of emergency.

10.3.4 Considerations regarding the renewal of a certificate

In addition to the considerations regarding certificate application and revocation, as a unique problem on the certificate update, the solution to prevent certificate update from being omitted is required from the system availability point of view.

10.3.5 Problem with certificate description

The information contained within a certificate must be carefully reviewed due to the possibility that a certificate will circulate extensively beyond the intent of the issuer.

Appendix I

Examples of service models

This appendix describes the service models of the mobile PKI.

I.1 Certificate management service models

In clause 9, an example of offline use of the system is provided in which a communication carrier issues certificates. This appendix provides other service models of certificate management.

I.1.1 Example of a system in which an ASP issues certificates

The examples shown in Figures I.1 and I.2 illustrate two kinds of certificate; the first certificate is provided by the 1st Slot CA (see Figure I.1) which is a CA of a carrier providing the certificate to a mobile terminal to be used in secure session transport. The second certificate is provided by the 2nd Slot CA (see Figure I.2) which is a CA of the ASP providing the certificate to a mobile terminal to be used by any applications of mobile terminal. An ASP uses a CA certificate issued by a communication carrier to issue its own certificate. To issue/revoke a certificate, the system on the carrier side (1st slot CA) uses offline processing and the system on the ASP's side (2nd slot CA) use online processing. Meanwhile, when applying for the certificate, the system on the ASP's side (2nd slot CA) uses a certificate issued by the communication carrier (1st slot CA) as communication path protection and applicant authentication and accepts the application online.

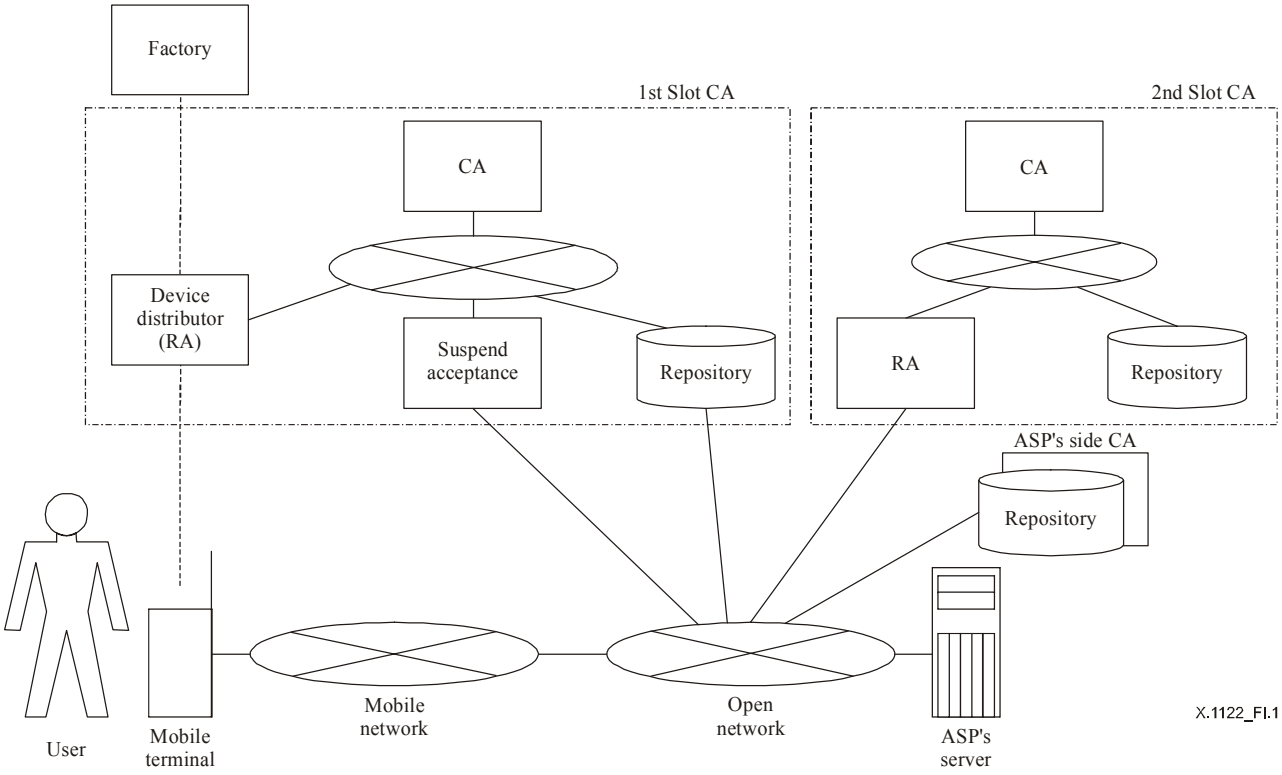

Figure I.1/X.1122 – Example of a system in which an ASP issues certificates

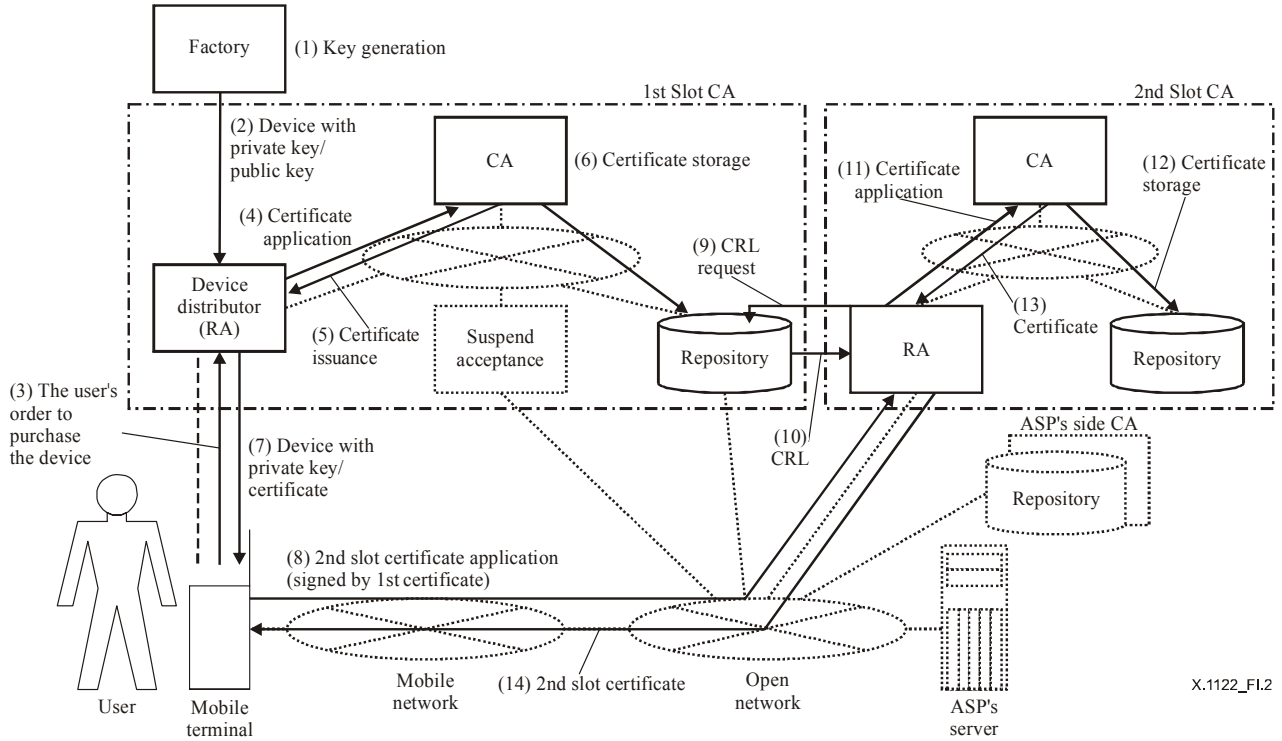

Figure I.2/X.1122 – Example of 2nd slot certificates issuance

To revoke a certificate issued by 2nd Slot CA, the user also accesses the RA through the network and follows the revocation procedure.

I.1.2 Example of a system in which an attribute certificate is utilized

This example (see Figure I.3) assumes that the ASP uses the certificate issued by a communication carrier for applicant identification and so on, and uses an attribute certificate for more sophisticated access control, for instance. While a User AA is used to issue an attribute certificate to the user, user CA is used to issue certificate to the user.

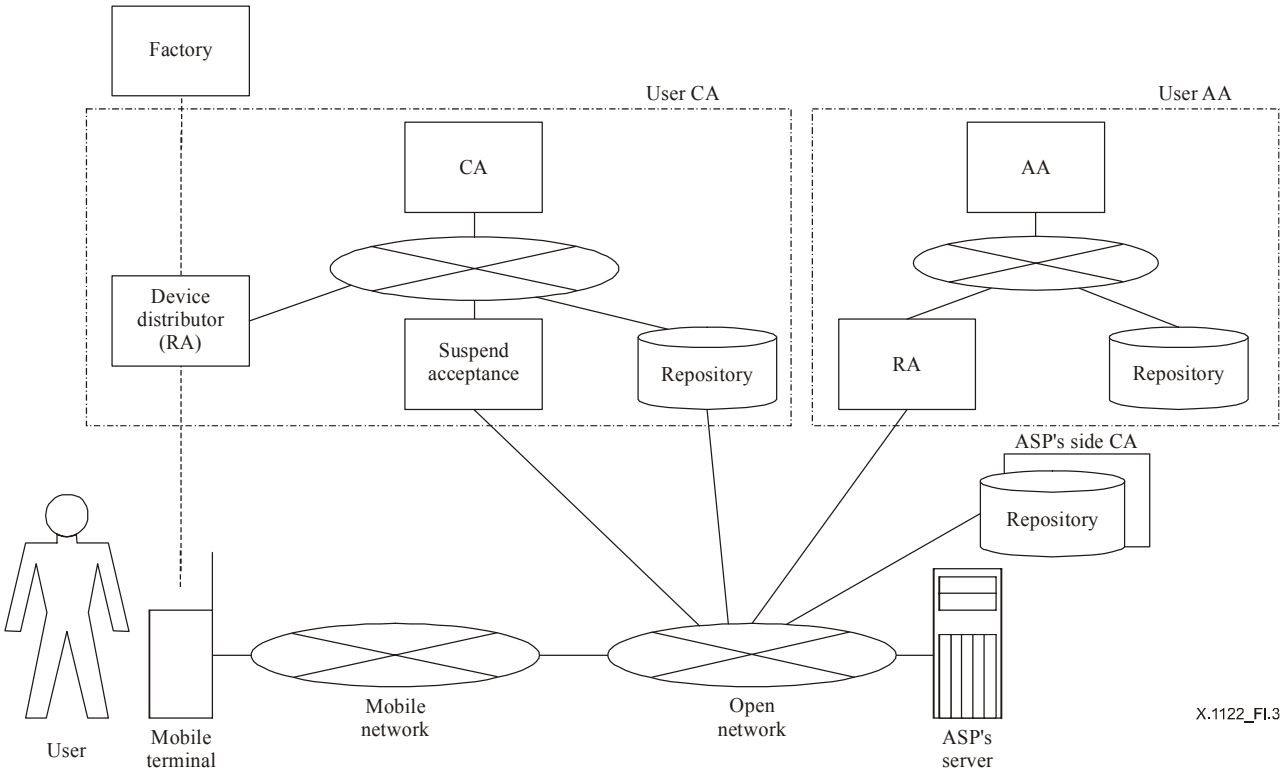

Figure I.3/X.1122 – Example of a system in which an attribute certificate is utilized

The system on the communication carrier side (User CA) utilizes offline processing for certificate issuance and revocation, and uses a VA for certificate verification.

The system on the ASP's side (User AA) accepts the application from a user online, generates an attribute certificate based on the application policies, and then associates it with the certificate issued by the communication carrier. The attribute certificate is stored in the repository within the AA. (A model in which an attribute certificate is transmitted to a user is also possible.)

If an ASP has received data with a signature from its user, it first acquires the CRL from the repository in the carrier side CA to verify the validity of the certificate. (The shop also verifies the signature on the data transmitted from the user.) Next, the ASP acquires the attribute certificate from the ASP's side AA to verify whether the user has the right to utilize the service, see Figure I.4.

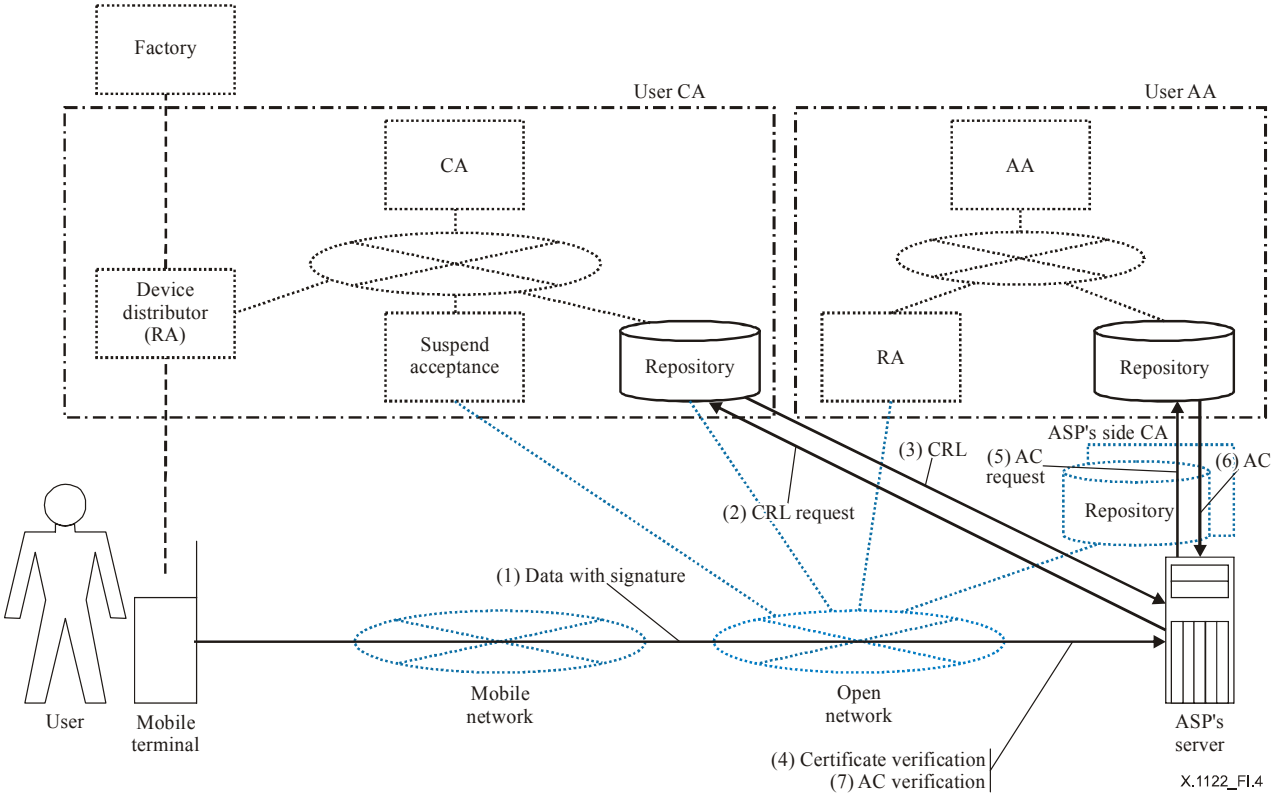

Figure I.4/X.1122 – Example of an authentication model using an attribute certificate

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks and open system communications**
Series Y	Global information infrastructure, Internet protocol aspects and Next Generation Networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2004